JOURNAL OF OPTOELECTRONICS LASER ISSN:1005-0086
Volume 41 Issue 3, 2022

# K-Means Algorithms to Enhance the Performance of Assess and Detection of Diabetes in Healthcare

**R. Ganesan[*1], D. Pavithra[2], Srilakshmi Ch[3], A. Karthikeyan[4], Anitha Christy Angelin. P[5] & Dinesh Mavaluru[6]**

[*1]Assistant Professor, Department of Computer Science and Engineering, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Avadi, Chennai, India

[2]Assistant Professor, Department of Information Technology , Dr. N.G.P Institute of Technology, Coimbatore -641048, Tamil Nadu, India

[3]Assistant Professor, R.M.D Engineering College, Kavaraipettai, Thiruvallur -601206, Tamil Nadu , India

[4]Assistant Professor, Department of Computer Science and Engineering, Panimalar Engineering College, Poonamallee, Chennai, Tamil Nadu

[5]Assistant Professor, PSNA College of Engineering and Technology, Kothandaraman Nagar, Dindigul, Tamilnadu, India

[6]Department of Information Technology, College of Computing and Informatics, Saudi Electronic University, Riyadh, Saudi Arabia

**ABSTRACT** Diabetes is one of the ancient diseases that cause disturbance to the person after limited ages in their life. In such cases, experts have introduced a vast algorithm related to the health care system. By enhancing the model algorithm to detect the presence and the spread of disease through this paper, the author has listed a few Machine Learning Algorithms. Most commonly K-means algorithm automatically eliminates the non- accessing data, which can reduce the identification timing. Finally, this proposed model has resulted in 98% of accuracy, and that is formed with a pack of Pima Indians Diabetes (PID).

**Keywords**: Diabetes detection, KNN algorithm, Decision Tree, Machine Learning.

## I. INTRODUCTION

It is one of the hardest things to learn about medicines and related studies about health care management systems. Even doctors sometimes collapse. They do not get the proper knowledge of analyzing the presence of disease inside the human body. In such a case, if there is a separate system to navigate and analyze the presence of disease, it would be more helpful for both the person, either doctors or the patients, to get early treatment. In diabetes mellitus, the patient's body would face trouble in the movement of glucose content within the body. Here Glucose is a kind of sugar that should be transferred all over the body. After a few days, this lack of glucose level would lead to high sugar levels in the blood and does not enough for the cells and remaining organs. To transfer energy from the cells to the body, glucose is considered one of the sources to transfer. The total glucose content is calculated by the average amount of insulin and glucagon being passed into the cells. Both the carrier options deal with a major portion, for example, insulin acts as the blood glucose level, and glucagon is used to rise and boost the blood glucose level. Both the portions are created by the islets, called the Langerhans, located in the pancreas of the human body.

Analysis of DM can be done in two different processes. For example, it can be done manually or else with the help of a medical practitioner. Most of the automated devices result from fake results and few drawbacks in showing the results. ML and AI methods have been advanced with this prediction task and built automatic DM detection systems. Several types of research have been made to match the Artificial Intelligence and Machine Learning modules to control the DM and make the management process with additional personalization methods. K means the Algorithm is being used in vast areas, and it has been alternated as per the data given to the system. The first thing related to the K-means algorithm is to select the number of clusters that require identifying the data in the clustering effect. Other than the K-means algorithm, KNN is being used in major things, which are considered as K nearest neighbors algorithm that is used in the analyses of labels from the given data.

## II. LITERATURE REVIEW

Diabetes mellitus is one of the unregulated diabetic diseases that is caused due to organ failure. If there is no more Machine learning and Artificial Intelligence in this world, we will still not get any updates about network connections and other data-sharing tool. Currently, most data analysis is based on the health care system, as per the same concept paper [1] evolves the personalization under diabetic disease. By introducing the evaluation process of classical and best-assembled ML models, it helps in most cases by creating different, and comparison data sets that can be deployed in the health-related analyzing system denoted as comparative analysis [2]. Besides the diabetic cause, cervical cancer has also become one of the numerous diseases recently. With this paper [3], the author has introduced a few machine

learning algorithms that function online and offline. While getting a result from its operational concepts, it deals with F1 scoring and proves one of the highest outputs receive that works in offline sessions. To cluster, an object clustering is considered one of the default objects that depend on the principle of showing similarities in approaching the performance list. Here the author of the paper [4] has analyzed the DICOM technology and acquired the dataset with the research-based network systems. For the last two years, people have been facing enough difficulties due to the spread of Covid-19. Apart from the working people, students are more concentrated and prepared to attend online classes, from this we can understand the importance of youngsters to this world.

On the other hand, liver syndrome results in the increased spread, mostly the young people. To overcome the spread by increasing the immunity strength of the teenagers, this paper consists of a few UCI datasets which give comprehensive outcomes [5]. In this paper [6], the author has developed AI-based chronic and cardiovascular detection with the ML modules. This data is being processed, which entails the variable with sufficient application to be deployed as a software engineering process. A study of blood groups is being used to create the assessment of the prevalence of ABO and different type blood groups to detect the presence of diabetes mellitus that is spread over with the help of type 2 causing [7] & [8]. Through this model [9], the author has tested and got accuracy in the nondiabetic employees from the Mexico state here, the author made BMI (Body Mass Index) the most level of guidance to detect the genetic variants and parental history to consider the risk evaluation. Usually, the cluster methods do not have any negative impacts. In that case, it has been implemented with the knowledge of microorganisms by adding simple colonies for evaluation purposes [10].

## III. PROPOSED WORK

Typically the KNN is a kind of classification algorithm, and the classification is used for determining the group in which the requirements are being stored, most experts use this kind of algorithm to make a future prediction, with the help of a computation network under the machine learning control. Apart from the concept of the classification algorithm, people used to mention it as reference data, which is being used for making a decision and things actual. What data to be classified here must be computed with the current knowledge and analyzed with the previous data records? For example, if the user mentioned numerical data, the system would automatically search for the given data in the reference folders that are collected. It can require millions of data, but this algorithm can hold enough data with it. This would be the reason to relate this as a predictive model. Typically not only from this part of the algorithm, one of the everyday things that match all sets of the algorithm is, but there should also be proper statistical data analysis, without having the static data, we cannot create a better analysis in the future. From Figure 1, we can understand the concept of separation and splitting up clusters into various sections. Here the acceptance of clusters are being terminated according to the conditions that are declared with the reduction of temperature.

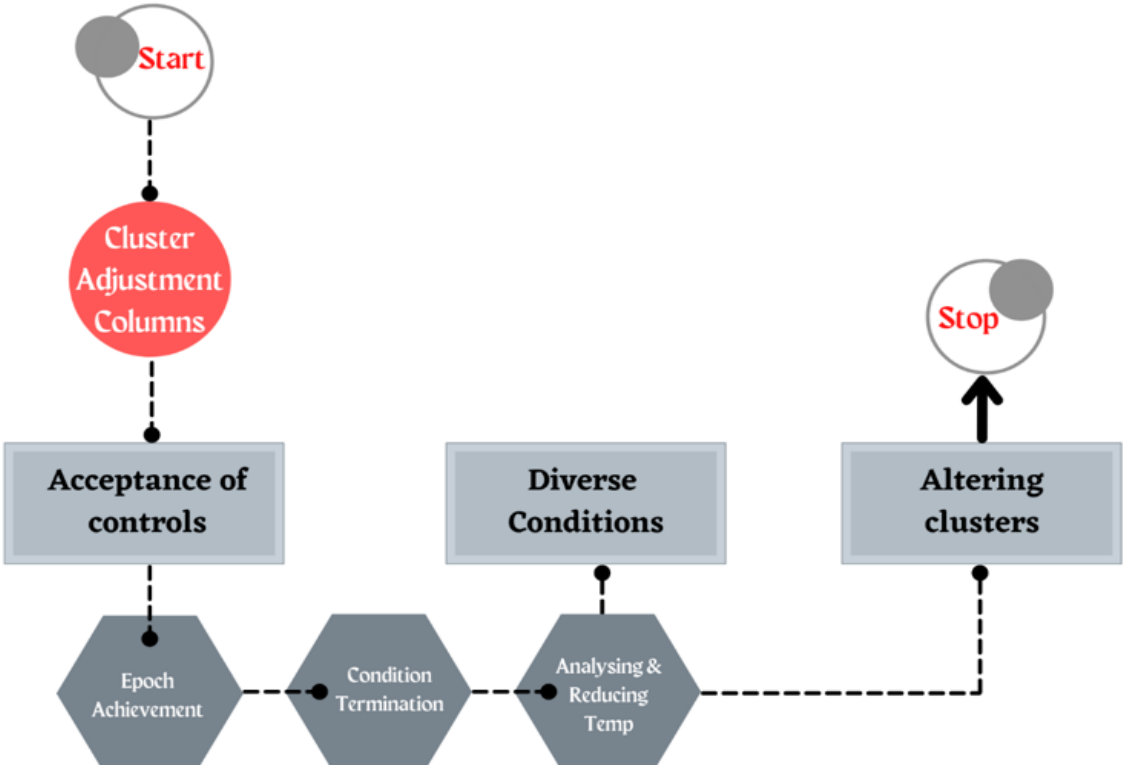



Figure: 1: Work flow of cluster in KNN algorithm

The **K-Means Algorithms to enhance the detection of diabetes in healthcare** using the machine learning network is denoted by $K = P \cup M\{0\}$. The letter $P$ stands for the collection of customer touch points. The processing facility is denoted by the number 0; $M$ denotes **to enhance the performance of assess and detection of diabetes in healthcare**, whereas K denotes a healthcare system. H is the set of time periods that occur throughout the day, $H = \{H_1, H_2, \ldots\ldots, H_n\}$; $n$ is the overall number of time intervals G denotes the collection of road segments in the road infrastructure, $G = \{G_1, G_2, \ldots., G_n\}$; $G$ denotes the number of road section types. $D = \{D_1, D_2, \ldots., D_n\}$; $D$ is the number of area types in the area set.

Let $\rho_i$ signify the required to charge stations able to charge equipment utilisation ratio $\rho_i = (\lambda_i / x_i \mu_i)$ According to the conventional slight Equation, the waiting period for such $g^{th}SK$ and trying to charge point $i$ is represented by Equation (1).

$$h_{ig}^{G} = \sum_{i=1}^{x} \frac{(x_i\rho_i)^{s_i}\rho_i}{\lambda_i x_i!\,(1-\rho_i)^2 \varphi_{D_i}} \cdot \left( \sum_{n=0}^{x_i - 1} \frac{(x_i\rho_i)^n}{n!} + \frac{(x_i\rho_i)^{x_i}}{s_i!\,(1-\rho_i)} \right)^{-1} H_{ig} \times g^{th}SK \qquad (1)$$

In the charging k-means method used to detect the diabetes for the $g^{th}SK$ at end point $i$ is as shown in Equation (2).

$$h_{ig}^{G} = \sum_{i=1}^{g} \frac{S_{max} - S_{ig}^{H}}{n_h} \qquad (2)$$

**K-Means Algorithms to enhance the e**nergy consumption is influenced not just by healthcare diabetes speeds. Whenever a $SK$ with a charge travels at $A_k$ transportation distance ŋkm/h $k$ on a flat, the able to run power $D(A_k, k)$ is represented by Equation (3).

$$D(A_k, k) = \frac{\left((y + A_k).g.\int k + (R_n.Z_i.k^3/22.56)\right)}{3700\text{ŋkm/h}k} \qquad (3)$$

In $x$ is the allocation of **detection of diabetes in healthcare** now no longer altering in identical timeframe. (i, j). $M$ healthcare range of things are considered, together with avenue type, delivery time period, however additionally $M_1, M_2, \ldots.. M_n$ time-various **to enhance the performance of assess and detection of diabetes in healthcare** of the transition as with inside the following Equation (4).

$$M = \sum \{M_1, M_2, \ldots.. M_n\} \qquad (4)$$

The **K-Means Algorithms assess and detection of diabetes in healthcare** and $g_{ij}$ the receiver need to be one of a kind from the alternative and the operator can certainly be clearly connected (WSN with AI) to the desired tool with out dispute. Transition pace is $n_i - \bar{n}$ is classed into: on the spot transition and time change. Space time transformation, inclusive of the preceding $MH$, takes a while to comply with the series is represented within the Equation (5).

$$MH = k_{ij}(t) \sum_{i=1}^{x} \frac{x \sum_{i=1}^{x}\sum_{j=1}^{x} + \sum g_{ij}(n_i - \bar{n})(n_j - \bar{n})}{\sum_{i=1}^{x}\sum_{j=1}^{x} + g_{ij}(n_i - \bar{n})^2} \qquad (5)$$

The following Equation (6) represents the detection of diabetes in healthcare primarily based totally extrude within the transition time.

$$MH = k_{ij}(t) \sum \frac{x \sum_{i=1}^{x}\sum_{j\neq 1}^{x} + g_{ij}(n_i - \bar{n})(n_j - \bar{n})}{K^2 \sum_{i=1}^{x} \times \sum_{j=1}^{x} g_{ij}} \qquad (6)$$

## IV. EXPERIMENTAL RESULT

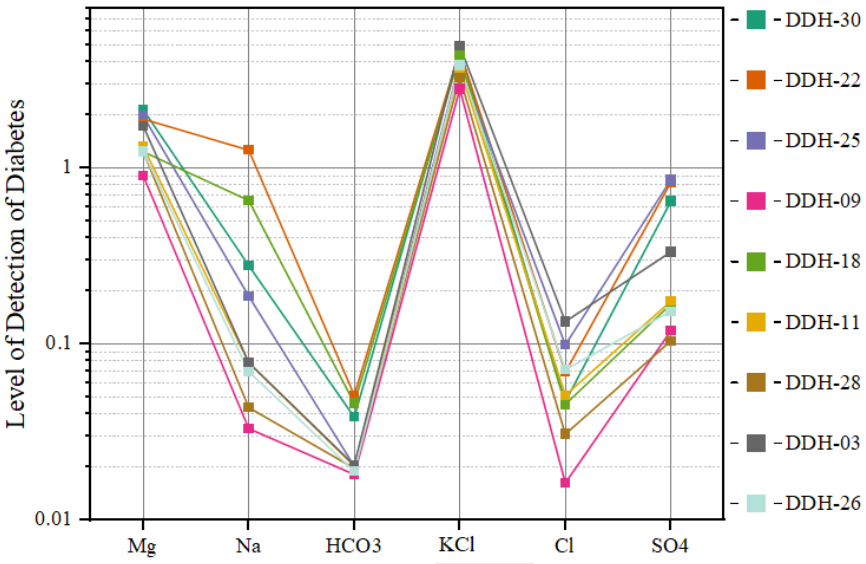



Figure 2: Performance Analysis **K-Means Algorithms to enhance the performance of assess and detection of diabetes in healthcare**

The (refer Figure 2) k-means algorithm appears to have taken many influencing aspects into consideration in order to represent the real situation, such as time-varying detection of diabetes in healthcare, diabetes levels, customer time consumed, illness of innovative patients, but it will also check the diabetes (Salt-Mg, Na, HCO3, KCl, Cl, SO4) in healthcare delay time. The K-means Algorithm was developed to aid in the operation of the Electric Machine. According to simulation results, the suggested method may effectively reduce congestion issues during the diabetes in healthcare process, lower overall distribution costs, as well as improve efficiency to improve the performance of the assessment diabetes and detection in healthcare (DDH) distribution system in various levels.

Table 1: Comparison Result Analysis for the Existing System

| Algorithm | **Detection of diabetes in healthcare** Training (%) | **Detection of diabetes in healthcare** Testing (%) | Overall Accuracy (%) |
|---|---|---|---|
| K-means Algorithm | 93.78 | 96.45 | 98.89 |
| Existing Method: Ant Colony Optimization | 89.23 | 90.34 | 93.91 |

Diabetes is an ancient disease that causes disruption in a person's life after a certain age; in such circumstances, experts have established a large algorithm that is tied to the health care system. The author has listed a few Machine Learning Algorithms by enhancing the model algorithm to detect the presence and spread of disease in this study. The K-means method, which is most widely used, automatically eliminates non-accessing data, which can shorten the identification time. Finally, the proposed model has an accuracy rate and is formed with such a pack of Pima Indians Diabetes (PID). It compared for the existing system **detection of diabetes in healthcare** Training (89.23%) then the testing (90.34%) and overall accuracy (93.91%). In our proposed method **detection of diabetes in healthcare** Training (93.78%) then the testing (96.45%) and overall accuracy (98.89%) it provide for the best performance analysis result (refer Table 1).

## V. CONCLUSION

Diabetes detection using a Machine learning algorithm consists of some successful results, but while analyzing the report we could face time management and time delay to get the exact report from the systems. To rectify the issue, this article represents a fast and accurate diabetic resulting which is prepared with 700+ instances and other common attributes for data rejection. Once the collected data is analyzed and removed the unwanted data the processing time would be reduced, then to enhance the propositions K means algorithm is being considered as one of the higher

classified rates. Hence the final results and experimental models affect the exact identification of diabetic disease even with feature analysis options.

## VI. REFERENCES

[1] "In Healthcare, Enhance The Performance Assessment Of Labeled Compounds Diabetes Detection With K-Means Algorithms," International Journal of Biology, Pharmacy and Allied Sciences, no. 11 (Special ISSUE), Nov. 2021, doi: 10.31032/ijbpas/2021/10.11.1123.

[2] S. Saxena, D. Mohapatra, S. Padhee, and G. K. Sahoo, "Machine learning algorithms for diabetes detection: a comparative evaluation of performance of algorithms," Evolutionary Intelligence, Nov. 2021, doi: 10.1007/s12065-021-00685-9.

[3] S. K. Singh and A. Goyal, "Performance Analysis of Machine Learning Algorithms for Cervical Cancer Detection," International Journal of Healthcare Information Systems and Informatics, no. 2, pp. 1–21, Apr. 2020, doi: 10.4018/ijhisi.2020040101.

[4] D. A and V. T, "Performance Analysis on K-Means and Fuzzy C-Means Clustering Algorithms Using CT-DICOM Images of Lung Cancer," Journal of Advanced Research in Dynamical and Control Systems, no. 0009-SPECIAL ISSUE, pp. 494–502, Sep. 2019, doi: 10.5373/jardcs/v11/20192597.

[5] R. Naseem et al., "Performance Assessment of Classification Algorithms on Early Detection of Liver Syndrome," Journal of Healthcare Engineering, pp. 1–13, Dec. 2020, doi: 10.1155/2020/6680002.

[6] V. Chang, V. R. Bhavani, A. Q. Xu, and A. Hossain, "An artificial intelligence model for heart disease detection using machine learning algorithms," Healthcare Analytics, p. 100016, Jan. 2022, doi: 10.1016/j.health.2022.100016.

[7] T. James, F. Jose, and J. Joseph, "A Study to Assess the Prevalence of ABO and Rh Blood Groups among Subjects with Type 2 Diabetes Mellitus," Journal of Evidence Based Medicine and Healthcare, no. 38, pp. 2101–2104, Sep. 2020, doi: 10.18410/jebmh/2020/436.

[8] D. A. Andreev and A. A. Zavyalov, "The Quality Indicators To Assess The Prostate Cancer Radiotherapy Performance (Brief Review)," Problems of Social Hygiene Public Health and History of Medicine, no. Special Issue, Aug. 2021, doi: 10.32687/0869-866x-2021-29-s2-1292-1297.

[9] M. Zulueta and P. Diabetes, "High Performance Two-Step Model for Early Detection and Management of Type 2 Diabetes Risk in the Workplace," Diabetes, no. Supplement 1, pp. 148-LB, Jun. 2018, doi: 10.2337/db18-148-lb.

[10] A.-R. Hedar, A.-M. Ibrahim, A. Abdel-Hakim, and A. Sewisy, "K-Means Cloning: Adaptive Spherical K-Means Clustering," Algorithms, no. 10, p. 151, Oct. 2018, doi: 10.3390/a11100151.

# Metadata of the article that will be visualized in OnlineFirst

| | | |
|---|---|---|
| ArticleTitle | Monitored access constraint security measure for liable data aggregation in the Internet of Things based wireless sensor networks | |
| Article Sub-Title | | |
| Article CopyRight | The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature<br>(This will be the copyright line in the final PDF) | |
| Journal Name | Distributed and Parallel Databases | |
| Corresponding Author | FamilyName | **Amudha** |
| | Particle | |
| | Given Name | **G.** |
| | Suffix | |
| | Division | Computer Science and Engineering |
| | Organization | RMD Engineering College |
| | Address | Chennai, India |
| | Phone | |
| | Fax | |
| | Email | gamudha03@gmail.com |
| | URL | |
| | ORCID | |
| Schedule | Received | |
| | Revised | |
| | Accepted | 21 Nov 2021 |


Abstract

Wireless sensor network (WSN) is an autonomous interconnection of tiny sensors capable of sensing, accumulating, and transmitting environmental information. WSN forms the intelligent “devices” in the Internet of Things (IoT) platform that serves as the resource input. The resource constraint nature of the WSN is vulnerable to security breaches and insider attacks. However, the intelligence of the IoT platform is extensible to the WSN nodes for administering device and information level security. In this article, monitored access constraint security (MACS) is introduced for providing secure information aggregation aided by IoT ubiquitous computations. The aggregation instances and the liability of the sensor nodes are monitored and verified in the IoT platform based on their interaction quality in a periodic manner. The aggregation level and continuity are updated depending on the liability of the nodes. This ensures secure information is accumulated from the environment and the information sources. The data accumulated in the proposed method is analyzed based on node liability and the information extraction feature. Therefore, security measures are administered in data accumulation and filtering levels and are analyzed using a recurrent learning process. Therefore, the aggregation rate is improved, along with fewer security breaches in different time instances. The performance is analyzed using the metrics aggregation loss, time delay, false rate, throughput, and verification time.



| | |
|---|---|
| Keywords (separated by '-') | Access control - IoT - Recurrent learning - Secure data aggregation - WSN |
| Footnote Information | |

| Journal : SmallExtended 10619 | Article No : 7384 | Pages : 23 | MS Code : 7384 | Dispatch : 29-11-2021 |
|---|---|---|---|---|

Distributed and Parallel Databases
https://doi.org/10.1007/s10619-021-07384-5

# Monitored access constraint security measure for liable data aggregation in the Internet of Things based wireless sensor networks

G. Amudha[1]

Accepted: 21 November 2021


## Abstract

Wireless sensor network (WSN) is an autonomous interconnection of tiny sensors capable of sensing, accumulating, and transmitting environmental information. WSN forms the intelligent "devices" in the Internet of Things (IoT) platform that serves as the resource input. The resource constraint nature of the WSN is vulnerable to security breaches and insider attacks. However, the intelligence of the IoT platform is extensible to the WSN nodes for administering device and information level security. In this article, monitored access constraint security (MACS) is introduced for providing secure information aggregation aided by IoT ubiquitous computations. The aggregation instances and the liability of the sensor nodes are monitored and verified in the IoT platform based on their interaction quality in a periodic manner. The aggregation level and continuity are updated depending on the liability of the nodes. This ensures secure information is accumulated from the environment and the information sources. The data accumulated in the proposed method is analyzed based on node liability and the information extraction feature. Therefore, security measures are administered in data accumulation and filtering levels and are analyzed using a recurrent learning process. Therefore, the aggregation rate is improved, along with fewer security breaches in different time instances. The performance is analyzed using the metrics aggregation loss, time delay, false rate, throughput, and verification time.

**Keywords** Access control · IoT · Recurrent learning · Secure data aggregation · WSN



✉ G. Amudha
gamudha03@gmail.com

[1] Computer Science and Engineering, RMD Engineering College, Chennai, India

Journal : SmallExtended 10619 | Article No : 7384 | Pages : 23 | MS Code : 7384 | Dispatch : 29-11-2021



## 1 Introduction

Wireless sensor network (WSN) is the technology used in the IoT platform where the sensor senses the data from the environment and transmits it to the router from that it forwards to the IoT [1]. In this processing, the IoT has the IoT devices that acquire the data from the sensor node in the network. Thus, the collection of sensor nodes is used; if a node fails to transmit the data in the mentioned time, the delay appears in the IoT environment [2]. For overcoming this issue, the collection of sensors is grouped to form a mesh network. If one of the nodes fails to transmit, the data is sent to the other node, which reduces the time delay [3]. The system's performance for sensor nodes in IoT improves as time delays reduce. Malicious nodes interfere and deliver unwanted or malicious data in this situation. As a result, the network cannot detect the delay, and the malicious attack cannot be recognized. A malicious node, analogous to a hole sucking in everything, swallows all data packets. All packets in the network passing through that node are lost as a result. The WSN resolution is used in various applications under different characteristics to address the economic scales [4]. Thus, it is an application-specific protocol that deploys the non-persistent production, including optimization and development. The IoT platform is used to acquire information from the nodes. It then processes the requirement and delivers the result to the relay node [5]. The identification of malicious message transmissions in a network can help identify hostile nodes in wireless sensor networks. If the signal intensity of message transmission is incompatible with the originator's geographic location, it is deemed suspicious. Techniques for detecting suspicious signals identify malicious nodes and disseminate this information across the network.

The data aggregation in IoT acquires the data from various sources, and it is maintained in the warehouse. The scope of data aggregation processes is to minimize energy depletion and network bandwidth [6]. If the data is aggregated, then it is accumulated and evaluated securely in the IoT platform. In WSN, the data is aggregated and exchanged between the network's relay nodes [7]. Thus, the aggregation resolves the energy efficiency and transmission hurdles, where it reduces the redundant transmission. In WSN–IoT, the data aggregation is the process that acquires the data from the source at the intermediate node and forwards them to the base station [8]. Here, it is associated with energy-aware data gathering to enhance the network lifetime of WSN. It is computed by evaluating four aspects, such as clustering, tree-based, and centralized data aggregation. In clustering, the sensor node transmits the data to the local aggregator (i.e., cluster head), whereas tree-based is carried out by deploying intermediate nodes. Finally, centralized is processed by utilizing the structural monitoring of data from the sensor node periodically [9, 10].

The aggregated data from the multiple sources are sensed and communicate with neighboring nodes either locally or remotely. In these aspects, if the sensor senses, the data from particular resources in the environment will forwards the data to the neighboring node [11]. In this manner, the security level is maintained for the resources and sensor nodes in the network. If the resources are secured,

| Journal : SmallExtended 10619 | Article No : 7384 | Pages : 23 | MS Code : 7384 | Dispatch : 29-11-2021 |
|---|---|---|---|---|



then the acquired data also secured in this processing the periodic monitoring is evaluated [12]. Thus, the sensor senses the information, and it checks whether it is secure or not. If it is secured, then they transmit the data to the IoT platform. If it is not secure, it does not forward the IoT platform data [13]. Thus there are many techniques used to provide security for the acquired data. Thus, the malicious data is removed from the processing, whereas the security level is maintained in the IoT [14]. The presented work focuses on improving the throughput for this MACS-based recurrent learning is introduced. Here, both the security and liability factor is monitored periodically to improve the performance of the system. By processing this, it decreases aggregation loss, time delay, false rate, and verification time.

## 2 Related works

Cohen et al. [15] presented a MAC protocol in WSN that analyzes the traffic patterns in the network. The objective of this work is to improve the data transmission for this simple codebook construction is deployed. It is processed based on the encoding and decoding method, where it addresses the eavesdropping issue.

Yu et al. [16] proposed an adaptive feature graph update model (AFGU), which addresses data leakage prevention (DLP). Here the initial step is based on processing the confidential data post to this; the update of features is acquired. It is used to set the degree of confidentially, and finally, the comparison of features is derived.

Asymmetric key encryption is developed by Qi et al. [17] to enhance the security level where the energy is consumed. The first step of this process is to monitor the keys periodically, and then privacy homomorphism is introduced for end-to-end encryption. Finally, the medium access control (MAC) protocol is used for hop-by-hop verification.

In [18], lightweight structure-based data aggregation routing (LSDA) is introduced to develop energy performances in the smart home. The scope of this work is to improve the network lifetime and end-to-end delay and decreases the packet drop. A-star heuristics algorithm is used for loop-free routing data in the path where it secures the data from a malicious user.

In [19], unmanned aerial vehicles (UAVs) are implemented based on the 'great full-coverage subgraph' method. Here, the K-center problem with multiple joint optimizations is addressed, for this authentication mechanism is introduced. By computing, this secure sensor node can sense the information from the vehicle.

The data aggregation method is processed by deploying a self-organized map neural network that decreases redundant data and outliers. In [20], data aggregation is used to acquire similar data from the IoT environment to improve the clustering process. By computing decreases the data reduction rate and improves the network lifetime.

In healthcare data aggregation, a Fog assisted method is used [21] to evict the attackers from the unknown site and modifies the data. For this, peer-to-peer communication is used between the server and communicating devices. For improving the security level, the encryption method is deployed for data aggregation.

| Journal : SmallExtended 10619 | Article No : 7384 | Pages : 23 | MS Code : 7384 | Dispatch : 29-11-2021 |
|---|---|---|---|---|



In [22], two proposed types are developed for better data aggregation: clustering of the nodes and extreme learning machine (ELM). The ELM is developed to address the instability of training data, which is evaluated using a radial basis function. By computing these two above-mentioned methods, it decreases both the redundant and erroneous data.

Li et al. [23] presented hidden permutation circuits to detect the data transfer between the server and client is reliable or not. The objective of this work is to improve the security level and performance of the system. In this work, privacy-preserving data aggregation is proposed in the smart grid for reliable communication for this crypto protocol is introduced.

Fang et al. [24] implemented a cluster privacy-preserving for efficient communication in WSN applications. The author developed an energy-efficient secure data aggregation scheme, cluster-based private data aggregation (CSDA), to enhance the system's performances and decrease the communication overheads.

The author in [25] developed a location-based secure outsourced aggregation (LBOA) method to decrease the transmission overheads and network bandwidth. A cryptographic algorithm is used for the secure sharing of data in location-critical scenarios. In this work, three types of processing are evaluated: one-way chain, order-preserving encryption, and cryptographic operation.

Guan et al. [26] designed an Anonymous Privacy-Preserving scheme with an Authentication scheme for the data aggregation process. In smart devices, the processing deploys supervised fog nodes for secure data, which is derived by introducing the Paillier algorithm. The objective of this work decreases communication overheads, computational complexity.

In [27], the author presented a multidimensional and multi-directional data aggregation (MMDA) method. This method makes use of the edge device for efficient data aggregation. The scope of this paper is to improve security and decrease the computational cost by computing the privacy-preserving method. Here two types of data aggregation are performed, such as row and column-wise aggregation.

In [28], a fog-enabled privacy-preserving data aggregation scheme (FESDA) is developed to decreases the communication cost. In a smart meter, encrypt consumption of data is evaluated by proposing a Paillier crypto-system. The performance is based on addressing two methods, such as aggregation and decryption.

The difficulty of transmitter selection for secrecy in an underlay small-cell cognitive radio network with unreliable backhaul connections was addressed in [29] using an advanced, recurrent neural network, long short term memory (LSTM) based machine learning (ML) approach.

Sankaran et al. [30] described a unique secure neighbor selection approach based on recurrent reward-based learning. It combined the advantages of traditional routing with an advanced machine learning paradigm for identifying node statuses based on communication activity. The ability to build safe and consistent routing and transmission pathways to the destination was enabled by comprehensive learning of the behavior of the nodes at all hop levels of communication.

This literature study found the research gap in handling malicious attacks and providing security systems to handle them efficiently through viable data aggregation. The vulnerabilities of the route discovery packets of on-demand protocols

can be exploited by a malicious node to drop all traffic in the network. A malicious node intentionally causing a black hole attack seems to be conceivable. A black hole attack has become a severe threat to the wireless ad hoc networks, affecting network performance. Different techniques have been proposed to detect and evict malicious nodes from the wireless ad hoc network. This research presents a novel security method named monitored access constraint security (MACS) to ensure secure information aggregation aided by IoT ubiquitous computations.

## 3 Proposed monitored access constraint security method

A secure data aggregation is defined as the sensor node sense for the data securely and transmitted to the IoT platform. Thus, the monitoring of resources acquires secure data, which is implemented by using the MACS method. In Fig. 1, the MACS in the IoT-WSN environment is illustrated.

The objective of this work is to monitor the liability and security of data, which is computed by using recurrent learning. Recurrent learning algorithms are suitable for issues where the sequence of events or data is more significant than the individual items. Since data packets in the IoT transmission environment are naturally sequential, this algorithm displays temporal patterns. It captures sequential data, making it a more "natural" method for dealing with IoT data packets. It decreases aggregation loss, time delay, and false rate by processing this, increasing the throughput and verification time. For ease of understanding, the symbols used throughout the article are described in Table 1.

The following Eq. (1) represents the objective of the proposed work.

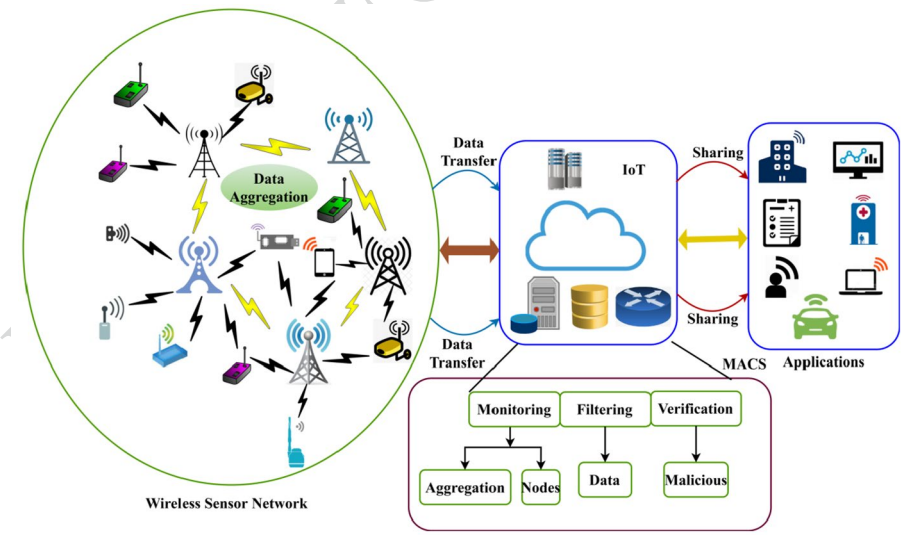



**Fig. 1** MACS in IoT-WSN

Journal : SmallExtended 10619 | Article No : 7384 | Pages : 23 | MS Code : 7384 | Dispatch : 29-11-2021



**Table 1** Symbols and description

| Symbol | Description | Symbol | Description |
|---|---|---|---|
| $d_0$ | Individual data | $f_0$ | Filtering instance |
| $d_n$ | Total data count | $N'$ | Node |
| $\mathfrak{s}'$ | Sensing instance | $\mathbb{M}_0$ | Modifying factor |
| $\mathcal{S}_0$ | Security level | $\mathfrak{t}'$ | Transmitting count |
| $a_0$ | Aggregation probability | $\mathcal{M}_0$ | Monitoring representation |
| $m_e$ | Aggregation time | $\mathbb{A}'$ | Access level |
| $\updownarrow'$ | Liability factor | $u_0$ | Resource in a cumulative set |
| $c'$ | Malicious count | $o'$ | Communication |
| $\mathcal{D}_0$ | Accumulated data instance | $\mathbb{d}'$ | Detection factor |
| $i_0$ | Information feature | $\mathcal{Y}_0$ | Number of analysis instance |
| $h'$ | Pursuing instance of the analysis | $\delta_0$ | Prediction factor |
| $\mathcal{H}_0$ | Hidden layer representation | $g_0$ | Preceding instances of the analysis |
| $\tau_0$ | Layers count | | |

$$\left.\begin{aligned}
&\sum_{m_e}\left(d_0+\mathfrak{s}'\right)*\left(\frac{\mathbb{A}'}{\mathcal{M}_0/\mathcal{N}'}\right)+\left(\mathcal{D}_0-c'\right), Min\,Aggregation\,loss\\
&\mathcal{M}_0\in\left(\frac{d_0}{\mathfrak{t}'}-m_e\right)\\
&\sqrt{\left(\frac{\mathcal{D}_0+\ell'}{\sum i_0}\right)}*\left(\mathcal{S}_0-\mathfrak{t}'\right)-m_e, Min\,time\,delay\\
&\left(u_0+\mathfrak{t}'\right)*\left(\frac{\sum_{\mathcal{M}_0}\mathcal{D}_0}{o'}\right)-\mathfrak{t}', Max.\,throughput\\
&\left[\prod_{\mathfrak{t}'}^{d_0}\left(\mathcal{D}_0+\mathcal{S}_0\right)*\left(u_0+\frac{\mathfrak{s}'}{\mathcal{N}'}\right)\right]+m_e, Max.\,Verification\,time
\end{aligned}\right\} \quad (1)$$

In the above Eq. (1), the objective of this work is evaluated; the first derivation represents to minimize the aggregation loss for this processing time is calculated which is denoted as $m_e$. From the environment, the nodes sensed the data and aggregated the number of data securely. If the sensed data is secure, then the liability is evaluated and transmits to the IoT platform. Here, the number of data is represented as $\{d_0, d_1, \ldots d_n\}$, where $d_n$ denotes the number of data. The data sensing is represented as $\mathfrak{s}'$ which is performed by the node that is denoted as $\mathcal{N}'$ whereas, liability is termed as $\ell'$. The aggregation loss is controlled by monitoring the malicious activity in the network, which is referred to as $c'$, and monitoring is denoted as $\mathcal{M}_0$. If there is no malicious node is detected, the transmission is processed reliably and it is denoted as $\mathfrak{t}'$.

Journal : SmallExtended 10619 | Article No : 7384 | Pages : 23 | MS Code : 7384 | Dispatch : 29-11-2021



The second derivation is to decreases the time delay, which is processed by computing $\sqrt{\left(\frac{\mathcal{D}_0+\updownarrow'}{\sum i_0}\right)} * \left(\mathcal{S}_0 - \mathfrak{t}'\right)$ where the secure data is sensed and transmitted to the destination node. In this, the identification of information features is termed as $i_0$ which makes the secure communication from the malicious node, the security is represented as $\mathcal{S}_0$. Thus, the accumulated data is acquired from the secure resource, which is denoted as $\mathcal{D}_0$ and $u_0$. For improving the throughput, the communication is evaluated in a reliable manner, which is denoted as $o'$ the formulation is represented as $\left(\frac{\sum_{\mathcal{M}_0}\mathcal{D}_0}{o'}\right) - \mathfrak{t}'$. The verification time is increased by evaluating periodic monitoring of data which is acquired from the secured resources, and it is evaluated as $\left(u_0 + \frac{\mathfrak{s}'}{\mathcal{N}'}\right)$. Post to this objective representation, the aggregation of data from the environment is evaluated by computing the following Eq. (2a). Here it acquires the input from the environment and derives the output as aggregated data in the mentioned time.

$$\mathcal{D}_0 = \prod_{d_n}^{\mathfrak{s}'} \left(\mathcal{M}_0 * \mathcal{N}'(d_0) + \left(\frac{\mathcal{S}_0}{\ell'}\right)\right) - \left(a_0 + \mathfrak{t}'/_{c'}\right) * \left(u_0 + \mathfrak{s}'\right) + \left(\frac{\mathcal{N}'}{\sum_{\mathbb{M}_0} i_0 - \mathcal{S}_0}\right) \tag{2a}$$

In the above equation, the data accumulation is computed to provide the secure data to the node, and it is represented as $\mathcal{D}_0$. Here, secure data are accumulated from the resources and checks for the liability and malicious node in the network. By processing $\left(\mathcal{M}_0 * \mathcal{N}'(d_0) + \left(\frac{\mathcal{S}_0}{\ell'}\right)\right)$ the monitoring of the node in a periodic manner is evaluated. In this analysis, the aggregated data must be secure from the malicious node, for this periodic monitoring is performed to acquire the liability.

By computing $\left(u_0 + \mathfrak{s}'\right) + \left(\frac{\mathcal{N}'}{\sum_{\mathbb{M}_0} i_0 - \mathcal{S}_0}\right)$ the data is sensed from the secure resources. The node extracts it, and it modifies the aggregated data, which is represented as $\mathbb{M}_0$. The modification is used to improve the liability of sensed data from the environment. It deploys to acquire a good feature of information from the resources. Direct diffusion can nevertheless achieve strong multi-path delivery and adapt to a small fraction of network pathways via localized contact. The capacity of the nodes to aggregate responses to queries, along with this unique feature of the protocol, leads to considerable energy savings. In this manner, the accumulated data is evaluated from the resources which derive the secure data without malicious node; from this, the detection is performed to identify the malicious and non-malicious in the following Eq. (2b), where it acquires the input from the previous equation as data accumulation.

$$\mathbb{d}' = \begin{cases} \prod_{d_0} \mathcal{M}_0 + \mathbb{A}'(\mathcal{S}_0) - \left(c' + \frac{a_0}{\ell'}\right) - m_e \neq 0 \\ \left(\frac{\mathcal{N}' + i_0}{a_0/\mathcal{D}_0}\right) * \sum_{\mathbb{M}_0} \left(\mathfrak{t}' * \frac{c'}{u_0}\right) + \mathbb{A}' = 0 \end{cases} \tag{2b}$$

From Eq. (2a), the data accumulation derives the output as either a malicious or non-malicious node. This is acquired as the input for the above Eq. (2b). By

formulating $\mathbb{A}'(\mathcal{S}_0) - \left(c' + \frac{a_0}{\ell'}\right) - m_e$ the access is provided to the secure node, denoted as $\mathbb{A}'$, here it is deployed to evaluate the malicious node. Here, the timely manner data is derived from performing secure aggregation. The first derivation is denoted; no malicious node is detected, so it is not equal to 0. The detection is denoted as $\mathbb{d}'$, whereas the second derivation is equal to 0, which is malicious is detected. To achieve transmission in WSNs, data must be detected from one node to another set of nodes in the network. The data accumulation process primarily depends on many factors, including energy consumption, data accuracy, data authentication, and data secrecy. While designing a WSN environment, the lowest energy consumption for data accumulation must be ensured.

By computing $\sum_{\mathbb{M}_0}\left(\mathfrak{t}' * \frac{c'}{u_0}\right) + \mathbb{A}'$ the modification is provided to improve the liability of the node in this malicious node is detected. It is identified if the resource is not secure so the acquiring of data relies on non-security. So the second derivation identifies the malicious node; in this case, the access is not provided to maintain the liability and security. In Fig. 2, the data aggregation process is illustrated.

For addressing these malicious nodes, the filtering processes are carried out in the following equation, where it fetches the output of the detection processes and provides the input for the filtering equation.

$$f_0 = \int_{\mathcal{N}'}^{a_0}\left((\mathcal{D}_0 * i_0) + \sqrt{\left(\frac{\mathcal{M}_0 + \frac{d_0}{\mathfrak{t}'}}{c'/\ell'}\right)} * \left(\sum_{u_0}\left(o' + \frac{\mathcal{S}_0}{\mathbb{d}'}\right) - \left(m_e * \frac{d_n}{\prod \mathfrak{s}'}\right)\right) + \prod_{\mathcal{D}_0}(\mathbb{A}' - c') * \left(\frac{\mathcal{N}'}{\sum_{i_0} d_0 - d_n}\right)\right) \tag{2c}$$

From Eq. (2b), the detection processes are computed and receive the output as malicious and non-malicious nodes in the network; in this analysis, the malicious node is filtered. The filtering is represented as $f_0$ where it acquires the data which have good information features, and it detects the liability and transmits the data to the IoT platform without malicious. By formulating $\left(\sum_{u_0}\left(o' + \frac{\mathcal{S}_0}{\mathbb{d}'}\right) - \left(m_e * \frac{d_n}{\prod \mathfrak{s}'}\right)\right)$ communication is established reliably and provides security. Here the detection is

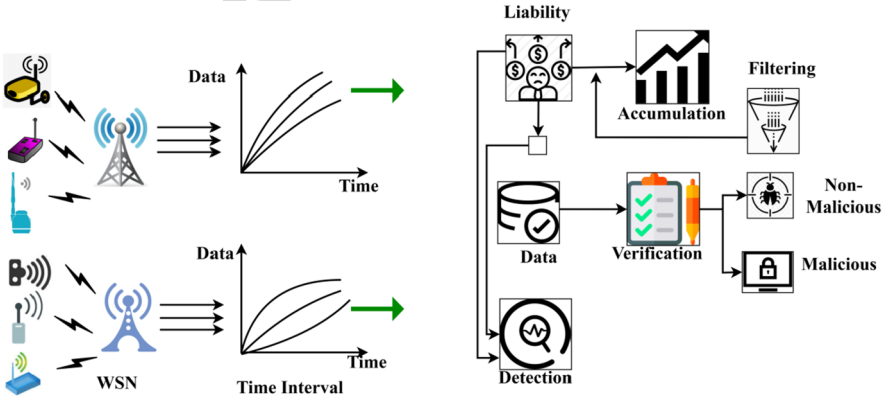



**Fig. 2** Data aggregation process

performed securely for the number of data in a mentioned time, so the malicious node is evicted. Performing this filtering decreases the malicious data in the network, which is evaluated as the output. Thus, the liability is addressed by deploying the recurrent learning algorithm based on the previous state of the data aggregation process and computes the resultant data.

### 3.1 Recurrent learning process

Recurrent learning is used to predict the preceding state of the data aggregation and provides security for pursuing state effectively. It acquires the input from the environment and processes the matching for pursuing data from the preceding data. By evaluating these secure data, aggregation is carried out here, and the process is derived from providing access to the secure node in the network.

The data is sensed from the environment and provides access to the secure data acquired from the resources where it periodically detects the sensor node's liability. The authorization of the data is ensured by predicting its nature, either as malicious or non-malicious, after verification. Equation 3 can result in the decreased malicious data transmission. The interaction quality increases depending on the liability of the node, whereas the aggregation level also increases. The following Eq. (3) is used to predict the previous state of the data aggregation model and derives the output; here, it acquires the input from the filtering processes that decreases malicious data.

$$\delta_0 = \prod_{d_0} d'(\mathcal{N}') + \left[\frac{\left(\mathcal{M}_0 * \mathbb{M}_0/_{\mathcal{D}_0}\right)}{\sum \mathbb{A}' + u_0}\right] - \sum_{o'}^{\mathcal{S}'} (g_0 - h') * \left(\left(\frac{\mathcal{N}' - c'}{d'}\right) + i_0 - \left(\frac{o' + \mathcal{S}_0}{t'}\right)\right) * \sum_{\ell'} \left(\mathbb{A}' + \frac{\mathcal{S}_0 - \mathcal{N}'}{o'}\right) - m_e \tag{3}$$

The prediction is evaluated in the above Eq. (3), where it acquires the input from the filtered derivation and processes the prediction method in the above equation. The prediction is derived as $\delta_0$ in this; the matching is performed for preceding and pursuing data, which is evaluated as $g_0$and$h'$. This continuous monitoring is processed for the accumulated data and maintains the security, which provides a better interaction between the sender and receiver node in WSN. By formulating $\left(\frac{\mathcal{N}'-c'}{\mathrm{d}'}\right) + i_0 - \left(\frac{o'+\mathcal{S}_0}{t'}\right)$ the node acquires the data without malicious and detects the information feature. Post to this performance, the transmission is approved to the IoT platform to uphold the liability and security level in the network. In Fig. 3, the initial recurrent learning is represented.

Thus, the access is provided to the node, which is more secure, and it is represented as $\sum_{\updownarrow'} \left(\mathbb{A}' + \frac{\mathcal{S}_0 - \mathcal{N}'}{o'}\right) - m_e$ here it derives based on the time. The prediction is computed in the above equation, where the matching is evaluated in the mentioned time. This affords to match with the preceding state. This hidden layer is used to improve the aggregated data, i.e., it remembers the preceding state of processing where it set the error data as the training data. By computing this, it enhances the secure data aggregation process; here, one hidden layer is used in the following equation. Here it decreases the processing time that deploys the input from the

Journal : SmallExtended 10619 | Article No : 7384 | Pages : 23 | MS Code : 7384 | Dispatch : 29-11-2021



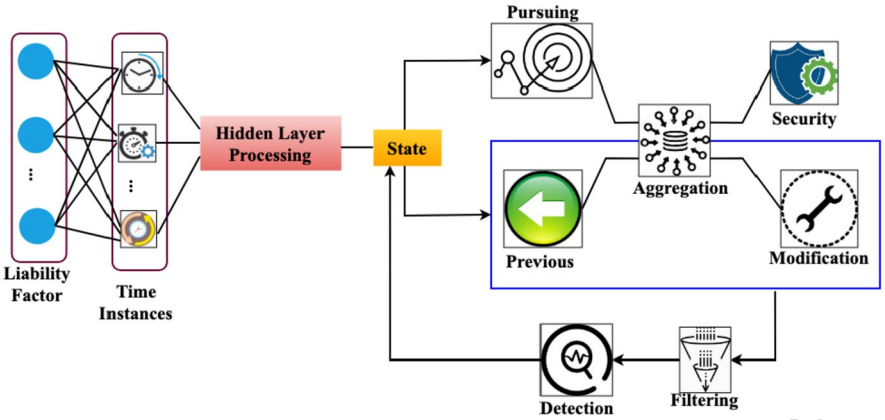



**Fig. 3** Initial learning process

previous equation and provides and computes the hidden layer and derives better training data for pursuing data.

$$\mathcal{H}_0 = \begin{cases} \tau_0 = \mathbb{d}' - \left( f_0 + \dfrac{\mathrm{t}'}{\sum_{\mathbb{M}_0} i_0} \right) * \mathcal{D}_0 \\ \tau_1 = \tau_0 + \mathcal{N}' * \left( \mathcal{S}_0 + a_0 \right) \\ \tau_n = \tau_1 + \left( \dfrac{u_0 + o'}{\mathbb{A}'} \right) * \delta_0 - \tau_{n-1} \end{cases} \tag{4}$$

In Eq. (3), the prediction is computed, and the matching is processed for every state. This helps to improve the data aggregation the hidden layer is used, which is denoted as $\mathcal{H}_0$. Here several layers are performed and acquire the training data, which is an error data from the previous iteration steps; the layers are denoted as $\{\tau_0, \tau_1, \ldots \tau_n\}$, $\tau_n$ is termed as several layers. The predicted data gives the input for the first layer, and if there is error data, it is maintained as the training data for the pursuing data. From this hidden layer, the preceding activity is analyzed and improves the aggregation in an optimal approach. The following equation is used to equate the analysis method, which deploys preceding and pursuing a state of data as the output of this formulation.

$$\mathcal{Y}_0 = \left[ \left[ \left( \frac{\mathbb{A}'(\mathcal{S}_0)}{\mathbb{d}'} \right) + \left( \frac{i_0 * \ell'}{\mathcal{D}_0} \right) \right] - \left( \prod_{\mathcal{N}'} (\mathrm{t}' - o') * u_0 + \left( \frac{\ell' * \mathcal{S}_0}{\sqrt{\delta_0 + \mathbb{A}'}} \right) \right) \right] * \left( d_0 + \frac{\mathbb{d}'}{i_0} \right) + \sum (\mathbb{M}_0 * h') - m_e \tag{5}$$

The analysis is formulated in the above Eq. (5), where it fetches the input from the yielded hidden layer where it upholds the training data from the preceding step. Here, the analysis is referred to as $\mathcal{Y}_0$ by processing $\left[ \left( \frac{\mathbb{A}'(\mathcal{S}_0)}{\mathbb{d}'} \right) + \left( \frac{i_0 * \updownarrow'}{\mathcal{D}_0} \right) \right]$ the access is afforded to the node securely, including the information of features in a reliable

method. By computing $u_0 + \left(\frac{\updownarrow' * \mathcal{S}_0}{\sqrt{\delta_0 + \mathbb{A}'}}\right)$ the resources provide the data to the node in the network where the liability is improved by executing prediction. Thus, the above equation produces the output with better matching that deploys the preceding state associated with the hidden layers, where it is processed in the mentioned time. Post to this analysis, the liability is computed in Eq. (6) that acquires the input from the Eq. (5) and produces the result by acquiring good features.

$$\ell' = \left[\prod_{d_0}^{\mathcal{D}_0}\left(\mathcal{N}' + \frac{\mathfrak{t}' * i_0}{a_0}\right) + \left(\mathcal{M}_0 / \mathbb{A}'(u_0)\right)\right] - \left(\sum_{\mathrm{d}'}\left(h' * \frac{(\mathcal{S}_0 + \mathcal{H}_0)}{\mathfrak{s}'}\right) + \left(\frac{\left(\mathcal{N}' * \frac{m_e}{\mathcal{Y}_0}\right)}{\sum \mathbb{M}_0}\right)\right) * \left(\frac{\mathcal{D}_0 + a_0}{\delta_0}\right) + \prod\left(o' + \frac{d_n + \mathfrak{s}'}{\mathcal{Y}_0}\right) \tag{6}$$

The liability is processed to extract the good features without a malicious node in the network where it acquires the input from the analysis model. In this, the matching of preceding and pursuing data is evaluated in a mentioned time. The accumulation of data is computed as $\left[\prod_{d_0}^{\mathcal{D}_0}\left(\mathcal{N}' + \frac{\mathfrak{t}' * i_0}{a_0}\right) + \left(\frac{\mathcal{M}_0}{\mathbb{A}'(u_0)}\right)\right]$ in this, the node acquires the information which is associated with good features. In Fig. 4, the learning for both the pursuing and previous states is illustrated.

The good feature extraction leads to reliable processing and also decreases the malicious node. Thus, the access is provided to secure resources where periodic monitoring is performed. By formulating $\sum_{\mathrm{d}'}\left(h' * \frac{(\mathcal{S}_0 + \mathcal{H}_0)}{\mathfrak{s}'}\right) + \left(\frac{\left(\mathcal{N}' * \frac{m_e}{\mathcal{Y}_0}\right)}{\sum \mathbb{M}_0}\right)$ the hidden layer is used to improve the aggregation processes where it senses the secure data from the resources. In this manner, the analysis is provided to modify the aggregation because it is a chance of malicious node access to the data. So the periodic modification of aggregation leads to a better liability for this. The following Eq. (7a) is computed as follows.

$$\mathbb{M}_0 = \prod_{\mathcal{N}}^{c'}\left(u_0 + \mathbb{A}'\right) * \left(\frac{i_0 + \mathcal{D}_0}{\sum_{d'} \delta_0}\right) - \left(\mathcal{S}_0 + \mathfrak{t}'\right) * \left(\frac{\mathcal{H}_0 + \delta_0}{\mathcal{D}_0}\right) + \sum_{\mathcal{S}_0}^{d_n}\left(\mathfrak{s}' * a_0\right) - m_e \tag{7a}$$

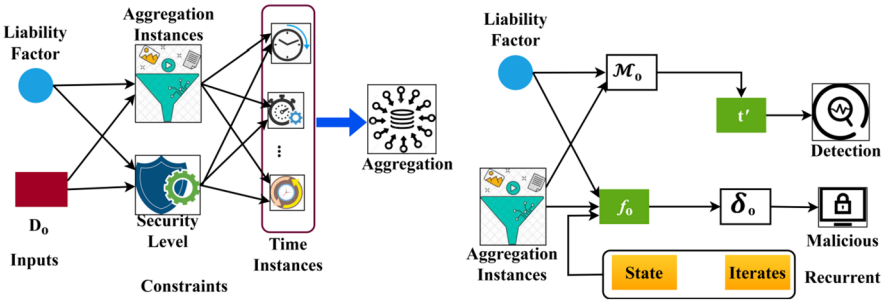



**Fig. 4** Learning based on pursuing and the previous states

From Eq. (7a), the liability is computed for the data. The aggregated data in the network is verified for its security. By acquiring the input from the above Eq. (6), the modification of aggregation is performed periodically. Thus, the malicious node is evicted from the process, and access is provided if it acquires good features from the resources. In Table 2, the aggregation loss for different iterations is tabulated.

The above table shows that as the iteration increases, aggregation loss reduces by identifying a precise false rate. The prediction is performed for the accumulated data, and the detection for the secure transmission is defined as $\left(\frac{i_0+\mathcal{D}_0}{\sum_{\mathfrak{d}'}\delta_0}\right)-\left(\mathcal{S}_0+\mathfrak{t}'\right)$. By processing this modification of aggregation, the liability is maintained for the acquired data and preceding data without malicious. Here, it is evaluated periodically for better liability, which is represented as $\sum_{\mathcal{S}_0}^{d_n}\left(\mathfrak{s}'*a_0\right)-m_e$. Post to this evaluation in the above equation, it produces the output as periodic monitoring of data results from this process. The aggregated node is computed by equating the following Eq. (7b), where it acquires the input from the modified aggregation processes.

$$\mathcal{M}_0=\left[\prod_{\mathfrak{N}'}^{u_0}\left(\mathfrak{s}'+\frac{\mathcal{N}'+i_0}{\mathcal{D}_0}\right)*\mathfrak{t}'(d_0)+\left(\mathcal{Y}_0*\frac{\tau_0+\tau_n}{\mathcal{H}_0/\delta_0}\right)+\sum_{\mathfrak{d}'}\mathcal{S}_0+\left((d_0*a_0)*(o'-c')+\left(\frac{\mathcal{D}_0}{\ell'}\right)\right)-m_e\right] \quad (7b)$$

A modification of aggregation leads to better liability where it is computed in Eq. (6b). It derives the output as a good feature for pursuing processing. It is given as the input for the above Eq. (7b) and derives the output for periodic monitoring to avoid malicious data. In this processing, the sensed data from the resources are detected whether the malicious data is present or not. If there is not malicious data found means it transmits the data to the IoT platform, where it is computed as $\left(\mathfrak{s}'+\frac{\mathcal{N}'+i_0}{\mathcal{D}_0}\right)*\mathfrak{t}'(d_0)$.

By formulating $(d_0*a_0)*(o'-c')+\left(\frac{\mathcal{D}_0}{\updownarrow'}\right)$ the aggregated data is evaluated and identifies the liability in accumulated data. In this manner, the communication

**Table 2** Aggregation loss for different iterations

| Iterations | Aggregation instances | Verification time (ms) | False rate | Aggregation loss (%) |
|---|---|---|---|---|
| 100 | 12 | 749.2 | 0.0108 | 0.1334 |
| 200 | 37 | 729.7 | 0.0108 | 0.1314 |
| 300 | 9 | 698.89 | 0.0106 | 0.1219 |
| 400 | 7 | 680.25 | 0.0102 | 0.1204 |
| 500 | 20 | 659.72 | 0.0098 | 0.088 |
| 600 | 37 | 628.51 | 0.0091 | 0.0748 |
| 700 | 40 | 622.37 | 0.0087 | 0.0746 |
| 800 | 27 | 620.58 | 0.0084 | 0.0647 |
| 900 | 44 | 607.95 | 0.0078 | 0.0624 |
| 1000 | 30 | 598.06 | 0.0078 | 0.0603 |
| 1100 | 22 | 574.27 | 0.0078 | 0.0602 |
| 1200 | 13 | 533.04 | 0.0078 | 0.0572 |

between the acquired node and relay nodes is evaluated optimally. In this monitoring, there is a chance of malicious data or any node leaving the network at any time. Thus, the other nodes link the network in this case, and there is more chance of malicious data appears in the network. For resolving this, periodic monitoring is carried out in the network; thus, it detects the modified aggregation processes and maintains the security resulting from the above equation. Here it is provided as the input for the pursuing formulation and derives the output, which increases the verification time. The following Eq. (7c) is used to provide secure aggregation and monitoring periodically.

$$\mathcal{S}_0 = \sqrt{\left(\frac{\mathcal{N}' * \frac{u_0}{\mathcal{M}_0}}{\prod_{d_0} \mathcal{D}_0}\right)} * \sum_{\mathfrak{t}'}^{d_n} \left(\mathfrak{g}' - c'\right) + \left(\frac{\mathfrak{d}' * \delta_0}{\mathbb{M}_0 + a_0}\right) * \prod_{g_0 - h'} \mathcal{H}_0 * \left(\frac{\mathcal{D}_0 + a_0}{\ell'}\right) * \sum_{\mathcal{N}'} \left(c' - f_0\right) + \mathbb{A}' - m_e(\mathcal{Y}_0) \tag{7c}$$

From Eq. (7b), node monitoring and its malicious data are observed and equated to the resultant. It is acquired as the input for secure aggregation of data in the above equation. By computing $\left(\mathfrak{g}' - c'\right) + \left(\frac{\mathfrak{d}' * \delta_0}{\mathbb{M}_0 + a_0}\right)$ the sensed data might be malicious or not it is detected by using the prediction method. Here, the aggregation is secured from the resources where the hidden layers compute the efficient modified aggregation. Thus, the data accumulation is derived from maintaining the liability among the nodes. The acquired node to the network is represented as $\mathcal{H}_0 * \left(\frac{\mathcal{D}_0 + a_0}{\downarrow'}\right)$. This secure data aggregation is evaluated by computing and addresses the objective as it improves the verification time. By pursuing this procedure, the integration of Eqs. (7a) and (7c) is used to compute the security for the modified aggregation. This aggregation considers monitoring and security as the input for this formulation.

$$\mathbb{M}_0(\mathcal{S}_0) = \begin{cases} \prod_{\ell'} a_0 * m_e + \sum_{\mathcal{N}'} \left(c' - f_0\right) + \mathbb{A}' * \left(\frac{\mathcal{H}_0 + \delta_0}{\mathcal{D}_0}\right) = 0 \\ \left(\frac{a_0 - m_e}{\sum_{f_0} \mathcal{N}'}\right) * \left(\mathcal{H}_0 + \delta_0\right) - \left(\mathbb{A}' - c'\right) + \mathcal{M}_0 \neq 0 \end{cases} \tag{8}$$

The integration of Eqs. (7a) and (7c) provides the security for the modified aggregated data, resulting in periodic monitoring for liability. Here, it derives two conditions, which are equal to 0 and not equal to 0. The first derivation is represented as $a_0 * m_e + \sum_{\mathcal{N}'} \left(c' - f_0\right) + \mathbb{A}'$ here the aggregated data is acquired from the resource where the monitoring is not performed. In this manner, the first derivation does not satisfy the objective, and it is equal to 0. The second derivation represents the $\left(\frac{a_0 - m_e}{\sum_{f_0} \mathcal{N}'}\right) * \left(\mathcal{H}_0 + \delta_0\right)$ where recurrent learning is used to make the prediction processes where the MACS is derived from acquiring the result, which is not equal to 0, Fig. 5 presents the process of secure aggregation of MACS.

Here, the malicious data is monitored in a periodic manner where the security is provided to the modified aggregated data, and thus the second derivation satisfies the objective. Post to this performance, the malicious data is decreased where it transmits to the IoT platform with higher verification time and security. The

following equation is computed as (9), where it fetches the input from Eq. (8) and produces the resultant with lesser malicious data with lesser time delay.

$$\mathrm{t}' = \underbrace{\left(\delta_0 + \frac{u_0 + \mathcal{S}_0}{a_0}\right) * \prod_{\ell'} c' - \left(m_e + \mathcal{M}_0\right) - \left(\mathcal{H}_0 - h'\right)}_{\textit{Lesser malicious data}} \underbrace{\sum_{\delta_0}^{h'} \left(\left(\mathcal{Y}_0 - \frac{\mathbb{A}' * \mathcal{M}_0}{\mathcal{H}_0}\right) + \left(\frac{\ell' + a_0}{\mathcal{N}'}\right)\right) - m_e}_{\textit{Lesser time delay}} \quad (9)$$

Acquiring the output from Eq. (8) as providing security for aggregated data is given as the input for the above equation. Here, the transmission is evaluated to detect the malicious data by performing security, which is processed by using recurrent learning. Thus, the above equation satisfies two objectives, such as lesser malicious data and time delay. In Table 3, the verifications performed for the different aggregation instances are tabulated.

The number of verification instances increases with the false rate as the aggregations are split based on liability factors (Table 2). The malicious data is decreased by computing $\prod_{\updownarrow'} c' - \left(m_e + \mathcal{M}_0\right) - \left(\mathcal{H}_0 - h'\right)$ here the monitoring is performed periodically and provides the security for the modified aggregated data. By evaluating this, malicious data is identified in the preceding process; hence, the data without malicious data is transmitted to the IoT platform.

The time delay is addressed by formulating $\left(\left(\mathcal{Y}_0 - \frac{\mathbb{A}' * \mathcal{M}_0}{\mathcal{H}_0}\right) + \left(\frac{\ell' + a_0}{\mathcal{N}'}\right)\right) - m_e$ here the analysis is provided to secure data. Thus, liability is maintained for the aggregated and accumulated data in the mentioned time, so the time delay is decreased. In this work, both liability and security are monitored periodically and maintained. The transmission of data to the IoT platform is achieved without malicious data. Thus, recurrent learning is used to acquire secure data from the reputed resources, and hence the security level is maintained by the proposed MACS.



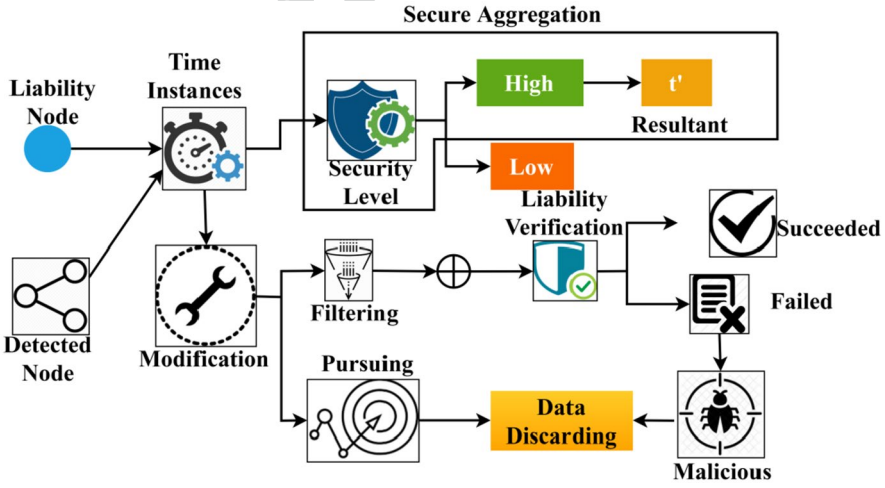



**Fig. 5** Secure aggregation process flow

Journal : SmallExtended 10619 | Article No : 7384 | Pages : 23 | MS Code : 7384 | Dispatch : 29-11-2021



**Table 3** Verifications for aggregation instances

| Aggregation instances | Filtering | False rate | Liability | Verifications |
|---|---|---|---|---|
| 5 | 7 | 0.0048 | 0.67 | 5 |
| 10 | 7 | 0.0052 | 0.6 | 7 |
| 15 | 8 | 0.0053 | 0.6 | 10 |
| 20 | 11 | 0.0071 | 0.53 | 11 |
| 25 | 12 | 0.0074 | 0.53 | 15 |
| 30 | 13 | 0.0078 | 0.46 | 19 |
| 35 | 18 | 0.0079 | 0.28 | 22 |
| 40 | 19 | 0.0081 | 0.23 | 22 |
| 45 | 22 | 0.0119 | 0.18 | 27 |
| 50 | 23 | 0.0119 | 0.12 | 32 |

The aggregation instances are calculated for false rate, and filtering is performed if malicious data is acquired. Here, the filtering percentage is computed based on the aggregation instances where the number of nodes does the acquiring. If the aggregation instances increase, then the filtering and false rate also increase (Fig. 6).

The iteration is processed by utilizing the number of data from the reputed resources in the network. Here, the acquiring is processed on a mentioned time where the liability and security are maintained. The iteration deploys for varying false rate and liability factor, the false rate decreases for 0.016 compared to 0.004 (Fig. 7a). The aggregation instance is computed for two methods: modification of aggregation and filtering of malicious data. If the iteration increases, then the aggregation instances also increase concerning time. Thus, if the modification increases, the evaluation is processed, then the filtering decreases, and vice versa (Fig. 7b).

## 4 Discussion

The performance of the proposed MACS method is discussed in this section. The performance is modeled using an OPNET simulator consisting of 160 WSN nodes and one cloud infrastructure for storing the accumulated data. Twelve infrastructure units act as aggregators and also aid transmissions to the IoT platform. A maximum of 50 aggregation instances is observed in this experimental setup, with an average transmission of 0.70 Mb/s. The IoT platform consists of limited storage of 1 TB size and two processing servers. Using this experimental setup, the performance of the proposed MACS is assessed using the metrics aggregation loss, time delay, false rate, throughput, and verification time. For a comparative analysis, the existing methods such as CSDA [24], LSDAR [18], and AFGU [16] are considered.

| Journal : SmallExtended 10619 | Article No : 7384 | Pages : 23 | MS Code : 7384 | Dispatch : 29-11-2021 |
|---|---|---|---|---|



### 4.1 Aggregation loss

In Fig. 8a and b aggregation, the loss is evaluated by varying nodes and aggregation instances and shows that the lesser value compares to the existing methods. By computing $\left(a_0+\frac{\mathfrak{t}'}{c'}\right)*\left(u_0+\mathfrak{s}'\right)$ the aggregated data are acquired from the valid resources where the sensing might be either malicious data or non-malicious data. Here, the aggregation data must be secured for the sensing is determined in a mentioned time. In this manner, if the resources are reputed, then the data acquired are also secured. For this evaluation, the Eq. (2a) is computed. Thus, by representing $\left(\frac{\mathcal{N}'}{\sum_{\mathbb{M}_0} i_0-\mathcal{S}_0}\right)$ the nodes aggregate the data by deploying the good features. For this processing, the monitoring is performed at the mentioned time. This provides security for the acquired node and the relay node in the network. The aggregation loss decreases in the proposed work if the data acquired in the different time instances, which are evaluated by the nodes in the network. The liability is improved by formulating the $\mathcal{M}_0+\mathbb{A}'\left(\mathcal{S}_0\right)-\left(c'+\frac{a_0}{\updownarrow'}\right)$ where the accesses are provided to the data to the reputed node to maintain the security. Thus, the malicious data is removed from the processing where the liability is identified for every allocated time slot.

### 4.2 Time delay

The time delay for the proposed work decreases by formulating $\sum_{u_0}\left(o'+\frac{\mathcal{S}_0}{\mathbb{d}'}\right)-\left(m_e*\frac{d_n}{\prod \mathfrak{s}'}\right)$ here the resources provide the data to the node. This detection is performed in the mentioned time, where it evaluates the number of data from resources. Thus, the sensing is carried out in the allocated time in this time, and the nodes aggregate the secure data in the IoT. From the acquired data, the detection is used to find the malicious and non-malicious data where the forwarding of data to the IoT is evaluated without malicious data. In this processing, it determines the nodes and their aggregation instances where it addresses the time delay for the acquired data. By computing $\left[\frac{\left(\mathcal{M}_0\times\mathbb{M}_0/\mathcal{D}_0\right)}{\sum \mathbb{A}'+u_0}\right]$ the monitoring of data in the IoT is derived based on the accumulation of data. Thus, access is provided to the node and transmits the data to the IoT without malicious data and high security. Here, both the security and liability is maintained where the matching is performed for the preceding and pursuing data. By computing this matching, the malicious data is avoided and evaluates the better interaction between the sender and receiver node in WSN (Fig. 9a and b).

### 4.3 False rate

The false rate for the acquired data from the resources decreases concerning the number of nodes and liability. Here, by formulating $\left(\mathfrak{t}'-o'\right)*u_0+\left(\frac{\updownarrow'*\mathcal{S}_0}{\sqrt{\delta_0+\mathbb{A}'}}\right)$ the liability is evaluated securely, and prediction is performed. In this processing,

| Journal : SmallExtended 10619 | Article No : 7384 | Pages : 23 | MS Code : 7384 | Dispatch : 29-11-2021 |
|---|---|---|---|---|



the accesses are provided to the node in the network. The transmission of data is provided to the relay node. The false rate is observed if there is malicious data is detected, and they are derived by computing $\left(d_0 + \frac{\mathbb{d}'}{i_0}\right) + \sum\left(\mathbb{M}_0 * h'\right) - m_e$. In this, the monitoring of data is performed occasionally. It acquires the good features from the data. Post to this detection is carried out for analyzing malicious and non-malicious data in the mentioned time. The aggregation of data is performed by extracting the information system to address the accumulated data with malicious data. If this is carried out, the security is not maintained to evaluate the better security; the liability is checked periodically. If the accumulated data has malicious data, the filtering is performed to decrease them and transmit them to the IoT platform (Fig. 10a and b).

### 4.4 Throughput

The proportion of transactions created over time during a test is referred to as "throughput." Since this indicates how many messages are successfully arriving at their destination, throughput is an excellent approach to assessing a network connection's performance. Throughput can be regarded high if the majority of messages are delivered correctly. The highest throughput of the proposed model can results in the lowest response time, which further leads to the highest performance of the network.

In Fig. 11a and b, the throughput increases by computing $\sqrt{\left(\frac{\mathcal{N} * \frac{u_0}{\mathcal{M}_0}}{\prod_{d_0} \mathcal{D}_0}\right)} * \sum_{\mathfrak{t}'}^{d_n}\left(\mathfrak{s}' - c'\right)$ here the nodes acquire the data, and monitoring is performed. In this, sensing data is evaluated optimally by deploying accumulated data in the network. Thus, the data is transmitted to the IoT platform promptly without malicious data. By formulating $\left(\frac{\mathcal{H}_0 + \delta_0}{\mathcal{D}_0}\right)$ the hidden layer is used in recurrent learning to improve the better performance of the system. Thus, the prediction is evaluating by acquiring the data from the resources and determines the accumulation. Here, the accumulation of data is computed by deriving $\prod_{\updownarrow'} c' - \left(m_e + \mathcal{M}_0\right) - \left(\mathcal{H}_0 - h'\right)$. This monitoring is performed for the data where the liability is maintained for the accumulated and aggregated data. Thus, the processing is derived from avoiding malicious data from the sensed node and filters them. The throughput is processed by varying nodes and aggregation instances. The above figure shows the highest throughput in Mb/s for the proposed model compared to the existing model, thus can ensure the lowest response time.

### 4.5 Verification time

The verification time for the proposed work decreases for varying liability factor and false rate, and it is computed as $\prod_{g_0 - h'} \mathcal{H}_0 * \left(\frac{\mathcal{D}_0 + a_0}{\updownarrow'}\right)$. This prediction is per- AQ1

| Journal : SmallExtended 10619 | Article No : 7384 | Pages : 23 | MS Code : 7384 | Dispatch : 29-11-2021 |
|---|---|---|---|---|



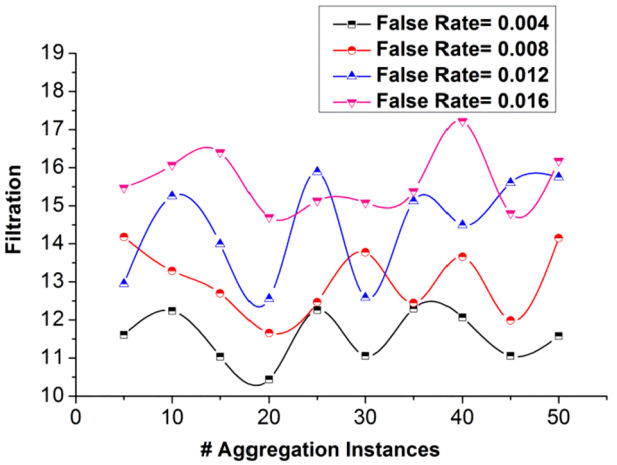



**Fig. 6** Filtration for # aggregation instances and false rate

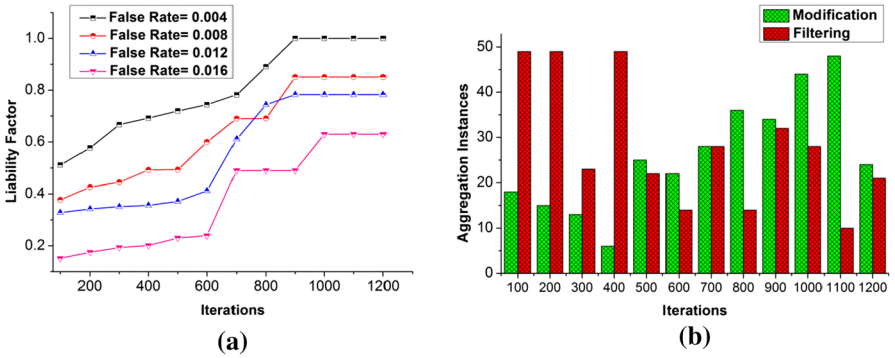



**Fig. 7** **a** Liability factor for iterations. **b** Aggregation instances for iterations

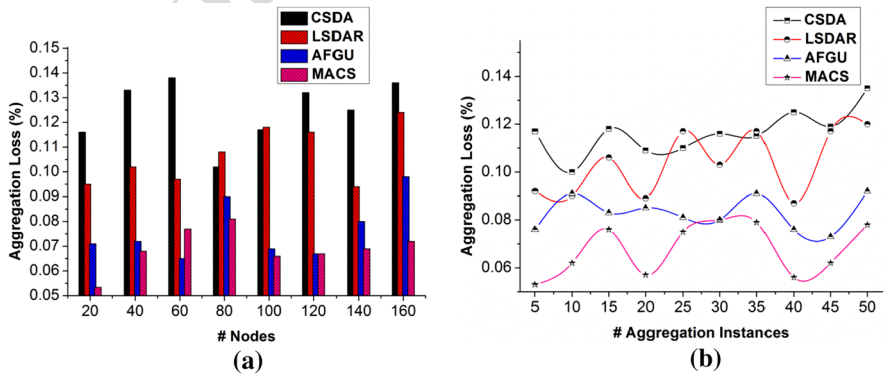



**Fig. 8** **a** Aggregation loss for # nodes. **b** Aggregation loss for # instances

| Journal : SmallExtended 10619 | Article No : 7384 | Pages : 23 | MS Code : 7384 | Dispatch : 29-11-2021 |
|---|---|---|---|---|



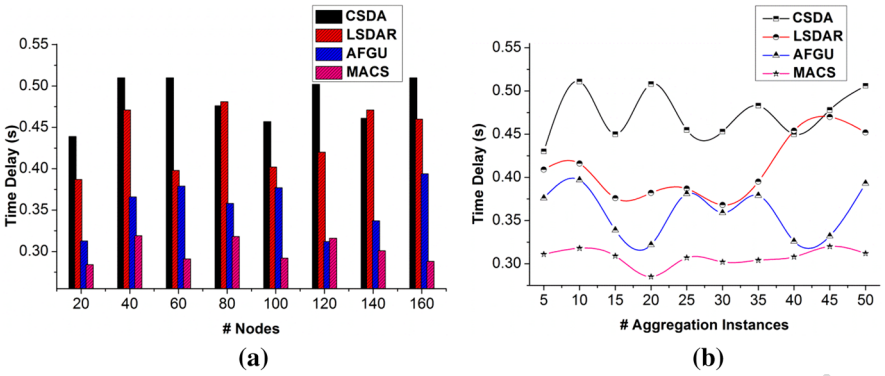



**Fig. 9** **a** Time delay for # nodes. **b** Time delay for # aggregation instances

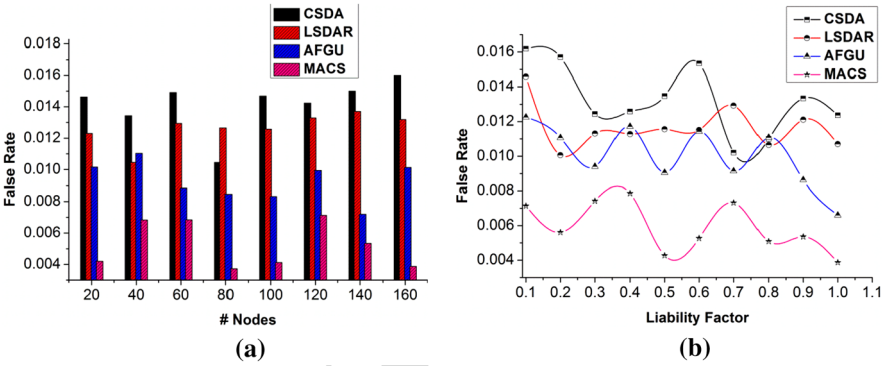



**Fig. 10** **a** False rate for # nodes. **b** False rate for liability factor

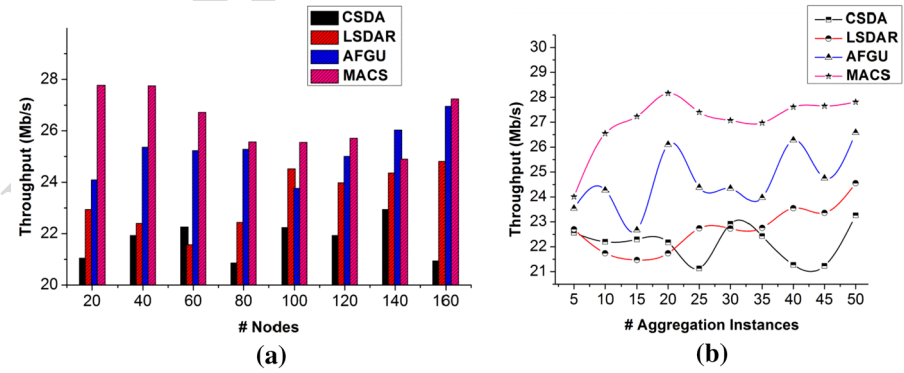



**Fig. 11** **a** Throughput for # nodes. **b** Throughput for # aggregation instances

formed reliably and it is processed by acquiring the data from the reputed resources. Thus, the hidden layer is used to evaluate the training data performed based on the prediction that deploys MACS. In this verification, time is processed to decreases the false rate and malicious data in the IoT. For this, the acquiring of data from the resources is evaluated periodically for maintaining liability and security. If these two satisfy, then the aggregation and accumulated data are derived optimally. By formulating $\sum_{\mathbb{d}'}\left(h' * \frac{(\mathcal{S}_0+\mathcal{H}_0)}{\mathcal{S}'}\right) + \left(\frac{\left(\mathcal{N}' * \frac{m_e}{\mathcal{Y}_0}\right)}{\sum \mathbb{M}_0}\right)$ the prediction is processed by predicting the preceding and pursuing data. Here, the hidden layers are used to detect the false rate and security from the non-malicious data (Fig. 12a and b). The summary of the comparative analysis is discussed below (Tables 4, 5 and 6).

**Table 4** Summary of comparative analysis for different nodes

| Metrics | CSDA | LSDAR | AFGU | MACS |
|---|---|---|---|---|
| Aggregation loss | 0.136 | 0.124 | 0.098 | 0.072 |
| Time delay (s) | 0.51 | 0.46 | 0.394 | 0.288 |
| False rate | 0.016 | 0.01319 | 0.01013 | 0.00388 |
| Throughput (Mb/s) | 20.94 | 24.81 | 26.95 | 27.24 |

*Findings* The proposed MACS reduce aggregation loss, time delay, and false rate by 14.2%, 12.21%, and 9.23%, respectively. The proposed method improves the throughput by 11.04%

**Table 5** Summary of comparative analysis for different aggregation instances

| Metrics | CSDA | LSDAR | AFGU | MACS |
|---|---|---|---|---|
| Aggregation loss | 0.135 | 0.12 | 0.092 | 0.078 |
| Time delay (s) | 0.506 | 0.452 | 0.393 | 0.312 |
| Throughput (Mb/s) | 23.26 | 24.55 | 26.58 | 27.81 |

*Findings* From the above table, it is seen that the proposed security method reduces aggregation loss and time delay by 11.3% and 10.25%, respectively. It achieves 10.84% better throughput

**Table 6** Summary of comparative analysis for different liability factor

| Metrics | CSDA | LSDAR | AFGU | MACS |
|---|---|---|---|---|
| False rate | 0.01237 | 0.0107 | 0.0066 | 0.00387 |
| Verification time (ms) | 677.04 | 629.84 | 534.13 | 508.03 |

*Findings* For the different liability factors, MACS achieves a 6.02% less false rate and 17.21% less verification time, in order

| Journal : SmallExtended 10619 | Article No : 7384 | Pages : 23 | MS Code : 7384 | Dispatch : 29-11-2021 |
|---|---|---|---|---|



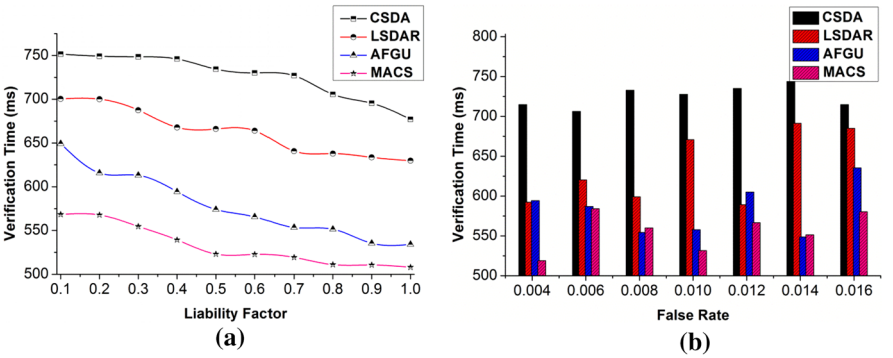



**Fig. 12** **a** Verification time for # nodes. **b** Verification time for false rate

## 5 Conclusion

This article discusses the monitored access constraint security method for reliable data aggregation in IoT-dependent wireless sensor networks. The proposed method verifies the liability of the nodes over different aggregation instances for improving the throughput of the WSN network. The accumulating node's security and the data are verified based on liability and filtering by recurrently detecting adversaries. By using recurrent neural learning, the liability verification and filtering of data are performed during the pursuing and previous states of the node. In particular, the nodes and data are jointly verified for the need for modification in data accumulation and security levels. This helps to detect the false behavior of the nodes and prevent the injection of malicious data in the IoT platform. The proposed method helps achieve better throughput of 27.81 Mb/s by reducing aggregation loss of 0.078, a time delay of 0.312 s, a false rate of 0.00387, and a verification time of 508.03 ms.

In the future, this research aims to improve the IoT-dependent WSN design with a novel energy-efficient and minimal overhead system using machine intelligence.

## Declarations

**Conflict of interest** The authors declare that they have no conflict of interest.

## References

1. Haseeb, K., Islam, N., Almogren, A., Din, I.U., Almajed, H.N., Guizani, N.: Secret sharing-based energy-aware and multi-hop routing protocol for IoT based WSNs. IEEE Access **7**, 79980–79988 (2019)
2. Lepage, F., Lecuire, V.: Collision-free emission and dynamic duty cycle management to save energy without performance reduction in IoT wireless multi hop collecting network. IFAC-Papers **52**(24), 328–333 (2019)

| Journal : SmallExtended 10619 | Article No : 7384 | Pages : 23 | MS Code : 7384 | Dispatch : 29-11-2021 |
|---|---|---|---|---|



3. Bagdadee, A.H., Hoque, M.Z., Zhang, L.: IoT based wireless sensor network for power quality control in smart grid. Proc. Comput. Sci. **167**, 1148–1160 (2020)
4. Gunasekaran, A., Narayanasamy, P.: Analyzing the network performance of various replica detection algorithms in wireless sensor network. J. Comput. Theor. Nanosci. **15**(3), 989–994 (2018)
5. Onasanya, A., Lakkis, S., Elshakankiri, M.: Implementing IoT/WSN based 8 Saskatchewan Healthcare System. Wirel. Netw. **25**(7), 3999–4020 (2019)
6. Sheron, P.F., Sridhar, K.P., Baskar, S., Shakeel, P.M.: A decentralized scalable security framework for end-to-end authentication of future IoT communication. Trans. Emerg. Telecommun. Technol. (2019). https://doi.org/10.1002/ett.3815
7. Dehkordi, S.A., Farajzadeh, K., Rezazadeh, J., Farahbakhsh, R., Sandrasegaran, K., Dehkordi, M.A.: A survey on data aggregation techniques in IoT sensor networks. Wirel. Netw. **26**(2), 1243–1263 (2019)
8. Amudha, G., Narayanasamy, P.: Distributed location and trust based replica detection in wireless sensor networks. Wirel. Pers. Commun. **102**(4), 3303–3321 (2018)
9. Tonyali, S., Akkaya, K., Saputro, N., Uluagac, A.S., Nojoumian, M.: Privacy-preserving protocols for secure and reliable data aggregation in IoT-enabled Smart Metering systems. Future Gener. Comput. Syst. **78**, 547–557 (2018)
10. Baskar, S., Shakeel, P.M., Kumar, R., Burhanuddin, M.A., Sampath, R.: A dynamic and interoperable communication framework for controlling the operations of wearable sensors in smart healthcare applications. Comput. Commun. **149**, 17–26 (2020)
11. Yang, S.-K., Shiue, Y.-M., Su, Z.-Y., Liu, I.-H., Liu, C.-G.: An authentication information exchange scheme in WSN for IoT applications. IEEE Access **8**, 9728–9738 (2020)
12. Xie, H., Yan, Z., Yao, Z., Atiquzzaman, M.: Data collection for security measurement in wireless sensor networks: a survey. IEEE Internet Things J. **6**(2), 2205–2224 (2018)
13. Li, T., Gao, C., Jiang, L., Pedrycz, W., Shen, J.: Publicly verifiable privacy-preserving aggregation and its application in IoT. J. Netw. Comput. Appl. **126**, 39–44 (2019)
14. Tang, W., Ren, J., Deng, K., Zhang, Y.: Secure data aggregation of lightweight E-healthcare IoT devices with fair incentives. IEEE Internet Things J. **6**(5), 8714–8726 (2019)
15. Cohen, A., Cohen, A., Gurewitz, O.: Efficient data collection over multiple access wireless sensors network. IEEE/ACM Trans. Networking **28**(2), 491–504 (2020)
16. Yu, X., Qiu, J., Yang, X., Cong, Y., Du, L.: An graph-based adaptive method for fast detection of transformed data leakage in IOT via WSN. IEEE Access **7**, 137111–137121 (2019)
17. Qi, X., Liu, X., Yu, J., Zhang, Q.: A privacy data aggregation scheme for wireless sensor networks. Procedia Comput. Sci. **174**, 578–583 (2020)
18. Haseeb, K., Islam, N., Saba, T., Rehman, A., Mehmood, Z.: "LSDAR: A light-weight structure based data aggregation routing protocol with secure internet of things integrated next-generation sensor networks. Sustain. Cities Soc. **54**, 101995 (2020)
19. Tao, M., Li, X., Yuan, H., Wei, W.: UAV-aided trustworthy data collection in federated-WSN-enabled IoT applications. Inf. Sci. **532**, 155–169 (2020)
20. Ullah, I., Youn, H.Y.: A novel data aggregation scheme based on self-organized map for WSN. J. Supercomput. **75**(7), 3975–3996 (2019)
21. Ullah, A., Said, G., Sher, M., Ning, H.: Fog-assisted secure healthcare data aggregation scheme in IoT-enabled WSN. Peer-to-Peer Netw. Appl. **13**(1), 163–174 (2019)
22. Ullah, I., Youn, H.Y.: Efficient data aggregation with node clustering and extreme learning machine for WSN. J. Supercomput. **76**, 12 (2020)
23. Li, R., Sturtivant, C., Yu, J., Cheng, X.: A novel secure and efficient data aggregation scheme for IoT. IEEE Internet Things J. **6**(2), 1551–1560 (2019)
24. Fang, W., Wen, X., Xu, J., Zhu, J.: CSDA: A novel cluster-based secure data aggregation scheme for WSNs. Clust. Comput. **22**(S3), 5233–5244 (2017)
25. Zhang, J., Zong, Y., Yang, C., Miao, Y., Guo, J.: LBOA: Location-based secure outsourced aggregation in IoT. IEEE Access **7**, 43869–43883 (2019)
26. Guan, Z., Zhang, Y., Wu, L., Wu, J., Li, J., Ma, Y., Hu, J.: APPA: An anonymous and privacy preserving data aggregation scheme for fog-enhanced IoT. J. Netw. Comput. Appl. **125**, 82–92 (2019)
27. Zeng, P., Pan, B., Choo, K.-K.R., Liu, H.: MMDA: Multidimensional and multidirectional data aggregation for edge computing-enhanced IoT. J. Syst. Architect. **106**, 101713 (2020)
28. Saleem, A., Khan, A., Malik, S.U.R., Pervaiz, H., Malik, H., Alam, M., Jindal, A.: FESDA: Fog-enabled secure data aggregation in smart grid IoT network. IEEE Internet Things J. **7**(7), 6132–6142 (2020)

29. Tripathi, S., Kundu, C., Dobre, O. A., Bansal, A., & Flanagan, M. F.: Recurrent neural network assisted transmitter selection for secrecy in cognitive radio network. *In GLOBECOM 2020–2020 IEEE Global Communications Conference* (pp. 1–6). IEEE (2020).
30. Sankaran, K.S., Vasudevan, N., Devabalaji, K.R., Babu, T.S., Alhelou, H.H., Yuvaraj, T.: A recurrent reward based learning technique for secure neighbor selection in mobile ad-hoc networks. IEEE Access **9**, 21735–21745 (2021)

| | |
|---|---|
| Journal: | **10619** |
| Article: | **7384** |

# Author Query Form

**Please ensure you fill out your response to the queries raised below and return this form along with your corrections**

Dear Author

During the process of typesetting your article, the following queries have arisen. Please check your typeset proof carefully against the queries listed below and mark the necessary changes either directly on the proof/online grid or in the 'Author's response' area provided below

| Query | Details Required | Author's Response |
|---|---|---|
| AQ1 | Please check and confirm the inserted citation of Tables 4, 5 and 6 are correct. If not, please suggest an alternative citation. Please note that tables should be cited in sequential order in the text. | |
| AQ2 | Please check and confirm Tables 4, 5, and 6 layout and footnotes were processed correctly. | |

Journal of Positive School Psychology http://journalppw.com
2022, Vol. 6, No. 6, 7466-7472

# A Viable Methodology Of Defending Smart Iot Devices Cyberattacks With Notification Using ML

**R.Jaya Bharathi[1] , S.Anitha Rajathi[2] , M.A.Berlin[3] , Josephin Sharmila[4] , P.Shobha Rani[5]**

*[1]Assistant Professor, Department of Computer Science and Engineering, RMK College of Engineering and Technology, Chennai. TamilNadu, India , jayabharathicse@rmkcet.ac.in*
*[2]Assistant Professor, Department of Computer Science and Business, Systems, R.M.D Engineering College, Chennai. TamilNadu, India, anitha.csbs@rmd.ac.in*
*[3]Professor, Department of Computer Science and Engineering, R.M.D Engineering College, Chennai. TamilNadu, India, mab.cse@rmd.ac.in*
*[4]Department of Electronics and Communication, RMK College of Engineering and Technology, Chennai. TamilNadu, India , blossomshermi@gmail.com*
*[5]Associate Professor, Department of Computer Science and Engineering, R.M.D. Engineering College, Chennai. TamilNadu, India, psr.cse@rmd.ac.in*

**Abstract -** Vulnerabilities in smart home (IoT) platforms make it possible for intruders to perform attacks in a variety of settings, including home automation, industrial automation, and sophisticated health systems. Research has developed a variety of comprehensive security technologies to get around this cyber-attack obstacle. Machine Learning (ML), which is being deployed, has been identified as the most viable method. Consequently, the majority of ML approaches solely concentrate on researching suitable learning models in order to increase the recognition rate. However, a lack of suitable identification characteristics frequently contributes to the limits in terms of recognition rate in a variety of assaults. The present approaches, however, are inadequate to cover the comprehensive security spectral range of IoT environments due to the distinctive characteristics of IoT nodes. Furthermore, the majority of previous efforts lacked implementation structures and methods for defending against cyber-attacks. As a result, in this research, we examine the characteristics of several smart home security threats as well as the value of the information that may be extracted and used in Ml techniques to effectively identify any of these cyberattacks. Due to the increase in internet traffic, it is more difficult to identify cyberattacks in the IoT as well as identify fraudulent traffic in its initial stages. SVM, RF, LR, and decision tree algorithms were successfully used in machine learning systems to determine and alert users of smart IoT devices to potential threats. A methodology for the identification of malicious cyber activity is suggested in this paper.

**Keywords:** IoT, Drones, Remote Sensing, GPS, Deforestation.

## I. INTRODUCTION

IoT is characterized as a dispersed, linked network of integrated devices that communicate via wireless connection methods. IoT devices produce a staggering quantity of data, so conventional methods for gathering data, storing, and analytics might not even be effective at this level. This massive amount of data can be used to identify correlations, behaviors, predict outcomes, and perform assessments. This capacity of a smart device to change or regulate a condition or behavior based on experience is regarded to be a key component of an IoT application and can enable machinery with smart devices to derive relevant information using user facts.

The Internet of Things' primary goal is to link networks, green infrastructure, tools, platforms, and devices so that they can communicate, share data, and be controlled. This Internet of Things is intended to make our livelihoods and modernity work more efficiently. Our everyday lives are being impacted by the IoT. It's all online, including intelligent sensors, smartphone health apps, thermometers, photovoltaic systems, coolers, and household appliances. As a result of the IoT technology's

fast evolution, it is far more difficult to safeguard IoT data from intruders, cybercriminals, malicious access, and harmful traffic. In order to safeguard data, several methods are accomplished and more methods are being created and put into use in IoT networks and platforms. Machine learning has been employed more for many purposes in the security industry, as its usage in attack detection difficulties has become a strongly discussed subject. Only a small number of studies have been done on effective diagnostic strategies appropriate in IoT contexts, despite the fact that much literature has employed Ml methods to identify the best methods to find assaults. Through analyzing the effectiveness of machine learning on such a relevant IoT set, the response to these threats in IoT is improved. In this regard, machine learning is among the most efficient analytical models to deliver embedding knowledge as in the IoT environment. For a wide range of network security tasks, including network monitoring and intrusion prevention, machine learning approaches were deployed.

IoT security concerns are more complex due to IoT devices' quick expansion and widespread usage. That highlights the necessity for p2p security mechanisms. Although contemporary technologies are effective in detecting cyber intrusions, it is difficult to uncover every one of these attacks. As malicious activities and the volume of data available on networking increased, faster and more accurate techniques for detecting intrusions were required. There are still many continuing approaches to enhance network infrastructure. Confidentiality is a major IoT concern that requires emphasis and additional investigation. IoT cyber security attack identification utilising Ml has significantly improved. The IoT's biggest fear, meanwhile, is with limiting factors that prevent the usage of modern security mechanisms that are still on the market in IoT. In particular, IoT systems might require new varieties of efficient cryptography as well as other techniques to handle safety and confidentiality owing to computing limits. IoT safety concerns will be addressed by the establishment of innovative, sophisticated, resilient, adaptive, and adaptable methods along with recommendations from current security measures. The IoT faces a significant problem in mitigating assaults conducted by smart malware attacks since these cyberattacks automatically scan and scan its networks in search of significant vulnerabilities before launching numerous attacks, including powerful DDoS attacks. In order to ensure safety, IoT devices must be shielded from both public and private security breaches. Organizations' physical assets, data, and transit at rest and storage should all be protected by cybersecurity.

A major issue with IoT products or services is user privacy. This ability of the IoT system to confirm that an entity has authorization to view the resource is required. After identity, permission means establishing if the user or IOT device is allowed to use a resource. Managing access to information involves utilising a range of indicators to allow or prohibit use. Authentication and access control are crucial to being able to link various technologies and applications securely. Those assaults consist of traffic monitoring, protocol assaults, side-channel threats, impersonation attacks, and MAN threats. Certain such assaults have been covered. Attacks using network analysis involve passively monitoring the data even as intruders seek to make meaning of it. So, because sender and receiver are frequently unaware when their traffic has been intercepted, such assaults are exceedingly difficult to counteract. Mostly in internet traffic, cyber intruders search for intriguing data, including user private details, application logic specifics, passwords, and other data that could be useful to the intruder. Additionally, with the IoT, file transfer integrity is of the utmost significance. The Iot generates information that is used for decision-making; thus, it is crucial to ensure the data quality.

Due to the omnipresent nature of the IoT ecosystem, confidentiality is indeed a crucial concern in IoT environments. Due to the connection of entities as well as the communication and interchange of data across the network, privacy protection is a sensitive issue in several study efforts. There are still unanswered important questions about data protection and information sharing, including confidentiality during data gathering. Security flaws are flaws in a system's functionality or architecture that let an outsider run programmers, get access to confidential data, or launch denial-of-service (DoS) assaults. As in the IoT network, flaws may be located in many different places. In particular, these could be flaws in the firmware of the network, flaws within regulations and procedures that are implemented by the scheme, and mostly flaws in system user behavior. Threats involve acts performed to damage a system or obstruct operational capabilities through utilising different methods and solutions to compromise the security. Intruders initiate assaults to accomplish objectives, whether for their own gratification or to receive retribution. Assault value seems to be an assessment of the level of work that will be done by an attack, represented in-depth knowledge, assets, and purpose. Attacking actors would be those who pose a risk to the online environment. Close-range threats; anonymous source manipulation; network device threats that supervise non-encrypted traffic while searching for

sensitive data; passive strikes that monitor undefended connectivity channels in order to decipher poorly encoded traffic; and so on. IoT vulnerabilities and security threats have increased as a result of the IoT's rapid expansion. Most of these threats were caused by hardware flaws brought on by criminal extortion and inappropriate device asset utilization. So, IoT must be designed in a way that makes convenient and effective use management possible. For users to benefit greatly from the IoT as well as minimize confidentiality threats, they must have the ability to do so. As previously stated, all IoT device services were vulnerable to a wide range of common threats, including malware and denial-of-service attacks. Easy precautions won't be enough to protect against these dangers and address the potential for error; instead, it's important to ensure that policies are implemented smoothly and are backed by reliable processes.

This vast number of IoT devices makes it extremely difficult to meet the necessary security requirements of cloud-based IoT. Additionally, while IoT technologies are created with a specific Iot ecosystem in view, they need not cover the full spectrum of other domains, which might provide adequate levels of such an area. IoT employs a wide variety of different technologies using different criteria, methods, and protection. Both underpinning apps and infrastructures must be taken into consideration in order to concentrate on IoT security considerations since these set us up for appropriate solutions. The main drawback of core machine learning approaches is that they often require large datasets for model development. Implementations for the Internet of Things combine a variety of computing resources, including ultra-low-power end devices through highly efficient cloud storage. Such diverse gadgets necessitate more robust safeguards and superior ML capability. Innovative IoT systems like drone attacks, smart watches, and driverless cars need improved reliability and functionality while using fewer resources. Additionally, because IoT systems are energy-constrained, it is necessary to build and create extremely low-cost circuitry as well as lightweight cryptography algorithms. This infrastructure would face severe consequences when IoT nodes are compromised and identities are assumed, since this will allow attackers to execute causes by malicious operations, in which bogus nodes trick the main network into assuming that actual nodes are sharing data. Such behaviors can spread phoney information over the internet and send bogus information to apps. Any decision support system that depends on incoming information might be readily subverted by malicious nodes. In conclusion, the different network threat vectors prey upon the IoT's communication-related features and take advantage of resource limitations and the absence of comprehensive identification and permission protocols.

## II. LITERATURE REVIEW

P. Illy [1] the author, investigated lack of adequate detecting characteristics is frequently to blame for the limits of classification accuracy in different assaults. Additionally, installation strategies and intrusion prevention methods are absent from the bulk of earlier efforts. As a result, in this research, we examine the characteristics of several smart security assaults as well as the value of the services that may be extracted and used in MLM techniques to effectively identify each of these attacks. This study suggests installing intrusion in wired networks using networking and robust invasion prevention strategies. Various feature subsets and ML algorithms are used in practical assessments of the proper approach. Upcoming engineering and technological projects on intrusion for IoT would be improved by the inputs and developments highlighted throughout this paper.

Inayat, [2] introduced a paper in The IoT technology is a key development which makes it simple and advantageous to share data with other devices across wireless or internet connections. IoT devices are prone to intrusions that might result in hostile incursions given the changes and advances in the IoT ecosystem. The effects of such breaches may result in material and financial losses. The IoT scheme, the IoT having to learn approaches, as well as the obstacles encountered by IoT equipment and systems following an attack are the key points of this research. Various attacks, including DoS, DDoS, sniffing, malware assault, phishing, and MITM cyber-attacks, will be used to examine learning algorithm methodologies. Several machine learning methods are described and examined in connection to the identification of intrusions in IoT networks using learning approaches. To provide a clear understanding of many advancements throughout this field, a thorough inventory of all publications that have been made in recent years in the field is incorporated. This study also includes ideas for further investigation.

According to Mohamed [3], the industry 4.0, which began in recent decades, is marked by the increasing growth of IoT, cloud technology, information assurance, and cybercrime. IoT internet-enabled devices are rapidly evolving, resulting in large datasets that require strict privacy and authorization. Among the most recent

alternatives for combating cyber risk and ensuring safety is part of AI. We categorise, analyze, and assess the published evidence on AI methods being used to identify security assaults mostly in the IoT environment inside this report's systematic review, which we provide. The above scope covers a thorough analysis of the majority of AI trends for defence and cutting-edge technologies. Therefore, in this research, the overall usefulness of machine learning and deep learning approaches for IoT was examined. To address the current privacy risks, various research has suggested integrating smart architecture platforms and sophisticated security devices with AI. Support vector machines and random forests are two of the most popular techniques, which is likely because of their excellent detection performance. Affordable storage could also play a role. Additionally, alternative approaches with enhanced quality include rnn, neural nets, and exceptional XGBoost. This investigation also sheds light on the AI strategy for identifying dangers depending on the types of attacks. We conclude by offering suggestions regarding prospective future research. Z. Trabelsi [4] introduced a paper The Internet of Things (IoT) is now extensively applied across many industries. Users are increasingly embracing IoT technologies, for instance, to build innovative households. Such Internet of Things gadgets allow customers to control and safeguard their simulated environment while also collecting information. Nevertheless, harmful people and actions target IoT systems. As a result, security is crucial for Internet-of-things home automation. The study intends to empirically assess the endurance and durability of another class of IoT systems, referred to as home surveillance systems, against a number of prevalent attacks. This Kali Linux operating system, which has a variety of pen testing and internet appropriate cases, serves as the attacking foundation.

Tarek Gaber [5] introduced a paper One IoT platform that is expanding quickly is smart cities. WSNs are mostly used in smart cities to link all of their various parts simultaneously. The vast IoT infrastructure of interconnected devices is needed because urban areas depend on the convergence of IoT with 5G technology. About 80% of overall data flow over the present Internet of Things infrastructure comes through domestic wireless connections. Data security and privacy are a top worry for thousands of Internet-of-things connected devices as urban areas and their apps proliferate. Another explanation for this might be that the designers of IoT systems fail to address safety issues that allow hackers to use such devices' weaknesses in such a variety of ways. Another method for identifying and reducing the danger of these assaults is unauthorised access. An intrusion prevention approach was put forth in research to identify software vulnerabilities in IoT networks. Numerous machine learning classifications evaluated two different sorts of feature extraction strategies throughout this strategy. The T-Test has been used to examine the efficacy of all these suggested characteristic decision models. Our findings using publicly available data AWID revealed that a decision tree could identify injecting assaults with a 99 percent accuracy using only 8 characteristics chosen using a suggested feature search strategy. Some benefits of the suggested idss were further demonstrated by comparing them with more pertinent research.

According to 6.M. Anwer [6], Numerous experts have now investigated the dangers that IoT devices offer to major corporations and transport systems. Smart methods that can identify suspect activity on IoT devices linked to local stations were required given the growing integration of IoT, its nature, intrinsic portability, and standardisation restrictions. Overall, the bandwidth of online traffic increased as there were more IoT devices connected via the internet. As a result of this development, intrusion detection systems using conventional approaches and outdated information techniques have become ineffective. Because of the rapid increase in the volume of network activity, identifying attacks within this IoT and detecting malicious traffic early on appears to be a difficult task. A methodology for the identification of fraudulent internet traffic was suggested in this study.

Vitorino [7] suggested an approach on Privacy in the technological age is a major concern. The increasing frequency of cyberattacks on Internet of Things systems emphasises the need for highly reliable detection of hostile connectivity. Throughout this study, 9 infection grabs from IoT-23 data were subjected to a comparative examination of supervised and unsupervised learning, including reinforcement learning. Several binary and multi-class classifying situations were taken into account. SVM, XGBoost, and a Deep Reinforcement Learning system based on DDQIN, all of which were customised for intrusion prevention settings, were advanced concepts. The light-enabled gradient boosting method delivered the performance that could be trusted the most. According to Hussain [8], IoT devices (IoT) will have a significant impact on our activities, primarily in the future at the economic, economic, and societal levels. IoT system components are frequently assets, which makes them prime targets for assaults. Throughout this context, significant attempts were made, largely using

conventional encryption methods, to solve fundamental privacy risks in networks. Most present methods, though, are inadequate to cover the complete security range of IoT networks due to the distinctive qualities of IoT. To deal with various security threats, deep learning and machine learning approaches that may incorporate knowledge from IoT devices are used. Within that study, we comprehensively examine the necessities, attack surfaces, including available security mechanisms in networks. Key holes in such security mechanisms that demand ML and DL strategies are therefore highlighted. Finally, we go into great detail about the ML and DL technologies that are now being used to solve IoT security challenges. We additionally go over a number of potentials lies in the following with ML and DL-based IoT security studies.

## III. PROPOSED METHODOLOGY

### 3.1 Data Collection

A device's user is able to receive service as required. IoT environments' many systems and applications should be durable throughout in order to continue to function, often in the midst of malevolent attackers or challenging circumstances. Different systems use different needs for reliability. In contrast, surveillance devices for disasters or medical conditions will probably need more reliability than detectors monitoring distorted noise.

Such organisations frequently serve their objectives through vengeance, stealing of proprietary information, corporate espionage, and attacks on the state infrastructure. The motivations of such organisations are fairly varied. It may entail providing personal information, including financial records, to terrorists, corporations, as well as other organised criminals. Several of these threats are caused by hardware flaws brought about by hacking extortion and inappropriate device asset utilization. This IoT must be made in a manner that makes simple and secure use management possible. For users to benefit greatly from the IoT and minimise user privacy threats, they must have the trust to do so. As was previously said, the bulk of IoT devices and services are vulnerable to a variety of typical dangers, including malware and DOS assaults. Precautions won't be enough to protect against such dangers and address the potential for error; instead, it's important to ensure that policies are implemented smoothly and are backed by reliable processes.

### 3.2 Threat Models in IOT

Persistent manipulation of a device inside an Iot is typically correlated with flaws, which frequently result from a major weakness in a system. To create a precise evaluation of the system overall, it is essential to study such vulnerabilities. In order to give a clear view of the origin of vulnerability in an IoT context and to underline the relevance of eliminating such flaws, we examined the weaknesses only at the gadget level. Iot systems have to be protected since vulnerabilities in security might possibly diminish the value of the device. In every IoT area, the increasing devaluation of sensors owing to inherent flaws might result in varying levels of damage.

### 3.3 Security Challenges

Weak security protocols raise the risk of data loss as well as other dangers. Owing to insufficient security procedures and regulations, the majority of experts perceive the IoT as a source of vulnerability for cybersecurity threats. Many safeguards have been created to safeguard IoT systems against intrusions; however, safety protocols really aren't properly documented. Nevertheless, because of the widespread use of smart devices that share and integrate data, many organisations are now very concerned about privacy or security breaches since they disrupt work processes, daily operations, and core networks. Experts are required to address such security issues, create thorough security policies and procedures to safeguard their corporate resources, and guarantee the continuation and reliability of their operations.

### 3.4 ML solutions in IoT

The implementation of IoT typically consists of a collection of comparable or pretty similar equipment with shared traits. Every vulnerability that seems to have a major impact on a few of those gets amplified by this commonality. Other organisations have developed instructions for conducting risk assessments based on this. Such action indicates there are probably an unparalleled number of linkages connecting IoT technologies. It is evident that even a large number of such gadgets have the chance to empathise with and speak informally and spontaneously with certain other gadgets. They demand that the analysis and assessment, approaches, and strategies linked to Iot be taken into account. The purpose of a recent study is to examine sophisticated assaults that might have been largely based on breaches of corporate security policies. When finished, an attacker is enabled to prey on people who link unapproved Internet of Things types to smart municipalities. Because of their high detecting precision and low false alarm rate, the preceding methods were widely used. They are unable to intercept new strikes, though. Outlier detection, on either hand, cannot accurately identify emerging assaults but does identify them. Traditional ML research has been

increasingly utilised for both processes. Modern gadgets that learn algorithms are unable to recognise sophisticated security breaches.

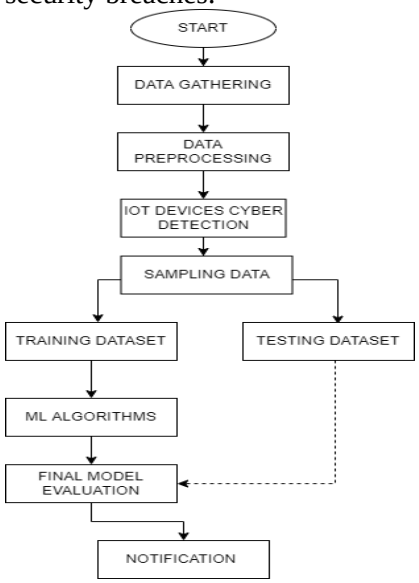



**Figure 1. Flow Representation**

## IV. DESIGN AND IMPLEMENTATION

### 4.1 Dataset

The IoT device market is expanding exponentially, giving hackers a larger system of vulnerabilities from which to conduct increasingly damaging cyber-attacks. This attacker wanted to use suspicious attacks to use up all of the bandwidth on the targeted network infrastructure. Iot's methodologies and detecting techniques necessitated well planned data. The most popular method in automated data analysis is categorization. The goal of categorization would be to build models using classified elements to predicate things. Assessment of contemporary intrusion prevention methodologies needs fresh, comprehensive data. The goal of categorization would be to build models using classified elements to predicate entities.

### 4.2 IOT Security Attacks

As IoT employs an information system comparable to the old network design for the interaction of many objects, it carries over the shortcomings of conventional system architecture. The Internet of Things has led to the creation of several threat vectors that aim to circumvent Internet of things safety. Efforts have been made to put up many defences against such assaults. Unfortunately, putting most of these safeguards and procedures into practise at once uses up gadget power consumption or processing power, which is unacceptable with IoT technology or its gadgets. Hence the need for a security feature that addresses all security vulnerabilities. It must be portable and strong enough to work with Iot. Numerous IoT threats have been explored and categorised here.

### 4.3 Machine Learning Algorithms

Similarly, to providing a model with numerous samples of documents to determine whether they are malicious software, all information must be labelled throughout. This algorithm might choose to include more information acquired here on data labelling. Another name for this is the task-driven method. Throughout this section, the issues with detecting attacks are investigated through the statistical categorization of measures utilising ML. Cybersecurity's search function isolates malware from various telecommunication services. Spam appears to be the most popular ML technique used in data security. In categorization, the training data labelling approach is typically utilised. The main drawback of core machine learning approaches is that they often require large datasets for model development.

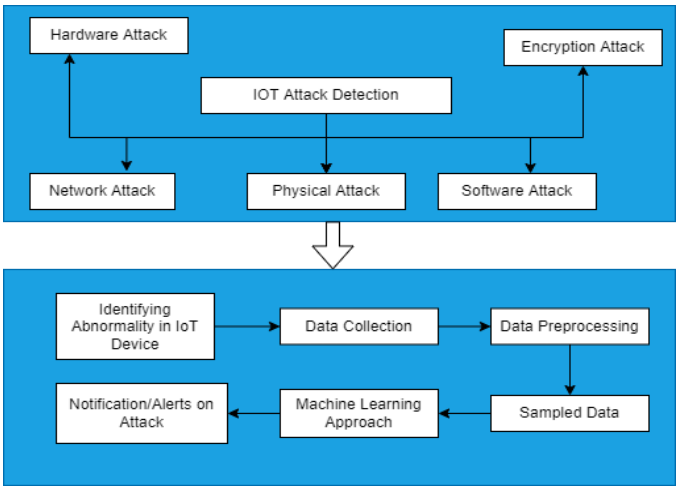



**Figure 2. IoT Attack Detection Mechanism Approach Using ML Techniques**

## VI. CONCLUSION

IoT confidentiality is still of utmost significance and is crucial to the development of the IoT market. This changing dynamic of Iot presents a variety of challenges for conventional confidentiality approaches. Through analysing statistics and environmental data, such training methods can promote self-organizing operations and increase the quality system efficiency. Every technology becomes more complicated whenever its capabilities cannot be reused or applied for multiple situations. Moreover, basic activities in complicated processes need several phases. SVM, RF, LR, and decision tree

algorithms were successfully used in machine learning systems to determine and alert users of smart IoT devices to potential threats.

## VII. REFERENCES


1. P. Illy, G. Kaddoum, K. Kaur and S. Garg, "ML-Based IDPS Enhancement with Complementary Features for Home IoT Networks," in IEEE Transactions on Network and Service Management, vol. 19, no. 2, pp. 772-783, June 2022, doi: 10.1109/TNSM.2022.3141942.
2. Inayat, Usman, et al. "Learning-Based Methods for Cyber Attacks Detection in IoT Systems: A Survey on Methods, Analysis, and Future Prospects." Electronics 11.9 (2022): 1502.
3. Mohamed, Yahia & Abdullahi, Mujaheed & Alhussian, Hitham & Alwadain, Ayed & Aziz, NorShakirah & Jadid Abdulkadir, Said. (2022). electronics Detecting Cybersecurity Attacks in Internet of Things Using Artificial Intelligence Methods: A Systematic Literature Review. Electronics. 11. 1-27. 10.3390/electronics11020198.
4. Z. Trabelsi, "Investigating the Robustness of IoT Security Cameras against Cyber Attacks*," 2022 5th Conference on Cloud and Internet of Things (CIoT), 2022, pp. 17-23, doi: 10.1109/CIoT53061.2022.9766814.
5. Tarek Gaber, Amir El-Ghamry, Aboul Ella Hassanien, Injection attack detection using machine learning for smart IoT applications, Physical Communication, Volume 52,2022,101685, ISSN 1874-4907, https://doi.org/10.1016/j.phycom.2022.101685.
6. M. Anwer, S. M. Khan, M. U. Farooq, and Waseemullah, "Attack Detection in IoT using Machine Learning", Eng. Technol. Appl. Sci. Res., vol. 11, no. 3, pp. 7273–7278, Jun. 2021.
7. Vitorino, J., Andrade, R., Praça, I., Sousa, O., Maia, E. (2022). A Comparative Analysis of Machine Learning Techniques for IoT Intrusion Detection. In: Aïmeur, E., Laurent, M., Yaich, R., Dupont, B., Garcia-Alfaro, J. (eds) Foundations and Practice of Security. FPS 2021. Lecture Notes in Computer Science, vol 13291. Springer, Cham. https://doi.org/10.1007/978-3-031-08147-7_13
8. Hussain, Fatima & Hussain, Rasheed & Hassan, Syed & Hossain, Ekram. (2020). Machine Learning in IoT Security: Current Solutions and Future Challenges. IEEE Communications Surveys & Tutorials. PP. 10.1109/COMST.2020.2986444.
9. K. Lounis and M. Zulkernine, "Attacks and Defenses in Short-Range Wireless Technologies for IoT," in IEEE Access, vol. 8, pp. 88892-88932, 2020, doi: 10.1109/ACCESS.2020.2993553.
10. Jadel Alsamiri and Khalid Alsubhi, "Internet of Things Cyber Attacks Detection using Machine Learning" International Journal of Advanced Computer Science and Applications (IJACSA), 2019.https://dx.doi.org/10.14569/IJACSA.2019.0101280
11. Prasanna Srinivasan.V, Balasubadra.K, Saravanan.K, Arjun.V.S and Malarkodi.S, (2021), "Multi Label Deep Learning classification approach for False Data Injection Attacks in Smart Grid", KSII Transactions on Internet and Information Systems, Vol. 15, No. 6.
12. A. Roukounaki, S. Efremidis, J. Soldatos, J. Neises, T. Walloschke and N. Kefalakis, "Scalable and Configurable End-to-End Collection and Analysis of IoT Security Data: Towards End-to-End Security in IoT Systems," 2019 Global IoT Summit (GIoTS), 2019, pp. 1-6, doi: 10.1109/GIOTS.2019.8766407.
13. A. Djenna and D. Eddine Saïdouni, "Cyber Attacks Classification in IoT-Based-Healthcare Infrastructure," 2018 2nd Cyber Security in Networking Conference (CSNet), 2018, pp. 1-4, doi: 10.1109/CSNET.2018.8602974.
14. I. You, K. Yim, V. Sharma, G. Choudhary, I. -R. Chen and J. -H. Cho, "On IoT Misbehavior Detection in Cyber Physical Systems," 2018 IEEE 23rd Pacific Rim International Symposium on Dependable Computing (PRDC), 2018, pp. 189-190, doi: 10.1109/PRDC.2018.00033.
15. Abomhara, Mohamed and Geir M. Køien. "Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks." J. Cyber Security. Mobil. 4 (2015): 65-88.

International Journal of Early Childhood Special Education (INT-JECSE)
DOI:10.9756/INTJECSE/V14I5.381 ISSN: 1308-5581 Vol 14, Issue 05 2022

# IoT-Smart Surgical System Treatment to Augment Safety For Hospital Management

**A.Sangeetha,**
Assistant Professor,
asangeethacse@rmkcet.ac.in,
Department of CSE,
R.M.KCollege of Engineering and Technology,
Chennai,Tamil Nadu,India

**S.Anitha Rajathi,**
Assistant Professor,
anitha.csbs@rmd.ac.in,
Department of CSBS,
R.M.D.Engineering College,
Chennai,TamilNadu,India

**Josephin Shermila.**
Assistant Professor,
blossomshermi@gmail.com,
Department of ECE ,
R.M.KCollege of Engineering College,
Chennai,TamilNadu,India

**P.S.Selvi,T.Ramesh**
Associate Professor,
ssi.cse@rmkec.ac.in,
trh.cse@rmkec.ac.in,
Department of CSE , Department of CSE,
R.M.K. Engineering College,
Chennai,Tamil Nadu,India

A***bstract*** - Based on the smart IoT, an intelligent surgical reporting system was created and implemented. The adoption of the system to write and retrieve data by health care staff saves time spent preparing forms and lowers the occurrence of mistakes, consequently enhance patient outcomes and care quality. Furthermore, this method enables all of the gathered information during the procedure to be accurately preserved and disseminated. This approach also reduced the cost of printing surgical record sheet and health-care record sheets and may be utilised as a knowledge repository for future procedures. The surgical information will save health care staff' time by constantly storing their personal information. In order to facilitate access to the information we have also used the voice-based information access. A chat bot is also trained on the surgical data which aids as a knowledge base on the surgeries.

***Keywords: IoT, Surgical records, Chatbot, knowledge repository***

## I. INTRODUCTION

The rise of the IoT becomes a key to innovation for health IoT, which enhances quality of patient care through more dependable and effective communication among physicians and nurses. The Internet of Things (IoT) is being incorporated into medical system in order to enable monitoring of patients and diagnostics through the use of intelligent healthcare equipment. Nurses may rapidly verify patient data using a smart phone, and updates are real-time. Information obtained from sensors in medical centers is steamed in real-time to perform accurate analysis. When executing a complex operation, the employment of an input technique by health care staff not only enables the rapid completion of numerous records required to finish the procedure, but also improves the completeness and quality of the input data. However, incidents of medical negligence such as inappropriate surgery sites, patient whose identification have not been verified, erroneous surgical processes and procedures, and other hazards continue to occur.

Because surgery is such an essential aspect of medical care, every examination and confirmation performed by nursing professionals from the point a patient is brought into the surgery room has an influence on the patient's safety. As a result, improving surgical processes is seen as a key safety indicator in enhancing treatment surgeries.

The standard surgical assistance system only provides a simple interface and does not give users with satisfactory operating results while utilising the system. Human mistakes and flaws in system validation procedures can readily compromise the quality and integrity of the medical data. Some articles advocated the construction of a surgical system that would utilise a new form of information technology to help health care staff manage the many data required throughout surgery. Furthermore, in terms of information system performance validation, various thesis studies used survey analysis to assess user satisfaction and operational effectiveness.

Furthermore, previous research offered six components for evaluating the performance of the system in terms of quantifying its success. In the regular procedure, On the day of the operation, the operating theatre control personnel alert the nurse’s stations to confirm the room number and patient's identification, finish all preparatory protocols, and wheel the patients into the surgery room. To maintain patient safety, before the anaesthetist gives anaesthetics, the nurse should validate data with the patients. Even before procedure, the physicians, anaesthesia nurse would take a "time off" from their job. This is the most crucial preparatory step: validate the patient's identification, surgical procedure, surgical location, and list of relevant medical professionals. Following surgery, the patient will be taken into the recovery area to wait for the anaesthetic to wear off.

In this work, we develop a smart integrated system to enhance safety of patients while seeking medical treatment and to improve the openness of hospital information. Using RFID technology, the Internet of Things provides a new medical information system. It has become the primary IoT technique. Radio frequency identification not only helps us identify physicians, nurses, and patient in the health information system, but it also allows us to follow physicians, nursing staff, and patients around the hospitals. In order to build a smart data system, information is collected into the system. In this work, we create an autonomous surgery management system to eliminate textual mistakes caused by human error, reduce nurse and surgeon burden, and improve quality of healthcare services.
Documentation used in operations are removed and recorded in computers through the construction of the planned intelligent surgical management system. The intelligent surgical information system is a combination of recording the surgery, store the same in a cloud-based storage for ease of access and to convert text to speech recordings which can be used for future research. The system uses a smart recording based on sensors. The smart surgery information management system helps medical staff import medical notes, scanning reports, audit results, and other related details before, during, and even after surgery. If the records are incomplete, the checking system can automatically view their completeness and maintain a high level of integrity.

**II. LITERATURE REVIEW**

Imran Ahmed [1] proposed a paper in which indicates that the health sector is paying attention towards the development of smart sensing devices, gadgets, data storage, and healthcare technology. IoT, particularly in medical image analysis, has indeed been identified as among the most potential discoveries in the field of medical services. For the analysis of clinical images, technique combines ai technology with a variety of advanced machine learning approaches. Such recently founded methods for diagnostics could help doctors diagnose illnesses at a preliminary phase, give precise, reliable, efficient findings quickly, and lower the risk of mortality.

Coronavirus (COVID-19) is currently one of the most serious and virulent illnesses, and it is expanding around the globe. In this way, a smart medical system for automated detection and categorization of infectious illnesses (such as influenza) in chest X-ray images was demonstrated. This way this works uses a multi-layer convolution layer and feature selection technique together with two separate deep learning architectures to categorize X-ray pictures of viral disorders. The stages involved in this work are as follows: Data augmentation is utilised to increase the variety of data collection, and deep learning models like VGG-19 and Inception-V3 were combined using transfer learning enabling feature extraction. This multi-logistic regression regulated entropy variation technique is used for fusing of features extracted acquired from deep learning approaches, a parallel maximal correlation, as well as for selecting features.

According to Fatima Alshehri [2], an essential component of linked existence is smart healthcare. Another of the fundamental human needs is health care, and it is predicted that in the near future, smart health care will generate many incomes. An Internet of Things (IoT), the Internet of Medical Things (IoMT), medical sensors, artificial intelligence (AI), edge computing, cloud computing, and next-generation wireless communication technologies are all just a few of the elements that make up smart healthcare coverage. Therefore, we give a thorough analysis of journal publications from 2014-2020 that primarily focus on IoT and IoMT-based edge-intelligent smart healthcare coverage. Through addressing numerous study fields on IoT and IoMT, AI, edge and cloud computing, security, and medical signals fusion, we review this literature. We also discuss contemporary difficulties in research.

Mohd Javaid [3] indicated that Healthcare can see radical innovation with the Internet of Things (IoT). A need to research various IoT-enabled applications and services in light of the COVID-19 Epidemic. A quick study is needed for it to choose the best course of inquiry. To determine the potential of technology, studies on COVID-19 Pandemic and IoT within healthcare are conducted. This literature-based analysis might help analysts believe of solutions to connected issues and combat pandemics of the COVID-19 kind. Using the aid of a flowchart, quickly analysed the key IoT accomplishments. Subsequently list out seven key IoT technologies which appear to be beneficial for healthcare it during COVID-19 Pandemic. This report concludes by listing and briefly describing sixteen fundamental Iot systems for the health industry as during COVID-19 Pandemic.

Aravind H [4] introduced a paper on the vital signs as it is the crucial component of tracking a patient's improvement while they are being treated in a clinic because they enable prompt identification of situations that might impede recuperation or be unfavourable. Throughout a surgical procedure and the recovery phase, the vitals were continually or regularly checked. Several electrodes placed to the patient's body using the well-known monitoring and diagnostic tools in order to evaluate change in the electrical stress in the system. Every individual getting inspected is obstructed by these wires and valves. This idea suggests a simple diagnosis and surveillance facility for post-operative patients.

Yazdan Ahmad Qadri [5] proposed a paper on the growth of the health sector has been greatly impacted by the IoT devices (IoT). The introduction of Medical 4.0 has led to an increase in infrastructure development efforts, at both hardware and source code levels. Healthcare IoT (H - IoT) technologies have been developed as a result of this idea. The methods of communication in between sensor and the processor are among the fundamental technological solutions, are the computational methods used to provide an outcome from sensor information. Nevertheless, a number of new innovations are now supporting these technological solutions.

The H-IoT sector has undergone nearly complete transformations because to the usage of ai technology (AI). The fog / edge concept minimizes several issues by deploying computer power near to the packet network. Although processing massive amounts of data is made possible by big data. Furthermore, the network is flexible thanks to Software - Defined Networks (SDNs), whereas blockchains are discovering the most inventive applications in H - IoT systems. Development in H-IoT technologies is being driven by the Internet of Nano Things (IoNT) as well as the Tactile Internet (TI). This article examines the extent in which these technologies are changing H-IoT networks and pinpoints the best potential route for enhancing QoS with these emerging innovations.

According to G. Yang [6], the industry 4.0 in healthcare technology has become underway, and it is being driven by manufacturing-related technology (Healthcare 4.0). Latest generation home health care robotic systems (HRS) built upon cyber-physical systems (CPS) featuring better speed and so smarter implementation are developing as an illustration of this revolution. These innovative concepts and functions for the CPS-based HRS are put out in this paper. Analysis of the most recent developments in relevant technological solutions, such as a.i., basics of sensors, material, and machineries, cloud services, connectivity, motion detection, and geolocation. Furthermore, the prospects for the CPS-based HRS are examined, along with the technical difficulties encountered in each technological area.According to Obaidulla Al-Mahmud [7], Furthermore, a sophisticated IoT medical system was proposed that includes medication boxes having cognition linked to sensors and a database for ongoing health tracking. This wireless internet access of these sophisticated medication boxes enables simple communication between healthcare professionals and patients even when they are not at the same specific address. As well as an email that would help patients in taking the medication, the suggested medication pack aids the patient with taking the proper medication so at right time. A laptop is often used as a webserver to keep detailed info on the client and therapist, as well as the medication prescribed as well as the schedule of the visit. While going through this process, both doctor as well as the patient require IDs and passwords.

Yazdan Ahmad Qadri [8] proposed a paper on implementing IoT which has an influence on lowering healthcare costs and improving the patient's recovery. Consequently, through providing a potential pathway to combat this COVID-19 epidemic, our current study-based research aims to examine, analyze, and emphasize its broad applicability of well IoT concept. Several important IoT devices are eventually listed and explored. In the end, it has compelled experts, academics, and scientists to suggest several useful countermeasures towards this epidemic. IoT helps a COVID-19 patient monitoring patients and receive higher therapy more quickly. Patients, doctors, surgeons, and hospital admin systems can all benefit from it.

According to Shuo Tian [9], since informational advanced, the design of smart health had steadily gained attention. Technology mainly transforms the standard medicine scheme in a comprehensive way, allowing healthcare access that is quite effective, quite simple, and far more individualized. It does this by utilising a future group of technological advancement, including the iot devices (loT), big data, cloud services, and machine intelligence. In order to bring the idea of health care, we initially identify the major platforms that help it here in this assessment. We next discuss where smart approach is right there in a number of significant areas. Next, we discuss the issues that significant quality now facing and make some suggestions for how to address them. Lastly, we assess the possibilities for smart health in the ahead.

P. Sundaravadivel introduced a paper on the traditional physician visit had deteriorated its usefulness due to the growing global population. As a result, significant quality is crucial. Smart healthcare may be adopted throughout all stages, including measuring infants' body temperatures through elder patients' physiological parameters. Depending upon that needed accuracy of specific devices, functions, and complexities of applications with that they are employed, the effort and installation cost vary. These converging fields of integrated devices, big data, deep learning, cloud services, as well as cognitive computing have included smart healthcare. These chapter examines the significance, needs, and uses of healthcare as well as marketing trends and developed. Also, it provides a clearer understanding of the many venues by which additional study inside this subject may be conducted.

## III. PROPOSED METHODOLOGY

The suggested surgical information app is a mobile device with a web-based interface organised as components which will handle all the procedures of the surgery. The nursing staff can check the surgical schedule data for the day prior to a surgery. This technology may be utilised throughout the operation to enter the surgical patient's physiological parameters, the number of surgical appliances used, surgery-related data, and nurse's data.

The postoperative statistics of surgery patients may also be accessible by clinics and nurses' stations, making it easier to tally and price back-end supplies, as well as for learning goals such as case research and teaching. It not only retains clear and accessible paper documentation of invasive procedures data, but it also offers validation and reminder methods to guarantee the fulfilment of the things that must be correctly filled out. Furthermore, the affirmation function enables the following attribution of accountability as well as the successful retention of experiences and knowledge during surgical operations, promoting future study advancement.

The initial information of the patients such as their personal data will be loaded in the system followed by the details on the surgical procedures. A unified format for maintaining a surgical record is created on the data base and the same format to be followed for all the surgeries making it efficient for future access and reference of data for research and other studies. A cloud based centralized storage is available to store the data which enables other doctors to verify the procedure done to the similar surgery on complex tasks.

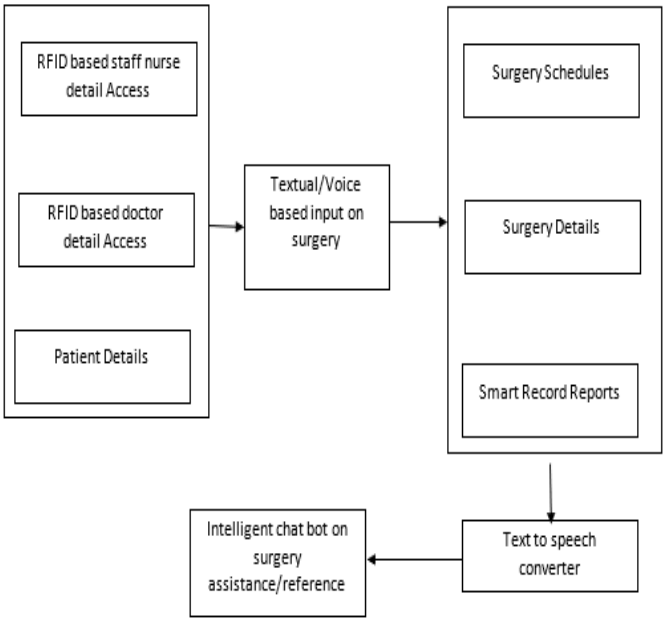



***Figure 1. Architecture Diagram***

The entire surgery details and the procedure will be recorded in digital format whereas the RFID tag details will be read by the smart system. The effective maintenance of the surgery records leads to an efficient and safe surgery. The findings of the details in the phase of surgery will also be recorded thus making it an effective knowledge base. A physician must verify the full health history information filled out before, during, after the surgery for discrepancies to assist the automated information gathering needed. The smart system also has a text to speech converter which aids in the form of hearing the entire surgery procedure in a voice form. An intelligent chat bot is also embedded in the design which is trained with the surgical data so as to assist the surgeries with the previously available data.

The primary goal of identifying the surgical site and special product placement site is to double-check the surgery markings on the patient before to surgery in order to avoid medical disputes caused by operating on the incorrect spot. The numbers of appliances utilised during the procedure is documented in the equipment logon. During the procedure, the use of the equipment may be documented several times. The system automatically adds the equipment utilised for the nurse to quickly tally and validate at the conclusion of the operation, after which the checker's name is inserted and the staff in responsibility of the equipment counting was recorded for the purpose of duty attribution.

## IV. DESIGN AND IMPLEMENTATION

### *4.1 Textual/Voice Based Input*

This voice to text conversion is carried out by using either voice to text models as well as context characteristics. The contextual

specifications are utilized to influence the results which are produced over voice to text model. Since voice response technology enables medication data to be recorded and heard instead of being written by a doctor, the development of speech-based mobile applications might help to minimise a few of these errors. This report describes the development of a voice-based mobile prescriptions to enhance healthcare services.

### *4.2 Smart Record Reports*

In the health sector, the process of documenting information and the people's clinical record is crucial and is termed as medical record data. This patient's medical record information may be utilized as a source for future patient health examinations and as verifiable proof of the patient's illness's diagnoses as well as the medical care she / he received. The development of an intelligent healthcare system must centre on the patient. Patients may rapidly get previous medical information, register online using a mobile application, and receive quick, measured treatments.

### *4.3 RFID Detail Access*

Medical failure minimization is among the major promises that were made by complicated RFID systems. Its incorporation of an RFID system which self-regulates is essential when one of healthcare's top priorities is to assure patient safety. This system is unable to function independently. Any clinic will require qualified organizations to work the hardware and software enabling full-scale installation and control of the network. Professional training and education are among of the most difficult barriers for RFID to conquer since they are frequently time-consuming and expensive.

## V. EXPERIMENTAL RESULTS

An effective technique to document the surgical operation in its three parts, including pre-operative information, operation information, and post-operative care. Accessibility to surgical data in the case of smart records is made possible via an interconnected system. Pre-operative, its smart surgical technology double-checks the patients' preoperative marks in order to prevent medical disputes brought on by improper operation. Mainly, to prevent human mistake in data upkeep throughout operational stages are developed. RFID-based data entry for personnel records on medical professionals and other staff members. For research and resource sharing, text to speech conversion makes it possible to voice out all of the information of the procedure. An intelligent assistant is a chatbots powered by neural networks that can autonomously adapt depending on surgery information.

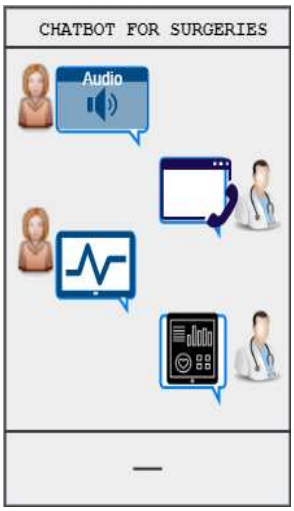



***Figure 2: Chatbot for surgeries***

Having improved access to large volumes of sensory data, data-driven approaches are increasingly appreciated for identifying potential flaws or variations from anticipated. Caretakers have access to real-time data through virtualized environments or other networking phenomena, enabling educated choices and providing evidence-based therapy. This guarantees prompt delivery of healthcare and enhanced therapeutic results. The patient's requirements are prioritised because of the internet of things' link with the healthcare system such as therapies that are swift, reactive, and increased in quality and reliability. Whenever it relates to diagnostics, prompt medical action and improved treatment results lead to responsible care that patients significantly value.

The IoT system is utilized to thoroughly identify and evaluate numerous specific health indicators and further mining this data. The difficulties of visiting a doctor can be considerably reduced with the remotely wireless health managed service system. The digitization and accessibility of hospital information have been fully accomplished through sophisticated treatment of patient equipment based on internet of Things. We investigate how to make training more humane, but we must additionally think about how to make instruction less problematic for such system detection phase.

## VI. CONCLUSION

An intellectual surgery reporting technology was implemented and put into use relying mostly on smart IoT. Use of a system for medical professionals to enter and collect data reduces errors or time saving consumed filling out paperwork, which improves clinical outcomes and the standard of care. Additionally, this technique makes it possible to precisely retain as well as share all the data that was obtained during process. The method could be used as a learning baseline for future treatments and also decreased reduced cost to produce surgery recording pages and patient records pages. By continuously saving the personal details of the medical team, the surgery data can save them time. We have implemented voice-based access to information to make it easier for people to get the data. Additionally, a chatbot that serves as a knowledge base for the procedures is educated on the medical data. An intelligent IoT-based surgery information management with RFID-based access to data for the medical team in the operating room will retain all surgical data entirely. Automatic Report Generation utilizing voice and text input during the surgical procedure. Smart Notes throughout the surgical procedure. Using a text-to-voice conversion to deliver out the full document and a CNN-powered intelligent chatbots to teach it all there is to know about the procedure and serve as a resource for subsequent usage.

## VII. REFERENCES

1. Ahmed, I., Jeon, G. & Chehri, A. An IoT-enabled smart health care system for screening of COVID-19 with multi layers features fusion and selection. Computing (2022). https://doi.org/10.1007/s00607-021-00992-0
2. F. Alshehri and G. Muhammad, "A Comprehensive Survey of the Internet of Things (IoT) and AI-Based Smart Healthcare," in IEEE Access, vol. 9, pp. 3660-3678, 2021, doi: 10.1109/ACCESS.2020.3047960.
3. Javaid M, Khan IH. Internet of Things (IoT) enabled healthcare helps to take the challenges of COVID-19 Pandemic. J Oral Biol Craniofac Res. 2021 Apr-Jun;11(2):209-214. doi: 10.1016/j.jobcr.2021.01.015. Epub 2021 Jan 30. PMID: 33665069; PMCID: PMC7897999.
4. H, Aravind. (2020). IOT based Wearable for Surgical and Post-Operative Patients. International Journal of Engineering Research and. V9. 10.17577/IJERTV9IS060666.
5. Yazdan, Qadri & Nauman P.hD, Ali & Zikria, Yousaf & Vasilakos, Athanasios & Kim, Sung Won. (2020). The Future of Healthcare Internet of Things: A Survey of Emerging Technologies. IEEE Communications Surveys & Tutorials. PP. 1-1. 10.1109/COMST.2020.2973314.
6. G. Yang et al., "Homecare Robotic Systems for Healthcare 4.0: Visions and Enabling Technologies," in IEEE Journal of Biomedical and Health Informatics, vol. 24, no. 9, pp. 2535-2549, Sept. 2020, doi: 10.1109/JBHI.2020.2990529.
7. O. Al-Mahmud, K. Khan, R. Roy and F. Mashuque Alamgir, "Internet of Things (IoT) Based Smart Health Care Medical Box for Elderly People," 2020 International Conference for Emerging Technology (INCET), 2020, pp. 1-6, doi: 10.1109/INCET49848.2020.9153994.
8. Singh RP, Javaid M, Haleem A, Suman R. Internet of things (IoT) applications to fight against COVID-19 pandemic. Diabetes Metab Syndr. 2020 Jul-Aug;14(4):521-524. doi: 10.1016/j.dsx.2020.04.041. Epub 2020 May 5. PMID: 32388333; PMCID: PMC7198990.
9. ES Madhan, KS Kannan, P Shobha Rani, J Vakula Rani, Dinesh Kumar Anguraj, 'A distributed submerged object detection and classification enhancement with deep learning', Distributed and Parallel Databases, 2021/5/22, Springer US
10. Shuo Tian, Wenbo Yang, Jehane Michael Le Grange, Peng Wang, Wei Huang, Zhewei Ye,Smart healthcare: making medical care more intelligent, Global Health Journal,Volume 3, Issue 3,2019,Pages 62-65,ISSN 2414-6447, https://doi.org/10.1016/j.glohj.2019.07.001.
11. P. Sundaravadivel, E. Kougianos, S. P. Mohanty and M. K. Ganapathiraju, "Everything You Wanted to Know about Smart Health Care: Evaluating the Different Technologies and Components of the Internet of Things for Better Health," in IEEE Consumer Electronics Magazine, vol. 7, no. 1, pp. 18-28, Jan. 2018, doi: 10.1109/MCE.2017.2755378.
12. M. K. Ishak and N. M. Kit, "Design and Implementation of Robot Assisted Surgery Based on Internet of Things (IoT)," 2017 International Conference on Advanced Computing and Applications (ACOMP), 2017, pp. 65-70, doi: 10.1109/ACOMP.2017.20.
13. V. Vippalapalli and S. Ananthula, "Internet of things (IoT) based smart health care system," 2016 International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES), 2016, pp. 1229-1233, doi: 10.1109/SCOPES.2016.7955637.
14. A Vasantharaj, Pacha Shoba Rani, Sirajul Huque, KS Raghuram, R Ganeshkumar, Sebahadin Nasir Shafi,' 'Automated brain imaging diagnosis and classification model using rat swarm optimization with deep learning based capsule network',International Journal of Image and Graphics, 2240001, World Scientific Publishing Company
15. P. Gupta, D. Agrawal, J. Chhabra and P. K. Dhir, "IoT based smart healthcare kit," 2016 International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT), 2016, pp. 237-242, doi: 10.1109/ICCTICT.2016.7514585.

16. S. M. R. Islam, D. Kwak, M. H. Kabir, M. Hossain and K. -S. Kwak, "The Internet of Things for Health Care: A Comprehensive Survey," in IEEE Access, vol. 3, pp. 678-708, 2015, doi: 10.1109/ACCESS.2015.2437951.
17. A. K. Jaithunbi P. Shobha Rani, Vasukidevi G.,C. S. Anita,Vimal Kumar M. N.,' COVID tweet analysis using NLP', International journal of Health Sciences, https://doi.org/10.53730/ijhs.v6nS3.8314, 2022/6/2,Vol 6,S3.8314
18. L. Catarinucci et al., "An IoT-Aware Architecture for Smart Healthcare Systems," in IEEE Internet of Things Journal, vol. 2, no. 6, pp. 515-526, Dec. 2015, doi: 10.1109/JIOT.2015.2417684.

INDIAN JOURNAL OF SCIENCE AND TECHNOLOGY

RESEARCH ARTICLE

# Ensuring Secure Routing in Wireless Sensor Network Using Active Trust

**G Amudha**[1]*

**1** Associate Professor, Computer Science and Business Systems, R.M.D Engineering College, Chennai, 601206, India

OPEN ACCESS

**Received:** 11.03.2021

**Accepted:** 23.11.2021

**Published:** 06.12.2021

**Citation:** Amudha G (2021) Ensuring Secure Routing in Wireless Sensor Network Using Active Trust. Indian Journal of Science and Technology 14(41): 3107-3113. https://doi.org/10.17485/IJST/v14i41.424

* **Corresponding author**.

gav.csbs@rmd.ac.in

**Funding:** None

**Competing Interests:** None



Published By Indian Society for Education and Environment (iSee)

**ISSN**
Print: 0974-6846
Electronic: 0974-5645

## Abstract

**Objective:** Main objective is to provide a secure router for transferring the valuable data being sensed. One of the major security threats in WSN is the Black hole attack, due to which incoming and outgoing traffic is silently discarded without informing the source that the data did not reach its intended recipient. Overcoming the Black hole attack in WSN is a current research topic. So, the proposed method of trust based secure routing will overcome the black hole attack. **Method:** The method implemented is integrated as Active Trust to the existing AODV routing protocol to avoid the Black hole attack in WSN. ActiveTrust can relevantly maintain the data route success quality and capacity against black hole attacks and can optimize network lifetime. **Findings:** Packet delivery ratio and Throughput are measured considering the attack and applying the method implemented. It is noticed that packet delivery ratio is less when there is an attack, and it gets increased when the attack is been rectified by Active trust method. **Novelty:** Trust based secure routing when compared with existing protocol AODV the attack is reduced and the throughput gets increased by reducing the packet loss. Our approach is efficient in terms of throughput and PDR. As trust factor is so important factor while compared to other factors like Node identity, Node Address etc., our proposed system is efficient. Because node identity can also be spoofed and node address can also be modified by an intruder, but the trust calculation based on the activity of the node cannot be modified by any attacker, because it involves the neighbour node to calculate the trust.

**Keywords:** Black hole attack; AODV; Trust; Secure routing

## 1 INTRODUCTION

A Wireless Sensor Network (WSN) has a wide range of applications [(1)], slowly becoming an integral part of life. (Wireless network can be physical or environmental conditions to monitor the sensor to be spatially distributed autonomous devices. The sensor network consists of multiple detection stations called sensor node, which is small, lightweight & portable.) The main task of WSN is to sense and collect data from a certain domain, process, and transmit into the sink. WSN application and communication are mainly tailored to provide high energy efficiency. (WSNs are a single embedded

system that is very much interacted through various kinds of sensors, local information, and communication with their neighbours. WSN applications are the area, health care, and air pollution monitoring, environmental/earth sensing, forest fire detection, landslide detection, data logging, and so on. The sensor network architecture is more important to understand that Wireless sensor networks are very popular technology). However, the limited computing power, storage capacity, energy, and other restrictions of the nodes influence the development of WSNs[2]. When randomly deployed in complex environments, WSNs are especially vulnerable to routing attacks from malicious nodes. Therefore, it is essential to establish new methods that can optimize security issues and reduce energy consumption in WSN[3].

A Black hole attack is a type (DoS) attack; it is also called the packet dropped attack. In networking, the black hole is saliently dropped the data packet not giving any more information to the source that the data did not reach the destination.The black hole attack is frequently deployed to wireless networking. It drops the data and bluffs the previous node.

Trust-based route strategies face some challenging issues such as[4]. The core of a trust route lies in obtaining trust: however, the node of trust is more difficult, (and how it can be done is still unclear. Energy efficiency: WSNs very low in energy, the trust accession, and spreading have high energy-draining, which seriously affects the network's lifetime. Security: It is hard to locate the unwanted nodes, the security route is still a target for future challenges.

## 2 LITERATURE REVIEW

The trust-based AODV (Ad hoc On-Demand Distance Vector) routing protocol by the exclusion of a black hole attack is suggested by[5]. The black hole attack is an ordinary security issue in the mobile ad hoc network (MANET) routing protocol. The routing table is inserted into the trust value. The route was established according to the routing table and the rest of the part is similar to the traditional AODV routing protocol. The trust value and threshold value are depending upon the black hole node is identified.

Bambi defines as (Black hole Attack Mitigation with Multiple Base station in WSN) techniques by[6] has suggests to effectively mitigate the adverse effects of black hole attacks on WSNs. An adversary captures the network and create some nodes to drop the packets which leads to Black hole attack.As multiple base stations are deployed in the network, copies of data packets are routed to these base stations and the solution is highly effective and requires very little message exchanges in the network, thus saving the energy. The Bambi identified all the black hole attack in the network. This attack technique completed more than 99% packet delivery success rate and prove that project can identify 100% of the black hole nodes.

Clean and efficient methods by[7] to discover and identify the silent failures, i.e. data packets are silently dropped inside the network without giving any responses. This method uses edge routers to raise alarms whenever end to end connectivity is interrupt at active measurement. In this tier-I ISP network successfully discover and confine the black holes and authors focus on the silent faults from the interactive b/w MPLS and IP layers of backbone networks. The real failure data get from a tier-1 network's IPFM and MPFM systems, then troubleshooting failures are demonstrated effectively using both systems at network operators.

In[8] to resist smart black-hole attacks empowered timers and baiting message consists of two phases: Baiting and Nonneighbor Reply. In Baiting phase each node has a bait-timer, the value of the timer is set randomly to B seconds, and each time the timer reaches B it creates and broadcasts a bait request with a randomly generated fake id. Depending on the natural behavior of a black-hole node when it receives any route request it responds with a reply claiming that it has the best path even if it does not exist.

To design a multipath routing protocol that detects and avoids the path containing black-hole. Our paper[9] proposes a way to defense the black-hole and gray-hole attacks with the help of intelligence in MANET.

In[10], a trust-based drone energy-saving data acquisition scheme which uses the quadratic optimization method of the drone path was proposed to find routing paths. Moreover, trust inference and evolve mechanisms are also utilized to identify the trust degree of the sensor node. Therefore, it can effectively find an optimized data collection trajectory and better balance the energy consumption of the network.

In[11], the beta and direct trust model is used for secure communication in WSNs to reduce energy consumption. However, large overlapping areas of communication range among the cluster heads often lead to too many cluster heads, which wastes energy accordingly. In addition, the defendable attacks were not specified in BRDT.

In[12], a secure routing protocol based on the trust levels of nodes called Grade Trust was proposed to defend against black-hole attacks. The packet delivery ratio is improved in Grade Trust, but only a black-hole attack can be defended against.

Therefore, to defend against other kinds of attacks, a clustering-based secure routing protocol was proposed in[13]. First, cluster heads are selected by the energy-efficient clustering algorithm. Next, a trusted hardware module is adopted to encrypt the data during the operation of the network, which can effectively defend against many kinds of attacks such as data confidence and data integrity, and compare node attacks. However, the cluster head nodes need to have permanent energy supply equipment,

which leads to high requirements for the WSN layout.

In [14], a trust-based energy-preserving multihop routing protocol which is a hybrid of encryption and a trust management-based protocol was proposed. However, it does not calculate the indirect trust value, so some errors will occur when calculating the trust values of neighbor nodes.

Therefore, based on semiring theory a trust sensing secure routing mechanic was proposed in [15]. It considers the direct trust calculation of nodes, indirect trust calculation of nodes, incentive factor, energy trust, and quality-of-service metrics to optimize secure routing paths. High computing power for the nodes is needed in [16]. Hence, to reduce the computational complexity of the nodes, a lightweight and quickly deployable trust–based secure routing protocol (TBSRP), which can detect and isolate the misbehaving nodes, was proposed in [17].

The protocol extends the route establishment process in ad hoc on-demand distance vector (AODV) routing [18] to select a reliable and effective path that includes all trusted nodes. The salient features of AODV include on-demand route finding, reduced control packet overhead, providing the latest routing information, broadcasting or unicasting routes at the same time, low storage cost, high scalability, and short connection analyzed [19]. In all the above mentioned techniques the amount of storage and time taken to compute the attack are very high compared to the proposed system,

## 3 PROPOSED WORK

The Active Trust method for WSN to avoids black holes by keeping track of their number and obtains a trust model. The method improves the data route security. ActiveTrust can relevantly maintain the data route success quality and capacity against black hole attacks and can optimize network lifetime.

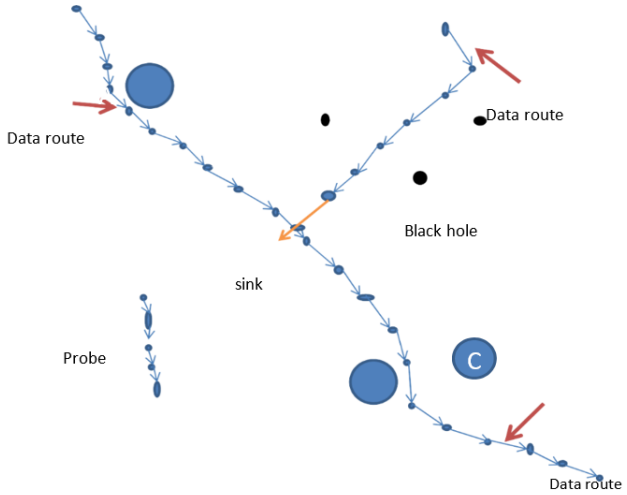



**Fig 1.** Illustration of the Activetrust

ActiveTrust methods have two routing protocols are, 1)Active detection routing protocol: A detection route has absent of data packets, the goal to satisfy the contender to launch a router attacker, then the black hole attack can be complex recognizer to mark the attack. The active detection routing guides the data route to select the node with a high-level trust to keep away from the black hole attack. 2)Data routing protocol: The data routing is the process of nodal data routing to the sink. The route will select a node with high trust to avoid the black hole attack and improves the success radio of reaching the destination.The idea of data routing is any node receives a data packet, it selects the 1 node from the set of the node with trust is greater than the threshold. The upper node recalculates the unselected and selected node to check if the node cannot find the next step of the hop node it sends a feedback failure report to the upper node.

In this work, Active Trust computation is implemented using the subjective logic method. Subjective logic [20] is involving unpredictability and untrustworthy sources in situations for model and analysis type of probabilistic logic. Subjective logic uses constant unpredictability and trust parameter alternative of using discrete trust values. Subjective opinions about state variables that can take values from the mark condition value can be an idea of as a proposition that can be true or false.Figure 2, The

subjective logic tubules are (b,d,u,a)where,

b = belief mass,

d =disbelief mass,

u =uncertainty,

a = base rate.

$\boxtimes_x$= (b,d,u,a), let x be the trust value of the binary domain.

b,d,u,a $\varepsilon$ [0,1], whereb+d+u=1;

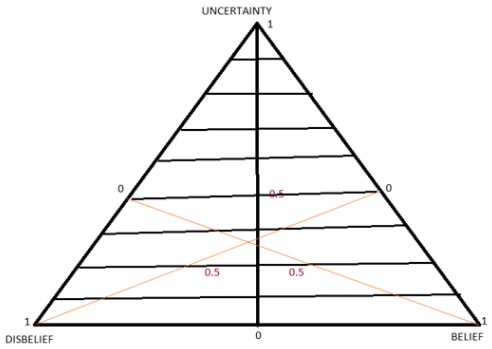



**Fig 2.** Opinion Triangle

The capacity of subjective logic in the presence of uncertainty, and modelling trust networks, combined with the power of Bayesian networks for modelling structures, creates a combination that calls a Subjective Network. A probabilistic logic for uncertain probabilities becomes subjective network logic. It distinguishes between certain and uncertain conclusions it is possible to make clear analysis throughput on preserved uncertainty is an advantage.

Trust network analysis using subjective logic (TNA-SL)[10] provides a simple notation for expressing transitive trust relationships and defines a method for simplifying complex trust networks, Trust measures are expressed as trust subjective logic is used to calculate between random reunion in the network. Trust values are components of an absolute structure(T;$\leq$), P is the set of principals and the trustspace is a partial function T: (P $\boxtimes$ T), P be the set of nodes in the network. Let $\varphi^{v}{}_{r}$= (x; y) be aroute(r) where x; y are the numbers of lucky and unlucky packet transmissions individually, the opinion corresponds to $\varphi$ be$\boxtimes(\varphi)$= (b; d; u) where

$$b = x = (x + y + r) \tag{1}$$

$$d = y = (x + y + r) \tag{2}$$

$$u = r = (x + y + r) \tag{3}$$

where r $\geq$1 is a parameter behavior of the rate of loss of unpredictability, which can be used to adjust the use of uncertainty.

The transitivity and fusion operators are modeled with a combination of subjective trust networks. Let [A;B] express the someone trust edge from A to B, and let [B, X] express the trust edge from B to X. As expressed on subjective trust node are $([A;B] : [B,X] \diamond [A;C] : [C,X])$

As shown in Figure 3. The source A, B, and C specify that consecutive order in which the trust edges and advices are formed. Then, given set of trust edges with index A, the origin trust A receives advice from B and C, and is able to gain trust in variable X. By expressing each trust edge and belief edge as an opinion, it is possible for A to derive belief in X.

The advantage of subjective logic is, it is real-world situations can be modelled and analyzed more realistically, it allows decision-makers to be better informed about uncertainties specific situations, and future outcomes, it is directly compatible with traditional mathematical frameworks and handling ignorance and uncertainty.

## 4 RESULT AND ANALYSIS

As shown in Figure 4. The Packet to Delivery ratio can analyze by introducing an attacker to any of the nodes. The transmission remains constant throughout the packet delivery ratio is very high and the absence of an attacker gets Normal transmissions

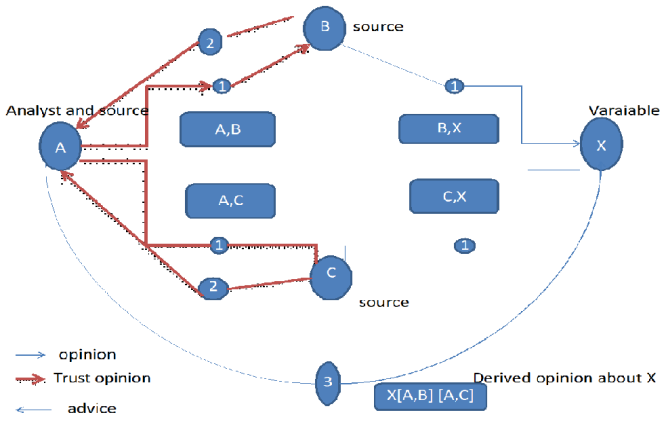



**Fig 3.** Subjective trust network

of packets.The number of packets sends the results to the number of packets received the performance very high. While in the packet delivery ratio has comedown to very low values to get a clear notice about the presence of an attacker. The attacker takes over the sent packets results from the source leading to the low delivery of packets to the destination.

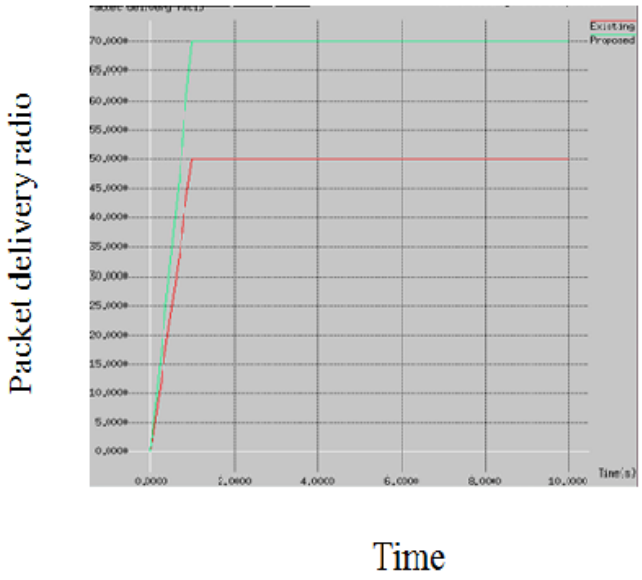



**Fig 4.** Packet delivery radio graph

As show in Figure 5 The midpoint in every part of the absence then the attacker is very high; the large part of packets sending from the source will reach the planned destination without any packet loss.

As the packet delivery ratio is good, the throughput is also high when there is a huge number of nodes.The throughput hears the packet pass by the sender will not be successful in reaching the destination.

The throughput and packet delivery ratio is AODV protocol using a black hole attack by analyzing the measure an attacker on a particular node. Whatever, the attacker declares for a specific node, it is possible to get various parameters like throughput, packet delivery ratio, etc. can differ accordingly.

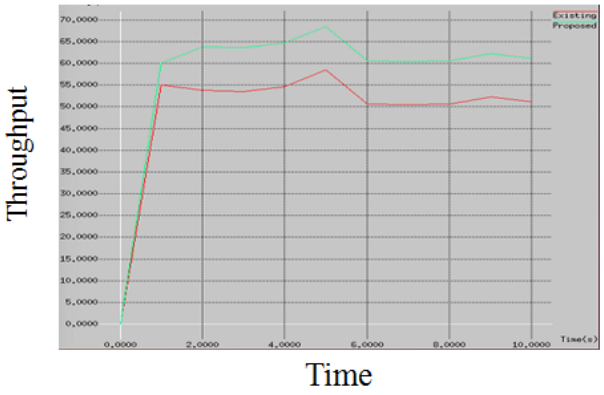



**Fig 5.** Throughput graph

## 5 CONCLUSION

The approach explained in this work is to detect and avoid the black hole attack in the WSN. The detection of these attacks has shown to improve the secure transmission of packets between the sensor nodes.The trust value is used to identify the black hole attack and it is barred from the route establishment process.The Active Trust plan can quickly discover the nodal trust and then avoid doubtful nodes to quickly achieves a 100% successful router probability. This scheme improves both energy efficiency and network security performance. Our proposed method after implemented in the network number of packets delivered ration gets improved by 5% for instance in case of existing AODV based routing method the PDR is in range of 50, our proposed method has got PDR as in range around 70. Similarly, throughput also gradually increasing compared to the existing algorithm. So active trust based algorithm is efficient when compared to the existing algorithms.

### ACKNOWLEDGMENT

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

## References

1) Sun Z, Wei M, Zhang Z, Qu G. Secure Routing Protocol based on Multi-objective Ant-colony-optimization for wireless sensor networks. *Applied Soft Computing*. 2019;77:366–375. Available from: https://dx.doi.org/10.1016/j.asoc.2019.01.034. doi:10.1016/j.asoc.2019.01.034.
2) Selvi M, Thangaramya K, Ganapathy S, Kulothungan K, Nehemiah HK, Kannan A. An Energy Aware Trust Based Secure Routing Algorithm for Effective Communication in Wireless Sensor Networks. *Wireless Personal Communications*. 2019;105(4):1475–1490. Available from: https://dx.doi.org/10.1007/s11277-019-06155-x. doi:10.1007/s11277-019-06155-x.
3) Li T, Liu W, Wang T, Ming Z, Li X, Ma M. Trust data collections via vehicles joint with unmanned aerial vehicles in the smart Internet of Things. *Transactions on Emerging Telecommunications Technologies*. 2020. Available from: https://dx.doi.org/10.1002/ett.3956. doi:10.1002/ett.3956.
4) Sun HM, Chen CM, Hsiao YC. An efficient countermeasure to the selective forwarding attack in wireless sensor networks. *IEEE TENCON*. 2007;p. 1–1. doi:10.1109/TENCON.2007.4428866.
5) Bar RK, Mandal JK, Singh MM. QoS of MANet Through Trust based AODV Routing Protocol by Exclusion of Black Hole Attack. *Procedia Technology*. 2013;10:530–537. Available from: https://dx.doi.org/10.1016/j.protcy.2013.12.392.
6) Satyajayantmisra K, Bhattarai G, Xue. BAMBi: Blackhole Attacks Mitigation with Multiple Base Stations in Wireless Sensor Networks. *the IEEE International Conference on Communications (ICC)*. 2011;p. 1–5.
7) Kompella RR, Yates J, Greenberg AA, Snoeren AC. Detection and Localization of Network Black Holes. *IEEE INFOCOM 2007 - 26th IEEE International Conference on Computer Communications*. 2007;p. 2180–2188. doi:10.1109/INFCOM.2007.252.
8) Yasin A, Zant MA. Detecting and Isolating Black-Hole Attacks in MANET Using Timer Based Baited Technique. *Wireless Communications and Mobile Computing*. 2018;2018:1–10. Available from: https://dx.doi.org/10.1155/2018/9812135.
9) Panda N, Pattanayak BK. Defense Against Co-Operative Black-hole Attack and Gray-hole Attack in MANET. *International Journal of Engineering & Technology*. 2018;7(3.4):84–84. Available from: https://dx.doi.org/10.14419/ijet.v7i3.4.16752.
10) Jiang B, Huang G, Wang T, Gui J, Zhu X. Trust based energy efficient data collection with unmanned aerial vehicle in edge network. *Transactions on Emerging Telecommunications Technologies*. 2020;p. 3942–3942. Available from: https://dx.doi.org/10.1002/ett.3942.
11) Priayoheswari B, Kulothungan K, Kannan A. Beta Reputation and Direct Trust Model for Secure Communication in Wireless Sensor Networks. *Proceedings of the International Conference on Informatics and Analytics*. 2016;73:1–11. Available from: https://doi.org/10.1145/2980258.2980413.
12) Airehrour D, Gutierrez J, Ray SK. GradeTrust: A secure trust based routing protocol for MANETs. In: 2015 International Telecommunication Networks and Applications Conference (ITNAC). IEEE. 2015;p. 65–70. doi:10.1109/ATNAC.2015.7366790.
13) Wang T, Zhang G, Yang X, Vajdi A. A Trusted and Energy Efficient Approach for Cluster-Based Wireless Sensor Networks. *International Journal of Distributed Sensor Networks*. 2016;12(4):3815834–3815834. Available from: https://dx.doi.org/10.1155/2016/3815834. doi:10.1155/2016/3815834.

14) Raza S, Haider W, Durrani NM, Khan NK, Abbasi MA. Trust Based Energy Preserving Routing Protocol in Multi-hop WSN. In: Networked Systems;vol. 9466. Springer International Publishing. 2015;p. 518–523. doi:10.1007/978-3-319-26850-7_42.
15) Qin D, Yang S, Jia S, Zhang Y, Ma J, Ding Q. Research on Trust Sensing Based Secure Routing Mechanism for Wireless Sensor Network. *IEEE Access*. 2017;5:9599–9609. Available from: https://dx.doi.org/10.1109/access.2017.2706973.
16) Ahmed A, Bakar KA, Channa MI, Haseeb K. Countering Node Misbehavior Attacks using Trust Based Secure Routing Protocol. *TELKOMNIKA (Telecommunication Computing Electronics and Control)*. 2015;13(1):260–260. Available from: https://dx.doi.org/10.12928/telkomnika.v13i1.1181.
17) Perkins CE, Royer EM. Ad-hoc on-demand distance vector routing. In: Proceedings WMCSA'99. Second IEEE Workshop on Mobile Computing Systems and Applications. IEEE. 1999;p. 90–100.
18) Heinzelman WR, Chandrakasan AP, Balakrishnan H. Energy-efficient communication protocol for wireless microsensor networks. In: Proceedings of the 33rd Annual Hawaii International Conference on System Sciences. IEEE Comput. Soc. 2000;p. 3005–3014.
19) Muzammal SM, Murugesan RK, Jhanjhi NZ. A Comprehensive Review on Secure Routing in Internet of Things: Mitigation Methods and Trust-Based Approaches. *IEEE Internet of Things Journal*. 2021;8(6):4186–4210. Available from: https://dx.doi.org/10.1109/jiot.2020.3031162.
20) Audunjosang. Artificial Reasoning with Subjective Logic. *Appears in the Proceedings of the 2nd Australian Workshop on CommonsenseReasoning*. 1997. doi:10.1.1.614.5935.

Wireless Personal Communications
https://doi.org/10.1007/s11277-021-08094-y

# Dilated Transaction Access and Retrieval: Improving the Information Retrieval of Blockchain-Assimilated Internet of Things Transactions

**G. Amudha**[1]

Accepted: 10 January 2021


**Abstract**
Blockchain technology is designed to improve the security features and information access of a transaction in a connected Internet of Things platform. The private information retrieval from the transactions using blockchain improves the quality of experience through systematic assessments. However, the information retrieval from the fore-gone transaction does not result in maximum profit due to time and sequence of transactions. This article introduces a dilated transaction access and retrieval method. The proposed method identifies the transaction history based on the non-replicated identity and recursive organization of the block. A non-recurrent binary searching process assists information access and retrieval randomly. The random process increases the time, and therefore, a transaction-time constraint is used to limit the number of random searches. In this method, multi-random searches are initiated in a branched manner for identifying the block. Pursued by this access, the relevance based retrieval is performed to improve the correctness of transaction assessment.

**Keywords** Blockchain · Information access · Internet of things · Non-recurrent learning · PIR

## 1 Introduction

Blockchain in IoT is used to prevent data replication that malicious user attacks in the network. Blockchain is a digital-based technology that utilizes the number of blocks to store the user transaction and ID [1]. In this manner, the evaluation is determined by processing each block to obtain the relevant result. In the IoT environment, blockchain is used to retrieve the necessary information from many blocks [2]. The identification is processed by user ID, where the histories of transactions are determined and provide the result. Here, the transaction record is evaluated in two private and public blockchain types, used between the user and IoT applications [3–5]. Many approaches are developed to derive the

✉ G. Amudha
amudha_guna@yahoo.co.in

[1] Computer Science and Engineering, R.M.D. Engineering College, Kavaraipettai, India

blockchain from retrieving the information in a time-efficient manner. For every processing of data and acquiring, the time limit is allocated; here, the evaluation of time is determined to derive the blockchain's data. Mostly blockchain used in IoT addresses and enhances scalability, privacy, and reliability [6–8].

Private Information Retrieval (PIR) is used to acquire the user's query and processes the computation steps to retrieve the blockchain's data. The PIR is defining as the user query for a particular process, and the server acquires the data and distributes the query independently [9]. By processing this user who is not a query for the particular service, access the data gets the time constraint addressed [10]. The PIR is an efficient method that decreases communication and information sharing between the user and the server. In this manner, the server searches for the request related service block and retrieves the relevant information [11, 12]. The information is processed based on matching time, which is used to acquire the data reliably. Here time-based PIR is used to improve the system's performance, whereas communication is also addressed [13]. As the name suggests, private related information is accessed and prevents unauthorized users from accessing the block. The protection of data is necessary to derive private information from the blockchain [14].

A blockchain transaction is tracked to secure the information in the block and acquires the relevant information. For every transaction, the ID and time-based processing are monitored to retrieve the queried user data [15–17]. This user query for the data and the server search with the blockchain and acquires the data by matching it promptly. Thus, the transaction is monitored efficiently and provides information regarding the multi-search user [18]. It uses the cryptography method to secure the transaction from the malicious user and decides the transaction [19]. The decision is derived based on the history of the transaction and provides the necessary information. For avoiding transaction risk, unnecessary data retrieval is minimized by proposing certain algorithms. The proposed work aims to increases the information retrieval rate and decreases retrieval time by introducing DTARM. Using this method, the correctness of transaction assessment is achieved by processing the pruning tree classification algorithm.

## 2 Related Work

Yang presented a **B**lockchain-based **m**ulti-keyword ranked search with **f**air **p**ayment (BMFP) to address the cost-efficient process. The ranking of data is performed in the cloud-based environment by integrating the verification algorithm. The verification is used for correctness and completeness.

Task Matching in Crowdsourcing is developed to improve security and feasibility based on privacy-preserving. Wu et al. [20] proposed a Blockchain task matching to deploy the cloud server and enhance efficiency and efficiency. It is processed in smart contracts to achieve better confidentiality and identity anonymity.

A trust-based Blockchain is developed by Yu et al. [21] to achieve reliable blockchain-based to the user and access the data by utilizing DNS. In this work, two types of processing are performed: a peer-to-peer network used to decrease unauthorized access. The second indicates the determining of nodes that utilize the system's free-riding behavior and improve the performances.

Named Data Networking (NDN) is modeled to retrieve the trusted content and security to the data [22]. Smart Contract-based Trusted Content Retrieval Mechanism (SCTCRM) is

developed for NDN to achieve trustworthy information. The analysis is used to finds the storage and gas in smart contracts.

Xue and Lu [23] presented a semantic differential transaction (SDT) to reduce information redundancy by processing BIM and blockchain integration. The objective of this work is to address the operable Blockchain building information modeling (BIM) systems. It is derived by introducing a BIM change contract (BCC).

Pattengale and Hudson [24] proposed a MultiChain*stream* application programming interface to deploy two levels catalog. By processing, these heuristic and binary search techniques are used efficiently to query the user. Thus the evaluation is computed in the allocated timestamp that decreases the complexity.

A cross-site genomic dataset access audit is implemented by Ma et al. [25] to improve the processing time and space-efficient. It is developed to resolve the indexing unassailable in the Blockchain system and enhance the query's speed. For this, the author presented two types of methods, such as baseline and enhanced method.

Tian et al. [26] presented secure digital evidence to provide stability in privacy and traceability. It uses a loose coupling structure to save the data in a trusted platform, derives the multi-signature technique, and retrieves the evidence. By proposing a mixed Blockchain, fault tolerance is reduced.

Farrugia et al. [27] address three sets of evaluations, such as 'Time diff between first and last (Mins),' 'Total Ether balance,' and 'Min value received. The scope of this paper is to find the illicit accounts and their transaction history efficiently on the Ethereum network. XGBoost classifier is used to improve the accuracy of the system.

A blockchain-based private keyword search is developed to decreases retrieval privacy and provides the guarantee of service [28]. Oblivious keyword search (OKS) is designed to retrieve the data based on the keyword; for this process, one-keyword restriction and public-key encryption with keyword search (PEKS) are deployed. By deriving this, bandwidth consumption is addressed and resolved.

Blockchain-based access control is introduced by Wang et al. [29] to evaluate this author introduced the Ethereum blockchain and ciphertext-policy attribute-based encryption (CP-ABE) method. The objective of this work is to improve the feasibility and security of the system. In this access, time is observed and evaluates the valid user.

Construction quality information management is developed by Zhong et al. [30] to resolve the deception information. The lifecycle and permission of data determine a consortium blockchain system. For this, a trust-based mutual model is determined and processed the application in the province of management.

Clarke et al. [31] presented a European Patent Office (EPO) to find false positives based on prioritized data that determines the relevant information. To find the Blockchain parent document, the author introduced two methods: unique methodology and specific search strategy.

Li et al. [32] implemented a trust-enhanced blockchain-based ICN (BICN) to address proper content delivery for end-user. In this paper, the security level is increased and prevents malicious nodes in the network, which is evaluated by determining the human-readable name and self-certifying name.

## 3 Proposed Method

Blockchain is a technique used to secure the data in a heterogeneous platform by processing some authentication methods. In this, communication and information sharing are monitored by blockchain for every particular time interval. By processing this, it monitors the number of transactions and number of transaction IDs of the user and derives a similar time from the split block. In Fig. 1, the blockchain process for the proposed method is illustrated.

The splitting is evaluated based on several blocks; thus, it is processed by dividing the sub-blocks. This work aims to improve the information retrieval rate and decrease retrieval time, which is processed by introducing DTARM. In Table 1, the symbols used in the article are described.

The following Eq. (1) is used to monitor the user's transaction history and ID, where it is easy to find the user's query lies in which block. Here it acquires the user's information, monitors the activity in a mentioned time, and derives similar data.

$$\mathbb{M}_0 = \prod_{b'}^{\mathcal{E}} (\mathcal{U}' + \mathcal{Q}_0) * \left[ \left( \frac{\mathcal{P}' + \mathcal{T}'}{\mathfrak{r}_0 - \mathcal{R}} \right) + \sum_{\frac{\mathcal{E}}{\mathcal{A}_0}}^{\mathcal{S}'} (\mathcal{C} + i') - \mathcal{T}' * \sqrt{\left( \frac{\mathcal{R} + \frac{d_0}{\mathfrak{M}}}{\mathcal{S}'/\mathfrak{t}} \right)} \right] + \left( \mathfrak{G} + \left( \frac{\mathcal{T}' + \mathfrak{t}}{\mathfrak{X}} \right) \right) * \prod_{\mathcal{D}'}^{d_0} (s' + \mathfrak{A}) - s_0 \tag{1}$$

The data are monitored which is represented as $\mathbb{M}_0$ based on the number of blocks and it is determined by processing $\sqrt{\left( \frac{\mathcal{R} + \frac{d_0}{\mathfrak{M}}}{\mathcal{S}'/\mathfrak{t}} \right)}$ in this non-replication, data are derived as $\mathcal{R}$.

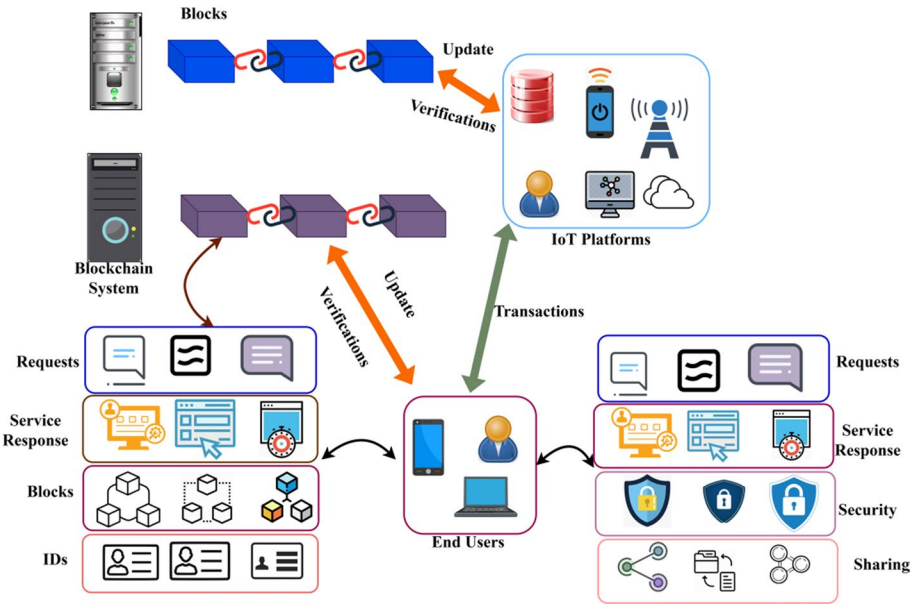



**Fig. 1** Proposed method

**Table 1** Symbols and description

| Symbols | Description | Symbols | Description |
|---|---|---|---|
| $\mathbb{M}_0$ | Monitoring instance of the transaction | $\mathcal{C}$ | Content similarity factor |
| $\mathcal{U}'$ | User | $\mathfrak{M}$ | Successful retrieval count |
| $\mathcal{E}$ | Blockchain identification | $\mathcal{D}'$ | Retrieval discard count |
| $\mathcal{Q}_0$ | Query | $\mathfrak{C}$ | Communication instances in a matching time |
| $\mathcal{T}'$ | Processing time | $i'$ | Information sharing interval |
| $\mathfrak{r}_0$ | Replication factor | $\mathfrak{X}$ | Similarity recognizaiton instance |
| $\mathcal{R}$ | Non-replication factor | $\mathfrak{A}$ | Data analysis count |
| $\mathcal{S}'$ | Searching count of the data | $b'$ | Blocking probability |
| $\mathcal{A}_0$ | Access request | $d_0$ | Data representation (similar and unsimilar) |
| $\mathbb{t}_0$ | Matching time | $s'$ | Unsimilarity factor |
| $\mathfrak{t}$ | Transaction | $s_0$ | Similarity factor |
| $\mathcal{I}'$ | ID | $\mathfrak{S}'$ | Classification count |
| $\mathcal{P}'$ | Number of block split | | |

Replication data are derived as $\mathfrak{r}_0$ by computing data which is termed as $d_0$ where it retrieves the similar data is denoted as $\mathfrak{M}(s_0)$. This searching is achieved by processing the data in the appropriate time $\mathcal{T}'$. It includes transaction and ID of the data that is referred to as $\mathfrak{t}$ and $\mathcal{I}'$ where it analysis similar content based on retrieval that is represented as $\mathcal{C}$. Blockchain is used to encrypt data through some authentication mechanisms on a heterogeneous network. Blockchain tracks this correspondence and knowledge exchange for each unique interval. It tracks the number and number of transaction IDs of the user and extracts equivalent time from the split block by processing it.

The monitoring is processed based on communication and information sharing, which is denoted as $\mathfrak{C}$ and $i'$ thus the analysis $\mathfrak{A}$ is recognized in the blockchain that is represented as $\mathcal{E}$ and $\mathfrak{X}$. Therefore, access is referred to as $\mathcal{A}_0$ to process the query from the split data that is termed as $\mathcal{Q}_0(\mathcal{P}')$. It splits the similar and dissimilar data that is represented as $s'$ and $s_0$ from the block $b'$ and provides the service to the user, which is denoted as $\mathcal{U}'$. It discards the non-match data, which is denoted as $\mathcal{D}'$ from the non-replications data. Thus, the monitoring of blockchain is processed, and it splits the number of transactions and ID given as the input for the pursuing equation. The data splitting is derived as the output, which is used to differentiate similar and dissimilar data.

$$\mathcal{P}' = \left[\sqrt{\left(\frac{\mathcal{S}' + s_0}{\sum \frac{d_0}{\mathcal{A}_0}}\right)} * \sum_{\mathfrak{A}}^{\mathcal{C}} \left(\mathcal{Q}_0 + \mathcal{U}'\right)\right] - \mathcal{T}' * \prod_{\mathfrak{C}}^{i'} \left(\mathfrak{t} + \mathcal{I}'\right) * \left[\left(\frac{\mathbb{M}_0}{b' + \mathfrak{A}}\right) + \left(\frac{\mathfrak{r}_0 - \mathcal{R}}{\frac{(\mathcal{A}_0 * \mathfrak{M})}{d_0}}\right)\right] + \left(\mathcal{E} * \frac{\mathfrak{X}}{\mathcal{U}'}\right) - \mathbb{t}_0 * \sum_{\mathcal{S}'}^{\mathfrak{M}} (d_0 + \mathcal{A}_0) \tag{2}$$

From the monitored data in Eq. (1), is given as the input for the above equation, where the data split is performed to differentiate the replication and non-replication data and retrieves the process from the query which is the output for this process. In the above equation, the searching is achieved efficiently where the monitoring of blockchain is derived. The process of information split is illustrated in Fig. 2. Thus the tracking of block chain is processed, and it divides the number of transactions and ID which is given as the input for

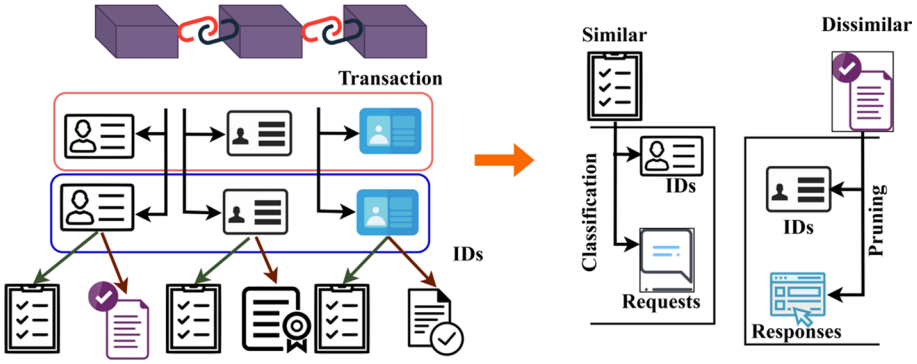



**Fig. 2** Process of information split

the pursuing equation. The data splitting is derived as the output and is used to separate identical and dissimilar data.

The information is retrieved based on transaction and ID in the block. By computing $\left(\frac{\mathfrak{r}_0-\mathcal{R}}{(\mathcal{A}_0*\mathfrak{M})/d_0}\right)$ the splitting is processed by accessing similar data based on time; thus, the analysis is used for multi-search. The following Eq. (3) is formulated to perform the pruning tree for classification of ID and transaction and matches the common information in the block. The tracking is conducted based on information and contact as known in the blockchain. Access to the query from the separated data is referred to as the same, which separates data defined by block b' and delivers the customer's service. It rejects non-corresponding data as denoted as non-replication statistics. Thus, blockchain tracking is processed, and the number of transactions and ID that are presented as the input for the search equation is divided. The division of data is obtained as the outcome used to separate identical and different data.

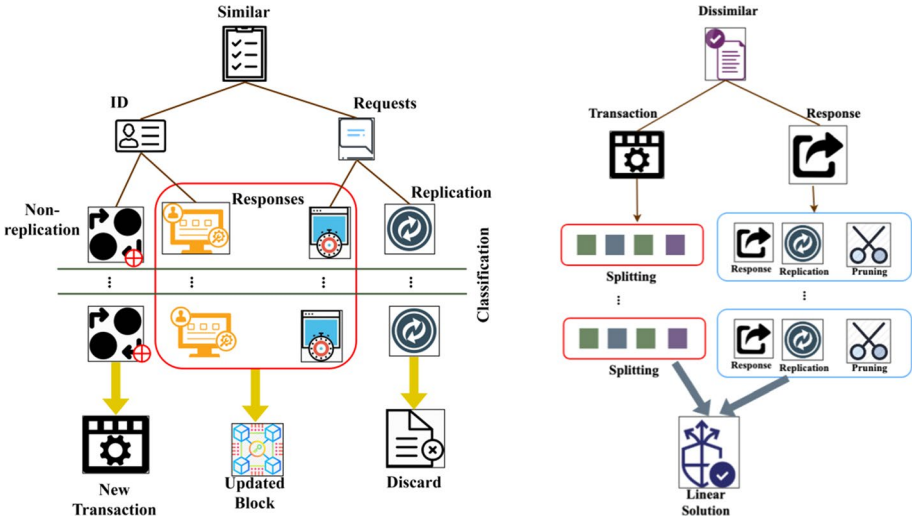
### 3.1 Pruning Process

The pruning tree is processed based on a top-down approach where the root nodes are subdivided into the child node; in this work, the root node is defined as blockchain, whereas the child node is denoted as several blocks. Post to the data splitting, the accurate results is evaluated by processing pruning, where it divides the blocks as the nodes. From the child node, the sub-node is separated and processed, which includes transaction and ID. This process's scope analyzes no block produced from the child node, whereas dissimilar data are avoided. It is computed in the below Eq. (3), where the top-down pruning tree classification is derived.

$$\mathfrak{S}' = \begin{cases} \prod_{\mathfrak{A}}^{d_0}\left(\mathcal{E}+b'\right) * \left[\left(\frac{\mathcal{S}'+s_0}{\mathcal{Q}_0/\mathbb{M}_0}\right) - \mathcal{T}'\right] + \left(\mathcal{A}_0 + \frac{i'}{\mathfrak{C}}\right) = \begin{cases} \Sigma\left(\frac{\mathfrak{M}}{\mathbb{t}_0} - \mathcal{T}'\right) + \left(\sqrt{\frac{\mathcal{E}-\mathfrak{A}}{\mathcal{R}+d_0/\mathcal{U}'}}\right) \\ \left(\frac{\mathcal{D}'-\mathbb{t}_0}{\sum_{\mathcal{T}'}(\mathfrak{C}+i')}\right) * \prod_{\mathcal{I}'}^{\mathbb{t}}(d_0 - \mathcal{D}') \end{cases} \\ \left[\sqrt{\left(\frac{\left(\frac{\mathcal{U}'}{\mathfrak{A}*d_0}\right)}{\sum_{\mathfrak{M}}^{d_0}(\mathbb{t}+\mathcal{I}')}\right)} * \left(\frac{\mathcal{A}_0}{\sum_{\mathcal{U}'}^{\mathcal{T}'}(s'-\mathfrak{A})}\right)\right] + \prod_{\frac{\mathcal{T}'}{\mathcal{E}}}^{\mathcal{Q}_0}(\mathcal{R}+\mathbb{M}_0) = \begin{cases} \left(\frac{\mathcal{C}+\mathfrak{M}}{\mathcal{R}/\mathcal{Q}_0+\mathcal{A}_0}\right) * \sqrt{(\mathcal{S}'+s_0)} - (\mathbb{t}_0 - \mathcal{D}') \\ \prod_{\mathbb{t}}^{\mathcal{T}'}\left(\mathfrak{A} * \frac{\mathcal{C}-\frac{b'}{\mathfrak{M}}}{\mathbb{M}_0}\right) + \mathcal{D}' - (\mathcal{Q}_0 + d_0) \end{cases} \end{cases} \tag{3}$$

The classification tree is represented as $\mathfrak{S}'$.The processing is based on right and left child nodes, divided using Eq. (3). The first derivation is divided into sub-nodes, where the dissimilar information in the block is discarded. By computing $\left[\left(\frac{\mathcal{S}'+s_0}{\mathcal{Q}_0/\mathbb{M}_0}\right) - \mathcal{J}'\right]$ The time-based query is processed and form that dissimilar data are analyzed. Again the processing is carried out by extracting the non-replication data. It is used to make the processing step easier, whereas the second derivation has the other side of the child from the root node. Here, it derives the output whether the child node has any leaf node or not used to monitor the replication and non-replication data. In Fig. 3a, b, the pruning tree initialization for similar and dissimilar data is presented. The tail tree is processed on the basis that the root node is subdivided into the child node. The root node is represented as a blockchain in this job, while the child node is denoted as many blocks. Posting the findings separating the data is assessed by the sorting, in which blocks as nodes are separated. The sub-node, which involves transaction and recognition, is separated and processed from the child node.

From that sub-division $\left(\mathfrak{A} * \frac{\mathcal{C}-\frac{b'}{\mathfrak{M}}}{\mathbb{M}_0}\right) + \mathcal{D}'$ it discards the data which are analyzed. Thus the first subdivision is processed as $\sqrt{(\mathcal{S}'+s_0)} - (\mathbb{t}_0 - \mathcal{D}')$ in this searching is achieved by evaluating $\sqrt{\left(\frac{\left(\frac{\mathcal{U}'}{\mathfrak{A}*d_0}\right)}{\sum_{\mathfrak{M}}^{d_0}(\mathbb{t}+\mathcal{I}')}\right)}$ where the user request query is processed; here,




**(a) Similar Data** **(b) Dissimilar Data**

**Fig. 3** **a** Similar data. **b** Dissimilar data

the transaction and ID are retrieved in the allocated time. This classification is obtained based on the left and right side of the root node. The sub-division of the nodes is derived from the root. Thus, the matching of similar data is obtained from the sequential model and derives the linear based model where the classification of similar and dissimilar information is analyzed in the following Eq. (4). It fetches the input from the pruning tree, where it detects the replication and non-replication data, and the analysis is processed based on the transaction ID of the user. The derivation is divided into sub-nodes in which the separate knowledge is discarded in the block. The time-based query is analyzed to evaluate different results. Again, non-replication data are processed by extraction. The second derivation of the child from the root node is used to simplify the processing stage. In this case, the output is generated on whether or not the child node has a leaf node used to track replication and non-replication data.

$$\begin{aligned}\mathfrak{A} = &\left(\frac{\mathcal{Q}_0 + \mathcal{A}_0}{b'}\right) * \left\{\left[\sum_{\mathcal{R}}^{\mathcal{U}'}(\mathcal{S}' + (s' - s_0)) * \left(\frac{\mathfrak{t} + \mathcal{T}'}{\mathfrak{X}/\mathfrak{C} + i'}\right)\right] - (\mathfrak{X} + \mathfrak{M})\right. \\ &\left. + \left[\int_{\mathcal{D}'}^{s'}(d_0 + b') * \left(\frac{\mathcal{S}' + \mathcal{U}'}{\mathcal{C}}\right) + \mathfrak{M}\right]\right\} * \prod_{\mathcal{R}}^{d_0}(\mathcal{A}_0 + \mathcal{Q}_0) * \left(\frac{\mathfrak{t} + \mathcal{T}'}{\mathbb{M}_0}\right) \\ &+ \sqrt{\left(\frac{\frac{\mathcal{R}}{\mathbb{t}_0}}{\mathfrak{X}/\mathfrak{M}}\right)} - \left\{\left[\sum_{\mathcal{C}}^{\mathfrak{M}+d_0}(\mathcal{U}' + \mathcal{Q}_0) * \left(\frac{s' - s_0}{\mathcal{S}'/i'}\right)\right] - (\mathcal{A}_0 + \mathcal{U}') * \left[\sum_{d_0}^{\mathcal{E}}(\mathbb{t}_0 * \mathcal{C}) + \mathfrak{S}'\right]\right\} - \mathfrak{t}\end{aligned} \tag{4}$$

The analysis is processed in the above Eq. (4), where it acquires the number of transactions and ID of the user and integrates similar data in the block. Form the linear model; the similar data are computed as $\left(\mathfrak{s}' - \mathfrak{s}_0\right) * \left(\frac{\mathfrak{t}+\mathcal{T}'}{\mathfrak{X}/\mathfrak{C}+i'}\right)$ in this, the transaction and ID are processed based on the communication and information sharing with the user. It is based on the content similarity that must match the time instance in the processing steps where there are derived by $\left(\mathcal{A}_0 + \mathcal{Q}_0\right) * \left(\frac{\mathfrak{t}+\mathcal{T}'}{\mathbb{M}_0}\right)$ in this, the analysis is based on a query from the user for the data estimation. From Eq. (4), the research is processed by deploying a linear model that is processed by the user query. This derivation is provided as the input to find the replication data. Thus, the following Eq. (5) is derived to evaluate the non-replication data from the transaction history, which is the output for this equation. The division of roots is derived from both the left and right sides of the root node. The match of related data is then derived from the sequential model. It derives from the linear model where the grouping of similar and different data in the following equation is evaluated. The information is obtained from the prune tree, where the replicative and non-replicative data are detected, and the processing is done according to the user's transaction ID.

$$\begin{aligned}\mathcal{R} = &\sum_{\mathfrak{t}}^{\mathcal{T}'}\left[\left(\mathcal{P}' * d_0 + \mathcal{A}_0\right) - \mathcal{T}' + \left(\left(\frac{\mathcal{C} * \mathfrak{M}}{\mathcal{S}'}\right) * \left(\frac{\mathcal{S}'}{i' + \mathfrak{C}}\right)\right)\right] \\ &- \prod_{\mathcal{A}_0}^{\mathcal{Q}_0}(s_0 - \mathfrak{S}') + \left(\frac{\mathcal{Q}_0}{b'/\mathcal{E}}\right) * \left(\mathcal{S}' + d_0\right) + \mathbb{t}_0\end{aligned} \tag{5}$$

Replication data are divided into the blockchain, and it is processed based on the transactions and their ID; thus, it is computed by evaluating $\left(\frac{\mathcal{C}*\mathfrak{M}}{\mathcal{S}'}\right) * \left(\frac{\mathcal{S}'}{i'+\mathfrak{C}}\right)$ here the retrieval of data similar content is achieved. In this time-based processing is formulated as

$\left(\mathcal{P}' * d_0 + \mathcal{A}_0\right) - \mathcal{T}'$ where the data are split by utilizing the query from the user. In this derivation, replication-based data is acquired from the transaction history, where the user's relevant information is stored and retrieved for user access. Access is provided to the user based on the similarity of the transaction; for this the following equation is used to identify the similarity data. Here, it fetches the output of the previous equation and provides as the input for this processing. Thus, the similarity is processed by linear tree classification. It is derived in the following Eq. (6) and produces the result by monitoring the transaction from the user query in an optimal manner. The data that are examined by this subdivision. The first subdivision is processed by analyzing the user request query; the transaction and ID are obtained here in the specified period. The division of roots is derived from the root. This designation is obtained on both left and right side of the root node.

$$\mathcal{A}_0 = \left.\begin{array}{l} \sqrt{\left(\frac{\mathcal{E}+\mathbb{M}_0}{\mathcal{R}+d_0}\right)} * \left(\frac{\mathfrak{t}+\mathcal{I}'}{\sum_{\mathcal{U}'}\left(\mathcal{Q}_0+d_0\right)}\right) + \left(\frac{\mathcal{S}'}{\mathbb{t}_0-\mathcal{T}'}\right) \\ \prod_{b'}^{\mathcal{E}}\left(\mathcal{P}' * \mathfrak{M}\right) + \left(\frac{\mathfrak{A}}{\mathfrak{C}+i'}\right) - \sum_{\mathcal{D}'}\left(\mathcal{U}' + \mathcal{Q}_0\right) * \left(\frac{s_0}{\mathcal{S}'+d_0}\right) \end{array}\right\} \tag{6}$$

The access is provided by formulating the above Eq. (6); based on this, the Blockchain process the user's relevant information. By computing $\left(\frac{\mathfrak{t}+\mathcal{I}'}{\sum_{\mathcal{U}'}\left(\mathcal{Q}_0+d_0\right)}\right) + \left(\frac{\mathcal{S}'}{\mathbb{t}_0-\mathcal{T}'}\right)$ The transaction is monitored based on user query, and retrieves the data in this searching are derived by processing data matching. The dissimilar data are discarded from the block, and it is evaluated by formulating $\left(\mathcal{U}' + \mathcal{Q}_0\right) * \left(\frac{s_0}{\mathcal{S}'+d_0}\right)$ here the processing is acquired based on searching similar data. Post to this process the classification pruning tree is derived by computing the blockchain and split into several blocks given in the below Eq. (7). This derivation incorporates replication-based data from the past of the transaction, storing and retrieving user-access related information. The user accesses based on the similarities of the transaction to define the similarity details using the next equation. Here the output for the previous equation is defined and the processing input is given.

$$\begin{aligned} \mathcal{P}'\left(b'\right) = &\left[\sum_{\mathcal{C}}^{\mathcal{A}_0}\left(\mathbb{t}_0 + \mathcal{T}'\right) * \left(\frac{\mathfrak{C} * \mathcal{U}'}{\mathfrak{M} + d_0}\right) + \mathbb{M}_0 * \prod_{\mathcal{E}}^{\mathfrak{A}}\left(\mathfrak{S}' + s_0\right) - \mathbb{t}_0 + \left(\frac{d_0 + s_0}{i'/\mathfrak{t} + \mathcal{E}}\right)\right] \\ &+ \left[\left(\frac{\mathcal{Q}_0}{\mathcal{S}' + d_0}\right) * \prod_{\mathcal{T}'}^{\mathcal{C}}\left(\mathfrak{X} + d_0\right) - \mathfrak{S}' + \left(\frac{\mathbb{M}_0}{i' + \mathcal{U}'}\right) - \mathbb{t}_0\right] \end{aligned} \tag{7}$$

From Eq. (6), the access is produced to the user with the similar data is given as the input for this above equation where it derives the output by splitting the blocks to make the processing easier. If the user requests the query, similar data is retrieved where it increases the co-relation factor. The blockchain classification is derived as $\mathcal{P}'\left(b'\right)$ in this, it is computed as $\left(\mathfrak{S}' + s_0\right) - \mathbb{t}_0$ here the similar data are classified using a tree. By acquiring the query, the processing is done accordingly to the user query that is formulated as $\left(\mathbb{t}_0 + \mathcal{T}'\right) * \left(\frac{\mathfrak{C} * \mathcal{U}'}{\mathfrak{M} + d_0}\right)$ here the user evaluates the required block and determines the data. The blockchain update process is portrayed in Fig. 4.

Based on the query, the block is defined, and thus it is monitored based on the requirement where it satisfies the timely manner of data processing. In Table 2, the block split for the different transactions is tabulated.

Thus, the blockchain classifies the number of blocks with several transactions and ID based on this, and the searching is performed by evaluating the following Eq. (8).

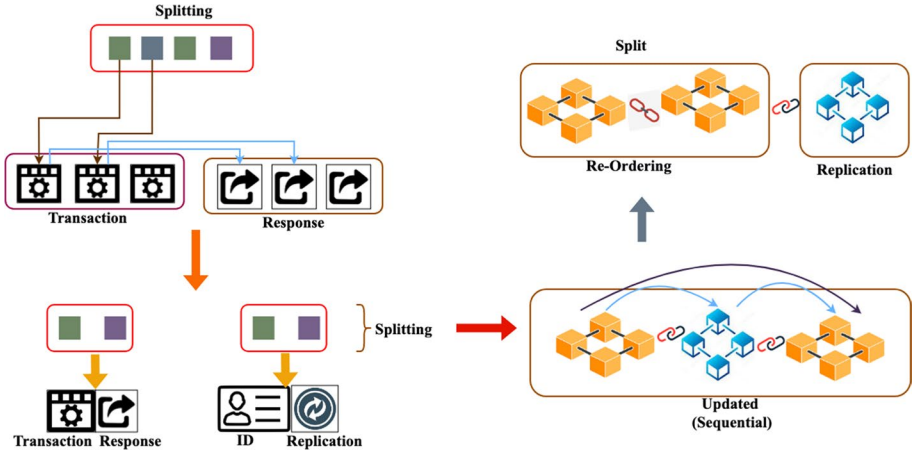



**Fig. 4** Blockchain update process

**Table 2** Block split rate

| Transactions | Similar data (%) | Dissimilar data (%) | Blocks | Split rate |
|---|---|---|---|---|
| 100 | 77.82 | 26.82 | 2 | 0.957 |
| 150 | 79.14 | 25.91 | 5 | 0.918 |
| 200 | 81.11 | 25.66 | 5 | 0.859 |
| 250 | 83.45 | 21.94 | 5 | 0.854 |
| 300 | 85.43 | 19.79 | 7 | 0.826 |
| 350 | 88.34 | 17.43 | 8 | 0.818 |
| 400 | 89.43 | 14.96 | 4 | 0.767 |
| 450 | 90.59 | 13.4 | 4 | 0.753 |
| 500 | 91.96 | 11.5 | 4 | 0.737 |
| 550 | 92.17 | 11.22 | 8 | 0.732 |
| 600 | 92.44 | 10.46 | 9 | 0.718 |
| 650 | 92.59 | 9.09 | 9 | 0.659 |
| 700 | 93.04 | 2.41 | 10 | 0.601 |

$$\mathcal{S}' = \prod_{\mathcal{R}}^{\mathcal{U}'}\left[(d_0 + b') - \left(\mathcal{T}' * \frac{\mathfrak{M} + \mathfrak{X}}{\mathfrak{t}}\right)\right] + \int_{\mathfrak{A}}^{b'}\left[(\mathfrak{C} * \mathcal{U}') + (\mathfrak{t} + \mathcal{I}')\right] * \left(\frac{\sum \mathfrak{S}' * \frac{b'}{d_0}}{\sum_{\mathcal{A}_0} \mathcal{P}' + s_0}\right) + \left[\prod_{\mathbb{M}_0}^{\mathcal{E}}(b' + \mathcal{Q}_0) * \left(\mathcal{I}' + \frac{\mathfrak{C} + \mathcal{U}'}{\mathcal{C}}\right)\right] - (\mathfrak{M} - \mathcal{A}_0) \tag{8}$$

In Eq. (7), the splitting of the block is computed based on this searching is performed in the above equation, and it is represented as $\mathcal{S}'$. It is computed to maintain the reliable data to the requested user where the evaluation is processed as $(d_0 + b') - \left(\mathcal{T}' * \frac{\mathfrak{M}+\mathfrak{X}}{\mathfrak{t}}\right)$ in this, the data are monitored in the split block and search for the required information. Thus, by

computing $\left(\frac{\sum \mathfrak{S}' * \frac{b'}{d_0}}{\sum_{\mathcal{A}_0} \mathcal{P}' + s_0}\right)$ the classification is determined based on split data and monitors a similar set of information. Here searching is achieved at the optimal rate where it determines the query from the user and processes the ID and transaction based on history. Post to this searching, it delivers the output for the queried user, it finds the data relies on which block is given as the input for the below equation. Processing this produces the output by making similar and dissimilar data that is performed by processing recognized. Different data are stored and evaluated on a time-dependent basis. The procedure is again performed using the non-replication data extracted. The second derivation comes from the other side of the child from the root node. It is used to make processing more simple. The consequence is whether the child node has or does not have a leaf node used to track replication and non-replication results.

$$\mathfrak{X} = \begin{cases} \sqrt{\left(\frac{\mathcal{C}+d_0-b'(\mathbb{M}_0)}{\sum_{\mathbb{Q}_0}(\mathcal{U}'+\mathcal{A}_0)}\right)} + \prod_{\mathcal{R}}^{d_0}\left(\mathbb{M}_0+\mathcal{C}\right) - \mathfrak{A} * \left(\mathfrak{t}+\mathcal{I}'\right) = s_0 \\ \left(\frac{\left(\mathfrak{C}+\frac{b'}{\mathfrak{S}'}\right)}{(\mathcal{C}+\mathfrak{t})/\frac{\mathbb{M}_0}{\sum_{d_0} b'}}\right) + \prod_{\mathbb{t}_0}\left(\mathbb{M}_0-\mathcal{R}\right) + \left(\mathcal{I}' * \mathcal{E}\right) - \mathcal{A}_0 = s' \end{cases} \tag{9}$$

The recognition of similar and dissimilar data is retrieved based on the user query, and it is obtained by evaluating the above Eq. (9). By computing two conditions, it processes the similarity and dissimilarity, and it states whether it is equal to $s_0$ *and* $s'$. The first derivation satisfies the similarity which is achieved by $\sqrt{\left(\frac{\mathcal{C}+d_0-b'(\mathbb{M}_0)}{\sum_{\mathbb{Q}_0}(\mathcal{U}'+\mathcal{A}_0)}\right)}$ where the monitoring of data is evaluated from the block, the analysis is derived from acquiring the user query and processing the transaction.

The second derivation represents the dissimilarity data that is formulated as $\left(\frac{\left(\mathfrak{C}+\frac{b'}{\mathfrak{S}'}\right)}{(\mathcal{C}+\mathfrak{t})/\frac{\mathbb{M}_0}{\sum_{d_0} b'}}\right)$ The classification is not processed at a similar time; that is, no block-based information matches the query. In this manner, the dissimilarity is derived from the classification based pruning tree method. The dissimilar data is discarded and process with the rest of the information in the block. Thus the recognition is processed to find similar and different data is provided as the input for the Eq. (10) and produces the output by better searching of data in the block.

$$\mathfrak{X}(s_0) = \left(\frac{\left(\mathbb{M}_0 * \frac{\mathcal{Q}_0}{\mathcal{E}}\right)}{\sum_{b'+i'}\left(\mathcal{I}'+\mathcal{U}'\right)}\right) * \prod_{\mathcal{R}}^{\mathcal{I}'}\left(\mathcal{S}'+\mathfrak{t}\right) - \left(\left(\mathbb{t}_0+\frac{\mathcal{C}}{\mathcal{P}'}\right) + \sum\left(\mathcal{A}_0 * \mathcal{I}'\right) + \left(\frac{d_0}{\mathfrak{C}}\right)\right) - i' \tag{10}$$

The similar data are recognized by representing $\mathfrak{X}(s_0)$ in this, the monitoring of user query are acquired and process the data on the number of split blocks. Here the time-based evaluation is determined by computing $\frac{\left(\mathbb{M}_0 * \frac{\mathcal{Q}_0}{\mathcal{E}}\right)}{\sum_{b'+i'}\left(\mathcal{I}'+\mathcal{U}'\right)}$.Here, information sharing is progressed by estimating the search process. The searching includes the previous history of data and determines the matching time for the queried data at the appropriate time. By formulating $\left(\mathcal{A}_0 * \mathcal{I}'\right) + \left(\frac{d_0}{\mathfrak{C}}\right)$ here the access of data is processed and provides the communication link

to the user. From the above equation, the searching is derived optimally to satisfy the matching time, the integration of Eqs. (10) and (9) is used. It evaluates the processing in the below Eq. (11).

$$\mathbb{t}_0(s_0) = \prod_{\mathcal{I}'} \left(\mathfrak{C} + d_0\right) * \left(\frac{\mathcal{Q}_0}{\mathfrak{M}} + \mathcal{R}\right) - \mathfrak{t} * \int \left(\mathcal{C} + \mathcal{T}'\right) * \left(\frac{d_0 + \mathcal{S}'}{\frac{\mathfrak{A}}{i'}}\right) + \left(\frac{\mathcal{C}}{\mathcal{P}'}\right) - \left(\mathbb{M}_0 + \mathcal{C}\right) * \left(\mathcal{I}' * \mathcal{E}\right) - \mathcal{A}_0 \tag{11}$$

The matching is determined based on the timely manner where the query is processed in the blockchain and it is represented as $\left(\mathfrak{C} + d_0\right) * \left(\frac{\mathcal{Q}_0}{\mathfrak{M}} + \mathcal{R}\right)$. Here the retrieval is achieved by computing the ID and transaction of the blocks.They are derived by processing the access to the user. in this equation the matching time is satisfied where the content similarity is provided by equating Eq. (12). Here, it acquires the matching processes' input and computes the resultant content similarity for the queried user. Thus, the similar transaction matching is evaluating at the appropriate time. The searching and retrieval are based on similar content that is denoted in the below Eq. (12). The user question has been tracked with exact details, and the data on the number of separated blocks are analyzed. Here, computation decides the time-based assessment. The quest method calculation advances informational exchange because the search contains the previous data history and determines at the right time the matching time for the queried data.

$$\mathcal{C} = \begin{cases} \sqrt{\left(\mathfrak{X} + d_0\right) * s_0} - \left(\mathcal{T}' + \frac{\mathfrak{t}}{\mathcal{A}_0}\right) + \sum_{\mathcal{R}} \left(\mathfrak{M} * \mathfrak{A}\right) < 1 \\ \prod \left(\mathcal{Q}_0 - \mathfrak{t}\right) * \left(\frac{\mathcal{S}'}{\mathcal{P}' + d_0}\right) + \left(\frac{\mathcal{U}' - i'}{\mathcal{E}/\mathbb{M}_0}\right) - \mathbb{t}_0 > 1 \end{cases} \tag{12}$$

The similarity content is acquired from the linear tree structure, where it is associated with two derivations greater than or lesser than 1. The first derivation is represented as $\sqrt{\left(\mathfrak{X} + d_0\right) * s_0}$ in this, the recognition of blocks is evaluated based on similar data. Figure 5 illustrates the information retrieval process.

The retrieval process is analyzed and derives the process is greater than 1 in this the similarity content is retrieved. The second derivation is denoted as $\left(\frac{\mathcal{S}'}{\mathcal{P}' + d_0}\right) + \left(\frac{\mathcal{U}' - i'}{\mathcal{E}/\mathbb{M}_0}\right)$ in this, the searching is obtained based on monitoring the data in the block. In Table 3, the matching and retrieval rate for the different classification instances is presented.

This blockchain is used to split the number of blocks, search the relevant content, and find data similarity. Thus, the matching is derived in the appropriate time interval, and it acquires the splitting of data and retrieves similar data. This pruning tree is processed to derive the sequential tree to a linear tree to evaluate the split block and retrieve it. Thus, the content similarity is derived from the above equation is the input for the following Eq. (13), where it is used to increases the information retrieval rate.

$$\mathfrak{M} = \left\{ \sum_{\mathcal{S}'}^{\mathcal{A}_0} \left(\mathcal{P}' * \mathcal{E}\right) + \left(\frac{\left(\mathfrak{t} + \mathcal{T}'\right)}{\mathcal{R} - \frac{\mathcal{T}'}{\mathbb{M}_0}}\right) * \left(\frac{\mathfrak{X} + d_0}{b' * \frac{\mathcal{S}'}{\mathbb{t}_0}}\right) + \left(\mathbb{t}_0 - \frac{\mathcal{E} + b'}{\sum \left(\mathfrak{t} + \mathbb{t}_0\right)}\right) * \left(\mathcal{D}' + b'\right) \right\} - \left(s_0 + \mathcal{C}\right) + \mathfrak{A} \tag{13}$$

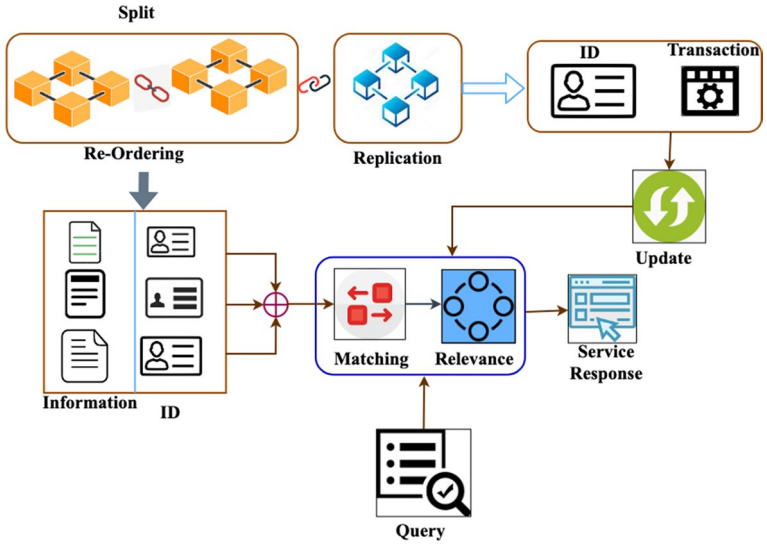



**Fig. 5** Information retrieval process

**Table 3** Matching and retrieval rate

| Classification | Prunes | Left child searches | Right child searches | Matching ratio | Retrieval % |
|---|---|---|---|---|---|
| 0.1 | 7 | 0.499 | 0.511 | 90.447 | 90.201 |
| 0.2 | 10 | 0.564 | 0.561 | 96.725 | 90.367 |
| 0.3 | 13 | 0.644 | 0.585 | 89.627 | 90.539 |
| 0.4 | 13 | 0.703 | 0.594 | 91.917 | 92.873 |
| 0.5 | 14 | 0.709 | 0.615 | 95.181 | 93.314 |
| 0.6 | 16 | 0.746 | 0.616 | 88.201 | 93.356 |
| 0.7 | 16 | 0.779 | 0.63 | 90.633 | 93.52 |
| 0.8 | 18 | 0.786 | 0.658 | 95.148 | 94.08 |
| 0.9 | 18 | 0.792 | 0.701 | 97.752 | 94.276 |
| 1 | 23 | 0.803 | 0.851 | 93.437 | 95.225 |

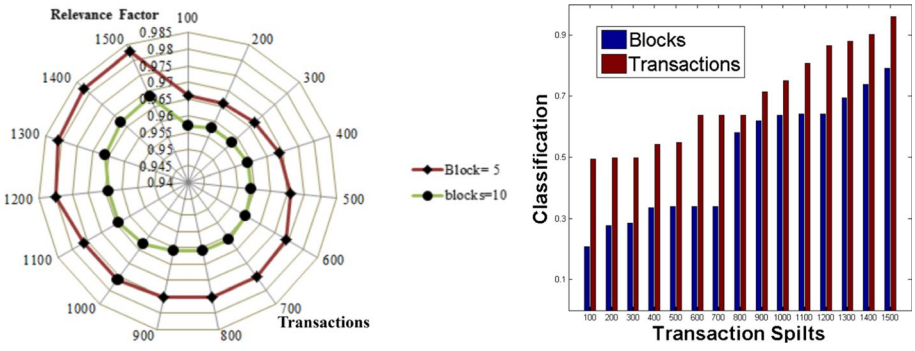
In the above equation, the retrieval process is evaluated by computing $\left(\frac{(t+\mathcal{T}')}{\mathcal{R}-\frac{\mathcal{T}'}{\mathbb{M}_0}}\right)$ where the ID is searched in the block, here the non-replication data are processed and search the query data from the user. The searching is determined in the split block, where both the similarity of data and content is achieved. The retrieval is achieved optimally by processing the block's relevant data based on the linear tree structure. From the retrieval rate processed by acquiring the content, the similarity is evaluated where retrieval is

formulated in the below equation. Here, it receives the input from the retrieval rate and computes the processing to decrease retrieval time.

$$\mathcal{T}' = \begin{cases} 1, \ if \ \sum_{\mathcal{S}'}^{\mathcal{R}} \left(\mathbb{t}_0 + \mathcal{Q}_0\right) * \frac{\mathcal{E}+\left(\mathcal{D}'-s'\right)}{\mathbb{M}_0/\mathcal{U}'+d_0} \\ 0, \ otherwise \end{cases} \tag{14}$$

The retrieval time is computed in the above Eq. (14).In this ', if and otherwise,' condition is determined to satisfy the objective. If the matching time is lesser for the retrieval process, then the determining of data are evaluated by $\frac{\mathcal{E}+\left(\mathcal{D}'-s'\right)}{\mathbb{M}_0/\mathcal{U}'+d_0}$.In this dissimilar data is discarded in the tree, and the process proceeds with the child node. Thus, the above two Eqs. (13) and (14) satisfies the objective and achieves the efficient retrieval process based on the pruning tree method in a linear model. Figure 6a, b indicate the relevance factor and classification for the different transaction splits. In this case, non-replication data is stored and the customer reviews the query data. The search is performed in the divided block, where data and content are processed. The block processing obtains the optimum compilation based on the linear tree structure of the related data. A similarity shall be determined by the rate of recovery processed by the acquisition of material when the recovery time in the following equation is formulated in Eq. (14).

The transaction splits are determined to achieve the non-replication data in the blockchain, where they are computed as $\left(\frac{\left(\mathbb{M}_0 * \frac{\mathcal{Q}_0}{\varepsilon}\right)}{\sum_{b'+i'}\left(\mathcal{I}'+\mathcal{U}'\right)}\right)$. The transaction increases based on relevant factors, calculated as two blocks, such as blocks 5 and 10. Compared to block five blocks, 10 shows better data retrieval efficiency (Fig. 6a). The transaction split is determined for classification and varying transaction, which is computed by deriving $\sqrt{\left(\mathfrak{X}+d_0\right) * s_0}$. Here the recognition of data is determined based on the similarity data. For every transaction splits, the varying blocks with similar data also increase and retrieve the classified similar data (Fig. 6b). Figure 7a, b illustrates the similar/dissimilar ratio and retrieval % for the different classifications.




**(a) Relevance Factor** **(b) Classification**

**Fig. 6** **a** Relevance factor. **b** Classification

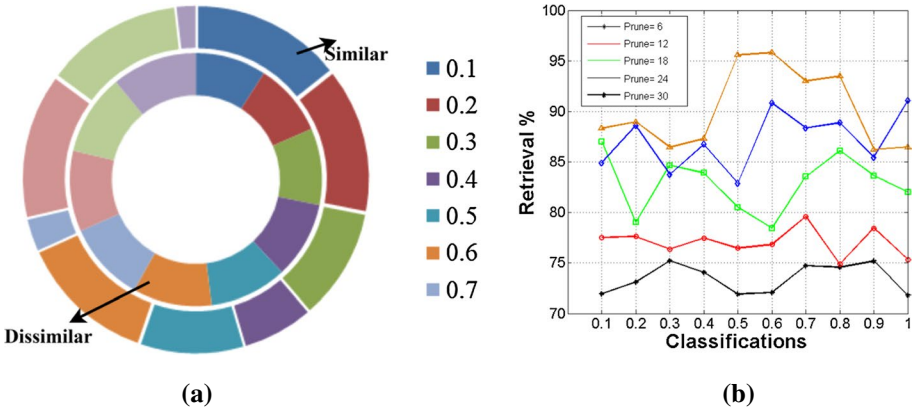



**Fig. 7** **a** Similarity/dissimilarity%. **b** Retrieval %

The classification is derived by formulating $\left(\frac{\mathcal{Q}_0}{\mathfrak{M}} + \mathcal{R}\right)$ where the non-replication data are evaluated, and the necessary data are retrieved. In this, if the classification of data increases, then the similarity of data also increases. It states if these two increases, the dissimilarity data in the blockchain decreases (Refer to Fig. 7a). The classification is achieved by dividing the similar and dissimilar data in the blockchain, and it is represented as $\mathbb{t}_0 - \frac{\mathcal{E}+b'}{\sum(\mathrm{t}+\mathbb{t}_0)}$. Thus, the matching time is determined and evaluated to get data using a pruning tree. Here the retrieval percentage decreases whereas, the relevant rate increases (Refer to Fig. 7b).

## 4 Discussion

The proposed DTARM is assessed using experiments designed in the NetSim emulator with 75 IoT devices communicating with a decentralized cloud. In this experimental setup, three blockchain systems are deployed for monitoring the transactions between IoT users and the cloud. The total transactions observed are 700 that fits into ten blocks of the blockchain system. The pruning process is performed under ten classification instances by splitting the transactions for a maximum of 1500. With this experimental setup, the proposed method is analyzed for access and retrieval time, retrieval ratio, and relevance factor. The variants in this analysis are the number of transactions and blocks. For verifying the consistency of the proposed method, it is compared with Block-DEF, ILQAT, and DNSTSM methods.

### 4.1 Access Time

In Fig. 8a, b, the proposed method's access time is less compared to the existing three methods. In this, the access is provided to the user who queries for the data, and it is computed as $\left(\frac{\mathbb{M}_0}{b'+\mathfrak{A}}\right) + \left(\frac{\mathfrak{r}_0-\mathcal{R}}{(\mathcal{A}_0*\mathfrak{M})/d_0}\right)$. In this, the replication and non-replication data are derived and monitors the block. Post the monitoring process; access is provided to the user. Based

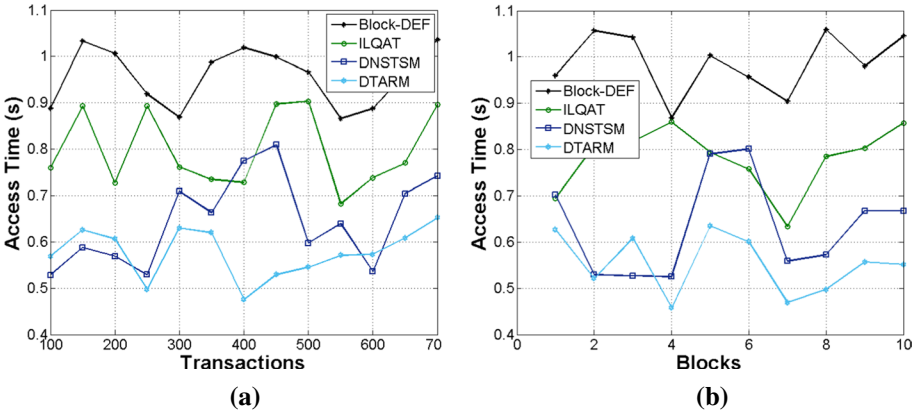
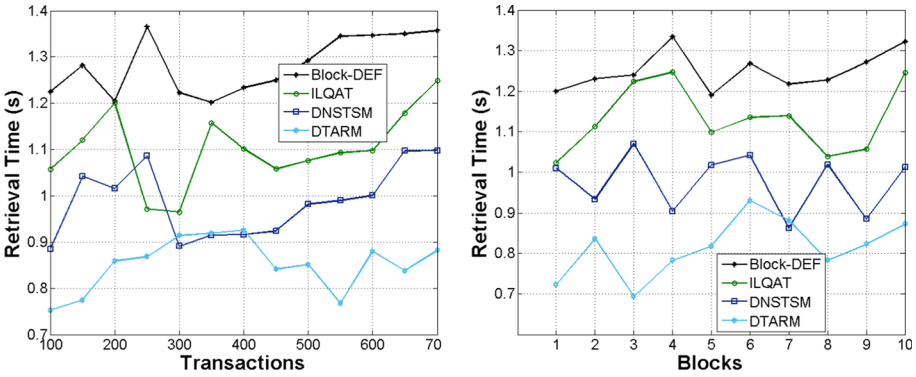



**Fig. 8** Access time **a** for transactions, **b** for blocks

on this, similar data are identified by formulating $\sqrt{\left(\frac{\mathcal{S}'+s_0)}{\sum \frac{d_0}{\mathcal{A}_0}}\right)}$ in these blocks are divided and process the identification of data. The accesses are given to the users who are authorized to access the particular service in the blockchain. In this transaction, the ID of the user is derived by matching the relevant information matching. By computing $\left[\left(\frac{\mathcal{S}'+s_0}{\mathcal{Q}_0/\mathbb{M}_0}\right)-\mathcal{T}'\right]$ The time-based data processing is achieved by monitoring the data from the query of the user. The sub-blocks are derived from the blockchain, and from that, the common match is evaluated. Thus, the non-replication data are assessed by computing $\left(\mathfrak{A}*\frac{\mathcal{C}-\frac{b'}{\mathfrak{M}}}{\mathbb{M}_0}\right)+\mathcal{D}'$ where the dissimilar data are discarded in the blockchain. The DTARM proposed shall be tested by NetSim simulator experiments using IoT devices with cloud communications. Three blockchain frameworks for tracking transactions between IoT users and the cloud are implemented in this experimental setup. The total number of transactions detected is, which can be divided into ten blocks. In ten classification instances, the pruning process is done by separating the transactions.

## 4.2 Retrieval Time

The retrieval time is evaluated concerning the number of transaction and blocks, and it derives the processing $\sqrt{\left(\mathcal{S}'+s_0\right)}-\left(\mathbb{t}_0-\mathcal{D}'\right)$. This searching is determined for the blocks and achieves the data based on time. Where the matching is evaluated based on matching the relevant and irrelevant data in the blockchain. By formulating $\sqrt{\left(\frac{\left(\frac{\iota d'}{\mathfrak{A}*d_0}\right)}{\sum_{\mathfrak{M}}^{d_0}(\mathbb{t}+\mathcal{I}')}\right)}$ the user query for the service, the data is allocated on the transaction of the user. The user's ID is derived and processes the evaluation by computing Eq. (4) in this, the analysis is determined based on the query. The user query for the data to the server; post to this process, the retrieval time is achieved. Here in Fig. 9a, b, the retrieval time is less for the proposed work by formulating $\left(\frac{\frac{\mathcal{R}}{\mathbb{t}_0}}{\frac{\mathfrak{x}}{\mathfrak{M}}}\right)$ in this, the recognition of data is achieved based on the query. Thus, the transaction and ID are processed based on the communication and information sharing,



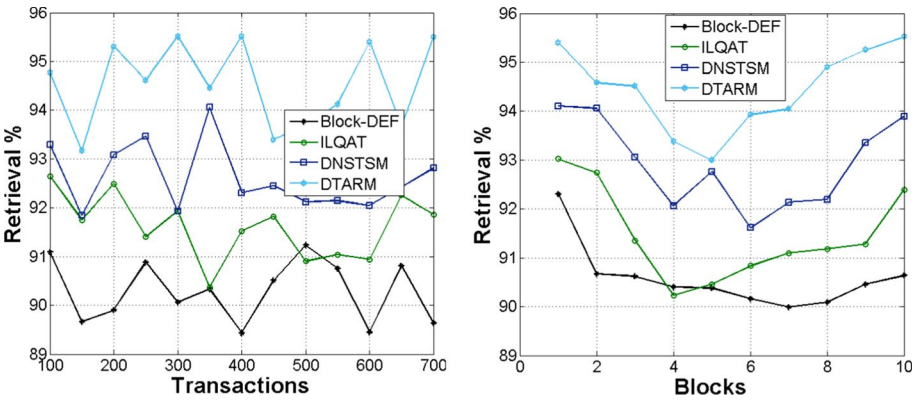

**(a) for Transactions** **(b) for Blocks**

**Fig. 9** Retrieval time **a** for transactions, **b** for blocks

decreasing the user's retrieval time. The retrieval is based on similar data analysis, where it is processed on non-replication data from the blockchain.

### 4.3 Retrieval %

In Fig. 10a, b, the retrieval percentage is high for the similarity data based on the number of transactions and blocks. By comparing with the retrieval time, the retrieval percentage increases in this it is processed by $\left(\frac{\mathcal{C}*\mathfrak{M}}{\mathcal{S}'}\right) * \left(\frac{\mathcal{S}'}{i'+\mathfrak{S}}\right)$. Here the classification based data are achieved based on relevant searching where the evaluation is determined based on the information sharing approach. Thus, effective communication and information sharing are derived by $\left(\frac{\mathcal{Q}_0}{b'/\mathcal{E}}\right) * \left(\mathcal{S}' + d_0\right)$. The blocks' data are evaluated based on the query, and the searching is determined in the blockchain. The utilization of user is computed as $\left(\mathcal{P}' * d_0 + \mathcal{A}_0\right) - \mathcal{T}'$ in this time-based processing is performed. This access is provided




**(a) forTransactions** **(b) for Blocks**

**Fig. 10** Retrieval % **a** for transactions, **b** for blocks

to the queried user, where the division of data is performed. The access is provided by formulating $\sqrt{(\mathcal{E}+\mathbb{M}_0/\mathcal{R}+d_0)}$ in this continuous monitoring of data are deployed. Where the non-replication data are processed in the blockchain by $\left(\mathbb{t}_0+\mathcal{T}'\right)*\left(\frac{\mathfrak{C}*\mathcal{U}'}{\mathfrak{M}+d_0}\right)$ in this, the matching time is monitored for the queried user—dilated access to the transaction and recovery process for exploiting the transaction knowledge recovery ratio. The approach suggested classifies the transaction based on similarities and variations to boost the customer request/question matching potential. This method reduces the access time for the information through non-recurring binary research with transaction-constraint.

### 4.4 Relevance Factor

The proposed work's relevance factor shows increases in value if the retrieval percentages increase, shown in Fig. 11. The processing is evaluated by determining $\left(\frac{\sum \mathfrak{S}'*\frac{b'}{d_0}}{\sum_{A_0}\mathcal{P}'+s_0}\right)$. The blocks are evaluated based on identifying similar data that retrieves the data from the blockchain's queried user. By computing $\left(d_0+b'\right)-\left(\mathcal{T}'*\frac{\mathfrak{M}+\mathfrak{X}}{\mathrm{t}}\right)$ The data-based blocks are determined, and it is deployed by retrieving the data. Thus, the transaction and ID of the user are evaluated on the number of split blocks. The content-based similarity is assessed by monitoring the data where the dissimilarity data are discarded. In this, communication and information sharing are addressed and resolved by improving the retrieval rate. In Eq. (9), the similarity and dissimilarity data are classified where the non-replication data are determined. Thus, the monitoring of data is evaluated from the block, and it is computed as $\sqrt{\left(\frac{\mathcal{C}+d_0-b'(\mathbb{M}_0)}{\sum_{\mathcal{Q}_0}(\mathcal{U}'+\mathcal{A}_0)}\right)}$ here the access based data retrieval is achieved. Table 4 summarizes the comparative analysis with the improvements.

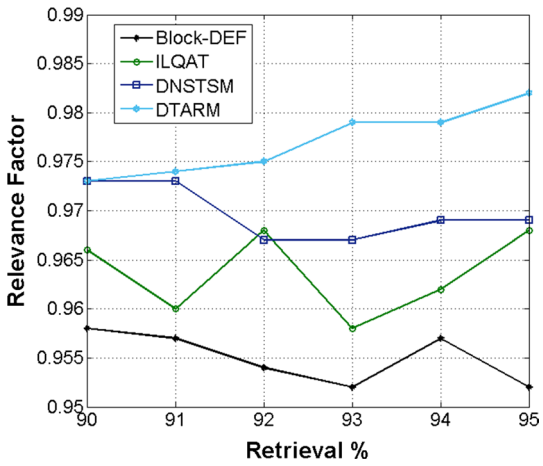



**Fig. 11** Relevance factor

**Table 4** Comparative analysis summarization

| Metrics | Block-DEF | ILQAT | DNSTSM | DTARM | Improvements |
|---|---|---|---|---|---|
| *Transactions* | | | | | |
| Access time (s) | 1.036 | 0.896 | 0.742 | 0.652 | 26.86% less |
| Retrieval time (s) | 1.357 | 1.249 | 1.098 | 0.882 | 28.56% less |
| Retrieval % | 89.638 | 91.862 | 92.808 | 95.49 | 12.16% high |
| *Blocks* | | | | | |
| Access time (s) | 1.045 | 0.857 | 0.668 | 0.551 | 25.67% less |
| Retrieval time (s) | 1.322 | 1.246 | 1.012 | 0.873 | 26.92% less |
| Retrieval % | 90.639 | 92.387 | 93.891 | 95.522 | 9.64% high |

## 5 Conclusion

This article discusses the dilated transaction access and retrieval method's performance for leveraging the retrieval ratio of the transaction information. The proposed method classifies the transaction based on similarity and dissimilarity to improve the user request/query's matching possibility. In this process, non-recurrent binary searching with transaction-constraint limits the access time of the information. The multi-split transactions based on the blocks and replication help identify the matching request/ query to respond with a service. This reduces the retrieval time of the available information. By performing periodic pruning, the replicated and non-replicated blocks with matching information are considerable reduced in a different classification. Therefore, the rate of retrieval increases by relevance for any number of transactions observed. This is updated in the blockchain system with the transaction history for further utilization. The proposed method improves information relevance and retrieval ratio by reducing access and retrieval time.

**Author contributions** Amudha. G- Writing- Reviewing and Editing.

**Funding** There is no funding available for this paper.

**Data availability** No data, models, or code were generated or used during the study.

**Complaince with Ethical Standards**

**Conflict of interest** All authors declare that they have no conflict of interests.

**Ethical Approval** All procedures performed in studies involving human participants were by the institutional and/or national research committee's ethical standards and with the 1964 Helsinki declaration and its later amendments or comparable ethical standards.

**Informed Consent** Informed consent was obtained from all individual participants included in the study.

## References


1. Ding, S., Cao, J., Li, C., Fan, K., & Li, H. (2019). A novel attribute-based access control scheme using blockchain for IoT. *IEEE Access, 7,* 38431–38441.
2. Choi, S., & Lee, J.-H. (2020). Blockchain-based distributed firmware update architecture for IoT devices. *IEEE Access, 8,* 37518–37525.
3. Preeth, S. S. L., Dhanalakshmi, R., Kumar, R., & Shakeel, P. M. (2018). An adaptive fuzzy rule based energy efficient clustering and immune-inspired routing protocol for WSN-assisted IoT system. *Journal of Ambient Intelligence and Humanized Computing*. https://doi.org/10.1007/s12652-018-1154-z.
4. Zhao, Q., Chen, S., Liu, Z., Baker, T., & Zhang, Y. (2020). Blockchain-based privacy-preserving remote data integrity checking scheme for IoT information systems. *Information Processing & Management, 57*(6), 102355.
5. Memon, R. A., Li, J. P., Ahmed, J., Nazeer, M. I., Ismail, M., & Ali, K. (2020). Cloud-based vs. blockchain-based IoT: A comparative survey and way forward. *Frontiers of Information Technology & Electronic Engineering, 21*(4), 563–586.
6. Sheron, P. F., Sridhar, K. P., Baskar, S., & Shakeel, P. M. (2019). A decentralized scalable security framework for endtoend authentication of future IoT communication. *Transactions on Emerging Telecommunications Technologies, 31,* e3815.
7. Rui, H., Huan, L., Yang, H., & Yunhao, Z. (2020). Research on secure transmission and storage of energy IoT information based on blockchain. *Peer-to-Peer Networking and Applications, 13*(4), 1225–1235.
8. Tseng, L., Yao, X., Otoum, S., Aloqaily, M., & Jararweh, Y. (2020). Blockchain-based database in an IoT environment: challenges, opportunities, and analysis. *Cluster Computing, 23,* 2151–2165.
9. Preeth, S. S. L., Dhanalakshmi, R., & Shakeel, P. M. (2019). An intelligent approach for energy efficient trajectory design for mobile sink based IoT supported wireless sensor networks. *Peer-to-Peer Networking and Applications, 13,* 1–12.
10. Lee, E., & Yoon, Y. (2019). Trusted information project platform based on blockchain for sharing strategy. *Journal of Ambient Intelligence and Humanized Computing*. https://doi.org/10.1007/s12652-019-01421-z.
11. Hei, Y., Liu, Y., Li, D., Liu, J., & Wu, Q. (2020). Themis: An accountable blockchain-based P2P cloud storage scheme. *Peer-to-Peer Networking and Applications*. https://doi.org/10.1007/s12083-020-00967-6.
12. Ozdayi, M. S., Kantarcioglu, M., & Malin, B. (2020). Leveraging blockchain for immutable logging and querying across multiple sites. *BMC Medical Genomics, 13*(S7), 1–6.
13. Ocheja, P., Flanagan, B., Ueda, H., & Ogata, H. (2019). Managing lifelong learning records through blockchain. *Research and Practice in Technology Enhanced Learning, 14*(1), 4.
14. Jiang, N., Wang, W., Wu, J., & Wang, J. (2020). Traceable method for personal information registration based on blockchain. *IEEE Access, 8,* 52700–52712.
15. Wan, P. K., Huang, L., & Holtskog, H. (2020). Blockchain-enabled information sharing within a supply chain: A systematic literature review. *IEEE Access, 8,* 49645–49656.
16. Wang, Z., Wang, T., Hu, H., Gong, J., Ren, X., & Xiao, Q. (2020). Blockchain-based framework for improving supply chain traceability and information sharing in precast construction. *Automation in Construction, 111,* 103063.
17. Li, M., Shen, L., & Huang, G. Q. (2019). Blockchain-enabled workflow operating system for logistics resources sharing in E-commerce logistics real estate service. *Computers & Industrial Engineering, 135,* 950–969.
18. Sifah, E. B., Xia, Q., Agyekum, K. O. B. O., Amofa, S., Gao, J., Chen, R., & Guizani, M. (2018). Chain-based big data access control infrastructure. *The Journal of Supercomputing, 74*(10), 4945–4964.
19. Yang, Y., Lin, H., Liu, X., Guo, W., Zheng, X., & Liu, Z. (2019). Blockchain-based verifiable multi-keyword ranked search on encrypted cloud with fair payment. *IEEE Access, 7,* 140818–140832.
20. Wu, Y., Tang, S., Zhao, B., & Peng, Z. (2019). BPTM: Blockchain-Based Privacy-Preserving Task Matching in Crowdsourcing. *IEEE Access, 7,* 45605–45617.
21. Yu, Z., Xue, D., Fan, J., & Guo, C. (2020). DNSTSM: DNS cache resources trusted sharing model based on consortium blockchain. *IEEE Access, 8,* 13640–13650.
22. Song, T., Cui, B., Li, R., Liu, J., & Shi, J. (2020). Smart contract-based trusted content retrieval mechanism for NDN. *IEEE Access, 8,* 85813–85825.
23. Xue, F., & Lu, W. (2020). A semantic differential transaction approach to minimizing information redundancy for BIM and blockchain integration. *Automation in Construction, 118,* 103270.

24. Pattengale, N. D., & Hudson, C. M. (2020). Decentralized genomics audit logging via permissioned blockchain ledgering. *BMC Medical Genomics, 13*(S7), 1–9.
25. Ma, S., Cao, Y., & Xiong, L. (2020). Efficient logging and querying for blockchain-based cross-site genomic dataset access audit. *BMC Medical Genomics, 13*(S7), 1–13.
26. Tian, Z., Li, M., Qiu, M., Sun, Y., & Su, S. (2019). Block-DEF: A secure digital evidence framework using blockchain. *Information Sciences, 491,* 151–165.
27. Farrugia, S., Ellul, J., & Azzopardi, G. (2020). Detection of illicit accounts over the Ethereum blockchain. *Expert Systems with Applications, 150,* 113318.
28. Jiang, P., Guo, F., Liang, K., Lai, J., & Wen, Q. (2020). Searchain: Blockchain-based private keyword search in decentralized storage. *Future Generation Computer Systems, 107,* 781–792.
29. Wang, S., Wang, X., & Zhang, Y. (2019). A secure cloud storage framework with access control based on blockchain. *IEEE Access, 7,* 112713–112725.
30. Zhong, B., Wu, H., Ding, L., Luo, H., Luo, Y., & Pan, X. (2020). Hyperledger fabric-based consortium blockchain for construction quality information management. *Frontiers of Engineering Management, 7*(4), 512–527.
31. Clarke, N. S., Jürgens, B., & Herrero-Solana, V. (2020). Blockchain patent landscaping: An expert based methodology and search query. *World Patent Information, 61,* 101964.
32. Li, H., Wang, K., Miyazaki, T., Xu, C., Guo, S., & Sun, Y. (2019). Trust-enhanced content delivery in blockchain-based information-centric networking. *IEEE Network, 33*(5), 183–189.



**Dr. G. Amudha** B.E, M.E, Ph.D., pursued her Bachelors of Engineering (CSE) in the year 2002 from Periyar University and Master of Engineering in Computer Science and Engineering in the year 2007 from Anna University, Chennai. She bagged Ninth University Rank in M.E(CSE). She has completed her Ph.D., in the area of Wireless Sensor Networks from Anna University, Chennai in the year 2019. She has 18 years of working experience in the teaching profession. She is coordinating Cyber Security Centre of Excellence activities. She obtained IBM—DB2, Tivoli, and RAD value added certifications. She bagged more than ten NPTEL certificates in the domain of Internet of Things and Network Security. Her areas of interest are Cryptography and Network Security, Compiler Design, and Sensor Networks. She has guided eight Master of Engineering projects. She was associated as Co-coordinator with AICTE Sponsored Faculty Development Programme on "Provision of Urban Amenities in Rural Areas" and National Level Conference RING 2015. She has published eleven research papers in journals and conferences. She was invited as a Guest Speaker in Anna University Sponsored Faculty Development Training Programme. She is been awarded as Motivational Learner by NPTEL. She also bagged CEH certification. She has completed several online courses in coursera related to security domain. She has attended four ATAL Faculty development programme in the domain cyber security and wearable devices.

Microprocessors and Microsystems xxx (xxxx) 104241

Contents lists available at ScienceDirect

Microprocessors and Microsystems

journal homepage: www.elsevier.com/locate/micpro

# ACDS—Assisted Cooperative Decision-Support for reliable interaction based navigation assistance for autonomous vehicles

G Amudha [a]

[a] RMD Engineering College, Chennai

ARTICLE INFO

*Keywords:*
AV
Cooperative computing
Navigation assistance
Neural learning

ABSTRACT

Autonomous vehicles (AV) technology is designed for replacing conventional transportation systems ahead of energy conservation, pollution control, accident prevention, etc. The benefits of AV are feasible by the incorporation of information technology and connected infrastructures. These provide seamless support for driving and navigation assistance with the knowledge of the environment. However, the vehicles' independent assistance relies on the cooperative nature of the neighbors and infrastructure units. In this article, assisted cooperative decision-support (ACDS) is proposed for improving the spontaneous decisions for vehicle connectivity and navigation issues. The interrupt due to multiple connectivity issues from a specific infrastructure region is addressed for leveraging the decision support for AVs. In this decision-making process, neural learning is used for improving the analysis of radial inputs. The learning process categorizes connectivity and outage information based on the assisted navigation ratio between the neighbors and infrastructures. This helps to provide flexible, cooperative analysis in different navigation scenarios, promoting accuracy, and reducing the input complexity. The performance of ACDS is verified using outage, complexity, analysis time, and accuracy measures.

## 1. Background and related works

An autonomous vehicle has the capability of performing functions by sensing the environment without human interventions. Many sensors and software systems are furnished with vehicles to provide an automatic driving capability for the vehicles [1]. The new criterion was presented by autonomous technology for relating the inventions with the functionalities of the vehicle [2]. After Mercedes Benz's robotic van's arrival, significant advancement in autonomous technology came into existence, which is vision-guided. Using LIDAR, RADAR, and GPS and vision guide into the autonomous technology developed flexible journey control, highway parking efficiency, steering assistance, etc. in modern cars [3, 4]. Both driving and navigation functions are performed by autonomous vehicles; there is no need for this task. Implementing autonomous vehicle technology in the modern environment provides mobility for non-drivers, increases road safety, supports shared vehicles, increases reliability, and decreases traffic collisions. The autonomous vehicle can travel faster with less chance of errors since it takes minimum computation time [4, 5].

Navigation is one of the significant functionality of autonomous vehicles carried out by sensing and control mechanisms. Localization, perception, planning, control, and system management are essential for navigation purposes in autonomous vehicles [6]. Crowdsource topological map and open street map (OSM) are two types of maps used for self-localization in rural road navigation and the local perception system [7]. OSM consists of all rules accomplice with road segments to overcome navigation problems in the rural environment. In a real-time environment, tracking the path is possible with sensors, sensor fusion, and detailed perceptions [8]. Another way of tracking includes remote control stations, which are human teleoperation vehicles; it processes vehicles' information at the control station. Distance traveled by the vehicles is measured. The longitude and latitude are detected and artificial land marks are designed for the vehicle to precede with the details disclosed to sensors automatically. Navigation in autonomous vehicles is needed to characterize the defect, consolidate scheme for sensor fusion, provide flexibility for drivers, represent environmental conditions, etc. [9, 10] Autonomous mobility for drivers and people with specific disabilities is enabled by autonomous vehicles. They make it more convenient for travelers to read rest or even work while traveling with more flexibility and thus increase their efficiency. It can cut paid driver costs for commercial and taxi vehicles. Other advantages such as improved safety, reduced risk of crash, and increased road capacity will play an important role in the market adoption of these vehicles. An autonomous vehicle decides by integrating the change in a dynamic and undetermined environment. Interactive decision making is required for autonomous vehicles to behave as humanlike driving. There are many ef-

*E-mail address:* gamudha03@gmail.com.

https://doi.org/10.1016/j.micpro.2021.104241
Received 8 December 2020; Received in revised form 17 February 2021; Accepted 28 February 2021
0141-9331/

ficient methods present to design the decision-making process in that one method is a game-theoretic setting [11]. Stackelberg game is a commonly used decision-making model in autonomous vehicles. Decision trees are used to solve the decision-making game while more vehicles travel simultaneously on the road. Other vehicles which are driven by the human are analyzed to know their intension [5, 12]. Then framework is designed that allows interactive decision-making without the help of inter-vehicle communication. This helps to avoid accidents between human driving vehicles and autonomous vehicles on the road [8, 13]. Partially observed Markov decision process (POMDP) is used for formulating the problem, which will not directly observe the intention and reorganization action of other games. Decisions are frequently changed in the traffic environment. POMDP solve real-time application problems to avoid complexity in decision making. By proper decision-making, autonomous vehicles provide potential on demand transportation to anyone, at any place, anytime [13, 14]. Vehicle-to-vehicle systems allow vehicles to communicate with one another to prevent drivers from accidents and crashes. The basic technology uses special short distance radios to communicate with cars and to transmit information such as location, speed, direction, and braking status. Interaction with the car claims that the radio technology will be around 300 m wide, offering a far range beyond sensors, and is not affected by obstacles or other vehicles as much as possible.

Liu et al. [15] proposed a novel lane change decision-making model based on a support vector machine (SVM) for an autonomous vehicle. Bayesian criterion optimization is accepted to deal with problems in lane change along with the SVM algorithm. The experiment is carried out with the vehicle's help to prove the proposed model's efficiency by comparing it with the rule-based lane change model.

A reinforcement learning approach was suggested by Xu et al. [16] to autonomous decision-making of intelligent vehicles on the highway. MO-API (multi objective approximate policy iteration) is used for learning the policies better than autonomous decision making. 14 degree of freedom vehicle dynamics model helped to verify the performance of various decision-making methods. The efficiency of the proposed model is verified by testing the learned decision policy in real-time autonomous vehicles.

In tactical decision making, Hoel et al. [17] implemented a combining planning and deep reinforcement learning method for autonomous driving. Monte Carlo tree is used for combining planning and learning concepts. AlphaGo Zero algorithm is used where self-pay is not possible. The proposed work's performance is examined by applying this framework to two various highway driving cases and compared its strength with the Monte Carlo tree search.

Liao et al. [18] designed a decision-making strategy on the highway with deep reinforcement learning (DRL) for autonomous vehicles. A hierarchical control framework is used to manage the speed, acceleration, and driving decision. For acquiring highway decision-making strategy, DDQN (Duelling deep Q- network) algorithm is used. The proposed method efficiently and safely achieves the highway driving task.

Oubbati et al. [19] recommended UAV (Unmanned Aerial Vehicles) - assisted supporting services connectivity in urban VANETs. An efficient routing solution is proposed to deliver more reliable data and guarantee robust paths based on flooding techniques. UAV provides a reliable path and solution for path failure. The performance of the work was compared with the other schemes and improved the activity of data delivery.

Jiang et al. [20] developed a flexible multi-layer map model in autonomous vehicles for lane-level route planning. To reinforce autonomous driving Tsinghua map model is used flexibly and efficiently. The algorithm is called hierarchical route searching used for the planning process—the performance of the algorithm is verified on the grid network and real lane level road network.

A vehicle-in-the-Loop (VIP) verification of an all autonomous intersection control scheme is designed in [21]. Traffic micro simulation layer is implemented for vehicles to interact between the cyber testing environment, actual test vehicles, and the physical layer. MILP (Mixed Integrated Linear Programming) is used to arrange landing vehicles at the intersection area with no traffic lights. The reliability of the proposed method and fuel consumption is reduced in the VIL environment.

For transparent and general decision making, Likmeta et al. [22] considered combining reinforcement learning with rule-based controllers. Handcrafted rule-based Black box reinforcement learning (RL) approach is combined for better performance. Evaluation of parameter-based RL Method is done on the highway with intersection and roundabout. The RL problem is identified, and the result is compared with existing techniques.

Path-guided time-varying formation control with collision avoidance and connectivity preservation of under actuated autonomous surface vehicle subjected to unknown input gains in [23]. The distributed guidance control law for the kinematic level is used for various approaches. An adaptive kinetic control law is used to develop a neural estimator. Three folds advantages are obtained, and cascade stability analysis is used for proving closed-loop system stability.

Levin [24] suggested a combinatorial dynamic network trajectory reservation algorithm. Guaranteed arrival times of nodes are included in space-time trajectories. The cell transmission model, Godunov approximation is used to design traffic flows. The proposed work is applicable to networks in the city. High priority vehicles have less travel time. The congestion is controlled while comparing with dynamic user balanced assignments.

For autonomous vehicle signaling and trajectory optimization, UCRLF unified, constrained reinforcement learning framework for phase-aware architecture in [25]. For pollution and energy consumption by a vehicle, the operating time and movement are analyzed. The result shows that the proposed work is reliable and reduces the overhead of penetrating data.

A decision making strategy for autonomous vehicle breaking in an emergency via deep reinforcement learning (DRL) is proposed by Fu et al. [26]. This work satisfies the efficiency, accuracy, safety, decision making, and comfort for passengers. For designing an autonomous breaking strategy, a vehicle lane changing process is used. The DRL process determines the rate of accident and passenger comfort. DDPG (Deep deterministic policy gradient) algorithm is used to solve the breaking problem.

Autonomous car decision making and trajectory tracking are considered by Receveur et al. [27] based on genetic algorithm and fractional potential fields. Multi-criteria optimization is reduced by genetic algorithm and nature, movement, the orientation of obstacles is considered by potential field. Repulsive and attractive potential fields are improved and minimize the drawbacks.

Dutta et al. [28] implemented a decentralized formation and next connectivity tracking controller for multiple unmanned aerial vehicles (UAVs). Time-varying functions are considered by multi UAV information exchange topology. Controller parameters maintain connectivity. For tracking the connectivity profile in target-centric formation, a decentralized controller is used.

## 2. Assisted cooperative decision-support (ACDS)

The autonomous vehicle is used to decrease the accident on the roadside and improve the user's driving experiences. Here it acquires the input from the neighboring vehicle and infrastructure to provide cooperative computing. The presented work introduces the ACDS method to improve performance and accuracy and minimizes the outage, complexity, and analysis time. The possibility of self-driving cars, especially those caused by driving distraction, is in the future likely, even in cases of bottlenecks, changes in lane, merges or other disruption, to reduce the number of deaths and injuries caused, as is normally the case. Self-driving cars should save valuable lives that are lost every day as a result

of excessive speed or alcohol influence. It is estimated that almost 1.3 million people worldwide die in road accidents. An autonomous car removes manual controls and prevents human error-induced deaths. A significantly decreased traffic queues that account for delays in travel are one of the main benefits of driverless cars they can foresee. Self-driving cars can interact on the road with other cars. With fully automatic brake functions, crashes between the nose and tail can largely be avoided. Cars ride from each other at reasonable distances. Speed limits can be raised as our confidence in our vehicles increases. Fig. 1 illustrates the ACDS in AV navigation.

The vehicle acquires the information from the neighbor and the infrastructure to provide better decision support. The distance between the initial vehicles and the neighboring vehicle is identified by the following equation for this processing.

$$h_e = \frac{1}{c_n} + \sum_{u_x}^{g_b} \left(y_w * r_t\right) + r_t - \left[\left(f_0 + g_b\right) + \left(n_v - b'\right)\right] - k' \tag{1}$$

The distance is analyzed to acquire the neighboring vehicle and infrastructure information to perform better navigation support. In the above Eq. (1), the distances are calculated, and it is denoted as $h_e$ here the neighbor and infrastructure of the vehicle is identified; it is represented as $g_b$ *and* $f_0$. The vehicle is termed as $c_e$ whereas; the number of vehicles is denoted as $c_n$ communicate $u_x$ with each other to improve accuracy. The periodic monitoring of vehicle is estimated for interaction, and it is denoted as $r_t'$, here the navigation is identified on time, and it is represented as $\left(n_v - b'\right) - k'$.

The navigation is termed as $n_v$, $k'$ represents the time, whereas; identification is referred to as $b'$ here the navigation is provided from the autonomous vehicle on lesser analysis time. Here, the ACDS method is proposed in an autonomous vehicle to support better decisions and improve accuracy. Automated driving systems often rely on the automation system, which means that it's able to drive automatically, not in all conditions during normal operations. A human driver is therefore needed to start the automated driving system, and may not even do if the driving conditions are beyond the system's capacity. If the automation system is all driving, the human being no longer drives the car however remains responsible for the performance of the automobile as the vehicle operator.

Thus, the distance is calculated with the previous $r_t$ state and neighbor vehicle position is monitored that is denoted as $y_w$ and evaluates the output and then identification of neighbor and infrastructure is computed in the following Eq. (2).

$$b' = \begin{Bmatrix} \left(\frac{y_w}{c_v}\right) * \prod_{n_v} \left(k' + c_e\right) * \left(h_e - r_t\right), \in g_b \\ \sum_{h_e} \left(n_v * \frac{i'}{u_x}\right) + \left(c_n - y_w\right), \in f_0 \end{Bmatrix} \tag{2}$$

In the above Eq. (2), the identification of neighbor and infrastructure is analyzed by deploying the computed distances in Eq. (1). Here, the first derivation is associated with distance and the previous state of the vehicle that includes the timely manner of processing, and it is denoted as $\prod_{n_v} \left(k' + c_e\right)$. The majority of autonomous vehicles will use supported cooperative decision-making support (ACDS) to process data from their sensors and to help them decide on their next move. These algorithms will allow the objects detected by the sensors to be identified and classified as pedestrians, street light and many more, according to training. The automobile then utilizes this knowledge to assess if the vehicle must take precautions to avoid a detected object, such as a braking or a swerving.

In this, the navigation is provided to the forthcoming autonomous vehicle. It considers the distance between the vehicle, and it is represented as $h_e - r_t$. This first derivation is estimated to identify the neighboring vehicle, whereas the second derivation is associated with the ve-

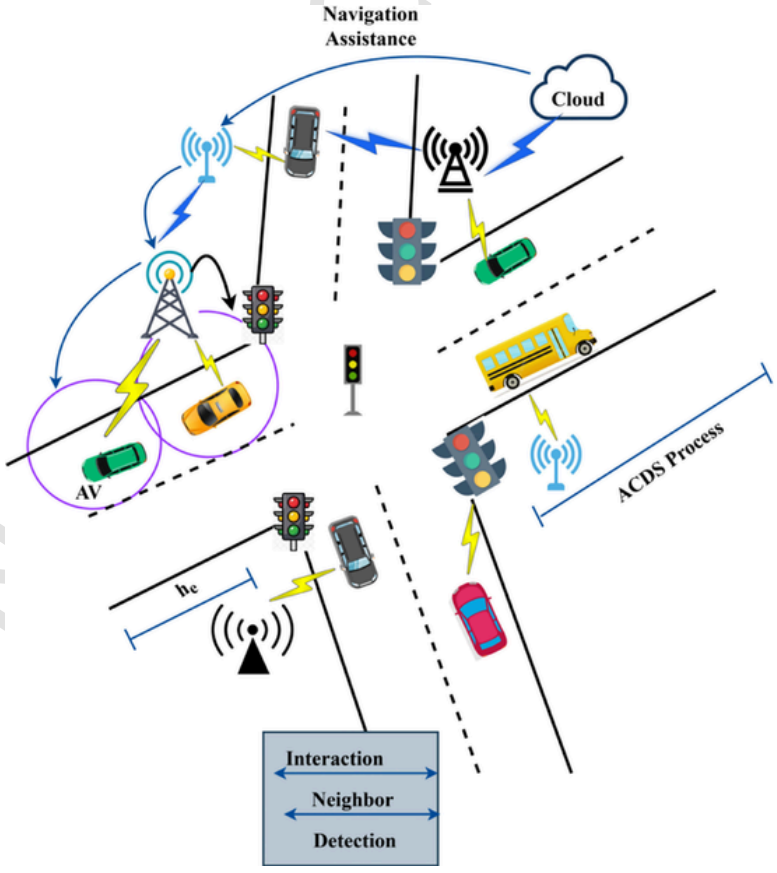



**Fig. 1.** ACDS in AV navigation.

hicle's connected infrastructure. The center of the bottom edge of a bounding box is used to calculate the width. During the calculation on the back wheels of the identified vehicle, the road surface is removed. The median color of the bounding box's last 8 lines is found to that effect. As the new lower edge of the bounding box, the first line on the bottom where more than 20 percent of the points are far from the medium color. A variety of vehicle locations are used to find directions in an automobile or an incorporate of a private entity. Usually, it uses a satellite navigation to obtain its location data which is connected to a position on a road. Routing can be determined when directions are required. The route can be changed with fly traffic information. Dead counts can be used for greater reliability by remoteness data from sensors connected to the driving gear, gyroscope and accelerometer, as the effect of urban canyons or tunnels can be GPS signal and/or multipath losses.

## 3. Navigation

The navigation is provided to the autonomous vehicle in the cooperative computing method; here, it distinguishes periodic monitoring for the vehicle number. However, it would be very sensitive to have a comparable two camera stereo vision device in a self-driving vehicle. If the cameras are even completely inconsistent, it results in the so-called "timing error" which results in inexact distance estimates. For that to happen, they use the ACDS and the data from one single front camera. The ACDS is trained to predict distance to objects with radar and collision avoidance sensor data. Engineers know that this information is correct, since direct radar and lidar signal reflections provide accurate information from distance to target regardless of the routes' topology. Here, the communication and interaction are carried out from the input acquired from the infrastructure; this detects the number of vehicle positions to provide the navigation. Automation of vehicles requires the implementation of mechatronics, virtual reality and multi-agent framework to support a vehicle operator. These characteristics and the vehicles they use can be called smart or intelligent. An automated vehicle for difficult tasks, especially navigation, can be called semi-autonomous. Consequently, a vehicle based solely on automation is called autonomous or independent. Thus, the infrastructure is identified in the second derivation, and then communication is established by equating the following equation.

$$n_v = \prod_{c_e}^{c_n} (h_e + \beta) * \left(\frac{g_b + f_0}{a_t}\right) * \Delta + (i' + c_e/b') * \sum k' + r_t\,(c_e) + u_x \tag{3a}$$

The analysis is done for the communication between the neighbor and autonomous, and infrastructure and autonomous vehicle, here the detection is carried out, and it is represented as $\beta$. In this equation, the navigation is provided to the autonomous vehicle and analysis of the vehicles' communication. Autonomous vehicle technology can offer some advantages over human-driven vehicles. One such possible gain is that road safety can be enriched – vehicle accidents are causing multiple deaths each year and automatic vehicles could decrease the number of victims as their machines will probably make fewer mistakes than humans. Decreased road congestion may minimize the number of collisions, an additional potential benefit of autonomous vehicles. This can be accomplished by autonomous driving by removing human conducts that trigger road obstructions, especially stop and traffic. The analysis is denoted as $\Delta$ here the infrastructure and neighboring of the autonomous vehicle are detected on time. In this, it decreases the outage that is referred to as $a_t$, and proceeds with better interaction with the vehicle, and it is represented as $(i' + c_e/b')$. In Fig. 2, the navigation analysis between the AVs and infrastructure is illustrated.

The distance is calculated for every instance because the vehicle shows a change in position; evaluating this decreases the outage factor

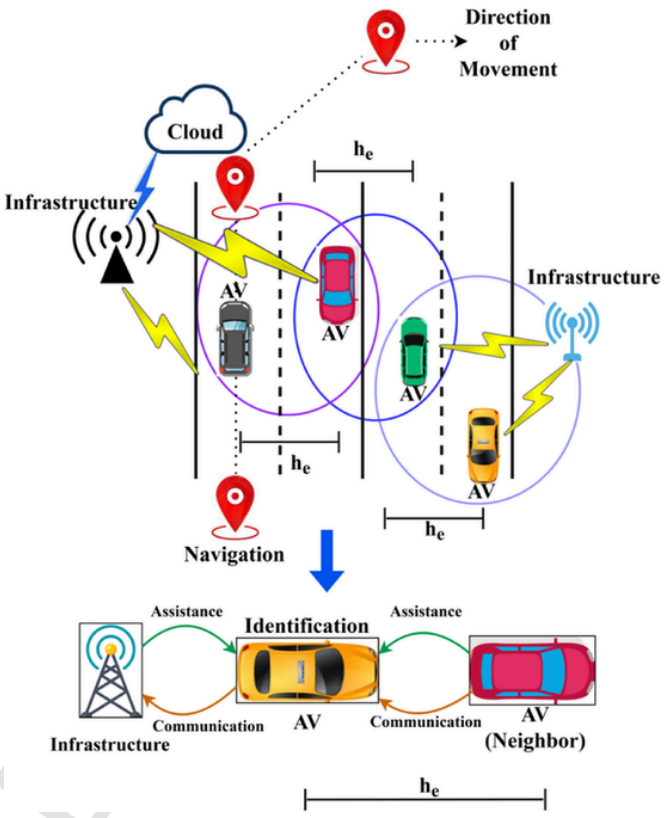



**Fig. 2.** Navigation analysis.

for this proposed work. Here, the vehicle's previous state is monitored and detects the current state of position by finding the distance between the autonomous vehicle. In this, detection of the vehicle is done on time, and it is represented as $\sum k' + r_t\,(c_e) + u_x$. From this equation, the analysis of communication is computed and addresses the outage. The following equation integrates the communication and identification of neighbor and infrastructure for reliable interaction between the autonomous vehicles.

$$\Delta = (c_n + h_e/u_x) * \sum_{y_w} (f_0 + g_b) * \left(\frac{\beta}{i' + k'}\right) + \left(\frac{y_w * u_x}{r_t}\right) - b' \tag{3b}$$

The analysis is done for the better interaction among the autonomous vehicle here the cooperative communication is evaluated on time. Here the number of the vehicle is considered to analyze the neighbor and infrastructure for the autonomous vehicle. It is represented as $\sum_{y_w} (f_0 + g_b)$. In this manner, the monitoring is done for the interaction on time, and it is denoted as $\left(\frac{\beta}{i'+k'}\right)$. Thus, the communication is monitored among the autonomous vehicle by deploying the previous state of vehicle identification. This identification is termed as $\left(\frac{y_w * u_x}{r_t}\right) - b'$.

Thus, the analysis for interaction is carried out by deploying the communication between the autonomous vehicles associated with cooperative computing. In this manner, the integration of neighbors and the vehicle's infrastructure is considered to perform the interaction and improve the driver's navigation. From some time ago in the automotive world, independent or self-driving cars have created enormous waves. Self-sufficient cars are nothing other than driverless cars that can drive without human driving. Augmented Reality (AR), GPS sensing awareness, various sensors etc., enable driverless automobiles to pave the way to a potential zero-incident. Traditional manufacturers, technical

giants and starting companies all compete in creating independent electric cars across a wide spectrum of funding, intelligence and investment. Here, the complexity is identified, and it is overcome by detecting the proper navigation to the vehicle on time, and it is formulated in the following equation.

$$\Delta\left(n_v\right)=\sum_{k'}\left(c_n*i'\right)+\left(\frac{r_{\parallel}/\beta}{\prod_{f_n}c_e}\right)*\left(h_e+u_x\right)+y_w*\left(a_t-p'\right) \tag{4}$$

In the above Eq. (4), the analysis for navigation is equated and addresses the complexity by deploying cooperative computing for an autonomous vehicle. Here, the interaction is carried out on time, and it is associated with $\sum_{k'}\left(c_n*i'\right)+\left(\frac{r_{\parallel}/\beta}{\prod_{f_n}c_e}\right)$ in this, the detection of infrastructure is analyzed. The monitoring is done to provide efficient navigation for the vehicle, and it is represented as $y_w*\left(a_t-p'\right)$, in this complexity, is decreased, and it is termed as $p'$. The main aspect is awareness, which is how the industry is able to process and distinguish road data from road signs to pedestrians and nearby traffic while driving. Driverless vehicles can identify and respond in real time with driverless control, enabling them to navigate safely. While they provide precise visuals, they are restricted by cameras. However, the distances of such objects can be measured to know exactly where they are. They can discern information from their surroundings. In low visibility conditions including fog, rain or night it is harder for camera-based sensors to detect objects.

The navigation is analyzed in cooperative computing that decreases the accident on the roadside and provides the vehicle connectivity by communicating and interacting. In this, it satisfies the cooperative analysis in different navigation scenarios and improves the accuracy and analysis time the neural learning is introduced. Recurrent neural learning is used to predict the vehicle on the road and provides better navigation to the autonomous vehicle. Connected vehicle technology leverages wireless technology developments in vehicle connectivity, infrastructure communication and other portable devices… As the technology of communication continues to evolve, automakers must remain focused on safety. The benefit of secure, more efficient, predictable and quicker technology is to make change across the world that saves lives and promotes society. Only communication within and outside the vehicles is needed to achieve the shape and function of the innovation stage.

## 4. RNN- ACDS

RNN is used to provide efficient navigation assistance for the neighbor and infrastructure autonomous vehicle and improve accuracy. Here, the prediction is made to analyze the vehicle's position and distance; it is performed by deploying the ACDS method associated with cooperative computing. Cooperative computing is used to decide on vehicle connectivity and navigation issues. In this RNN, the initial step is to find the vehicle's current and previous state to evaluate the prediction method; the following equation is used to find the current state of the vehicle in the neuron layer.

$$v_0=\left(\Delta*c_n\right)+\left(\frac{u_x*n_v}{\prod y_w}\right)-r_t+\left(f_0+g_b\right) \tag{5a}$$

The current state is analyzed in the neuron layer, and it is denoted as $v_0$ in this, it detects the neighbor and infrastructure data from the autonomous vehicle. This previous state is used to detect the vehicle's position to improve the navigation assistance for the neighboring vehicle. For this communication is used to deploy between the autonomous vehicle, and it is represented as $\left(\frac{u_x*n_v}{\prod y_w}\right)$ in this navigation is monitored and provided on time. Human drivers use their intellectual ability to predict how the future motions of others will based on their experiences, the performers around them and the scene context. Drivers should proactively prepare safe interactions by forecasting the trajectories of local agents rather than reactions to unpredictable events which can lead to risky behavior, such as hard braking or failure to execute critical maneuvers.

In this manner, the RNN is used to predict the forthcoming vehicle and connect it with the previous state to improve its accuracy. The following equation is used to assign the weight for the acquired data from the vehicle.

$$\mu=c_e\left(l_a\right)*\left(g_b+f_0\right)+\left[\sum_{\beta}\left(k'+h_e\right)*\left(\frac{v_0+\Delta}{r_t+c_e}\right)\right]+l_i \tag{5b}$$

The weight is assigned to the vehicle's current and previous state in this distance between autonomous vehicles to provide efficient navigation. The weight is termed as $l_i$ and assigning is represented as $\mu$, in this monitoring of data is acquired from the neighbor and infrastructure. In this distance between the vehicles is calculated and provides the detection that is represented as $\sum_{\beta}\left(k'+h_e\right)$, here the current state of the vehicle is analyzed, and it is denoted as $\left(\frac{v_0+\Delta}{r_t+c_e}\right)$. The RNN process for ACDS is illustrated in Fig. 3.

The weights are assigned for the neighbor vehicle's data, and infrastructure is cooperated to produce the assistance navigation. From the vehicle's current state, the data is forwarded to the next neuron layer to deploy the cooperative computing approach. Here the identification of data deploys cooperative computing to provide flexible and cooperative analysis. The following equation is used to evaluate the activation function that deploys the RNN learning.

$$z_s=v_0+l_i\left(c_n\right)+\left(c_e*b'\right)*\left(\frac{o'+n_v}{\Delta+l_a}\right)+\prod y_w*\left(i'+u_x\right) \tag{6}$$

The activation function acquires the input from the previous state of the neuron layer and forwards the output to the next neuron layer; processing this improves navigation and communication between the autonomous vehicles. It acts as the transformation function, and it is used to operate on the neuron layer. The activation function is denoted as $z_s$ in this, the current state of the vehicle is detected. These weights are assigned to every state of the vehicle termed as $v_0+l_i\left(c_n\right)+\left(c_e*b'\right)$. The activation function for navigation assistance is presented in Fig. 4.

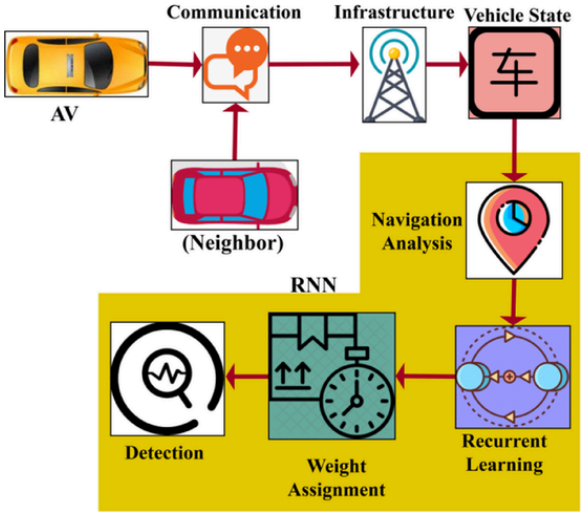



**Fig. 3.** RNN process for ACDS.

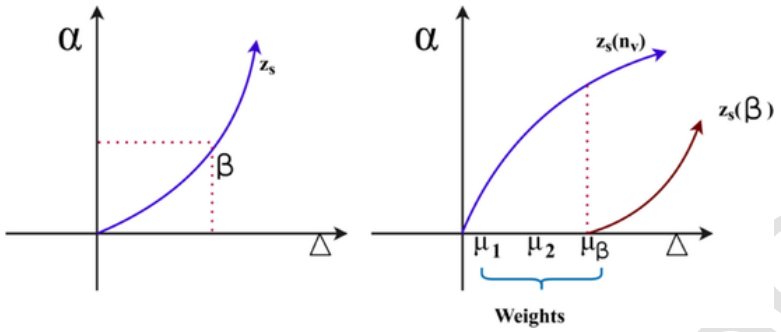



**Fig. 4.** Activation function for assistance (Reliability).

The data acquired from the neighbor vehicle and infrastructure is forwarded to the next neuron layer evaluated by the ACDS method. The forwarding is represented as $o'$ here the analysis is done for the data that is referred to as $l_a$ in this; the navigation is provided on time that is represented as $\left(\frac{o'+n_v}{\Delta+l_a}\right)$. The periodic monitoring is carried out in this interaction, and communication is established between the autonomous vehicle, and it is termed as $\prod y_w * (i' + u_x)$. By deploying this activation function, the prediction is performed for the forthcoming vehicle; here, the matching is done with the vehicle's previous state.

$$\alpha = \left(\frac{1}{c_n}\right) + \prod_{y_w} (c_e * l_i) + \left(l_a + o'/\sum(\Delta * v_0)\right) * \left(\frac{b' + h_e}{z_s}\right) - k' \tag{7}$$

In the above equation, the prediction is carried out for the current state and previous state of neurons in RNN, and it acquires the data from the neighbor and infrastructure. The prediction is termed as $\alpha$, in this matching is done between the current and previous state of the vehicle that deploys the assistance navigation, and it is represented as $(l_a + o'/\sum(\Delta * v_0))$. Here, the identification is made to calculate the distance between the vehicle's current and previous state.

The prediction in RNN deploys by fetching the neighboring and infrastructure data and map with the previous state in the neuron layer and produces the output. Here the data from the initial layer is forwarded to the second neuron layer. In this, it deploys the activation function, and it is denoted as $\left(\frac{b'+h_e}{z_s}\right) - k'$. In this manner, the distance and communication between the autonomous vehicles are identified that deploys the prediction. Thus, the prediction is done for every acquired data from the neighbor and infrastructure and provides navigation efficiency. The following Eq. (8a) and (8b) are used to compute the hidden layer; here, two hidden layers are used in this RNN learning.

$$\left.\begin{aligned} m_0 &= \beta * \left(\tfrac{c_0 - u_x}{h_e}\right) * l_i + \partial_1 \\ m_1 &= m_0 + \beta * \left(\tfrac{c_1 - u_x}{h_e}\right) * l_i + \partial_2 \\ &\vdots \\ m_n &= m_1 + \beta * \left(\tfrac{c_{n-1} - u_x}{h_e}\right) * l_i + \partial_{n-1} \end{aligned}\right\} \tag{8a}$$

$$\left.\begin{aligned} \beta(c_0) + m_0 &= (f_0 + n_v) * (\Delta + v_0/\alpha + g_b) * c_0(h_e) + \partial_1 \\ \beta(c_1) + m_1 &= m_0 + (f_0 + n_v) * (\Delta + v_0/\alpha + g_b) * c_1(h_e) + \partial_2 \\ &\vdots \\ \beta(c_n) + m_n &= m_1 + (f_0 + n_v) * (\Delta + v_0/\alpha + g_b) * c_{n-1}(h_e) + \partial_{n-1} \end{aligned}\right\} \tag{8b}$$

In Eq. (8a), the first hidden layer is computed in this detection of the initial vehicle is monitored and it is represented as $c_0$, the layers are denoted as $m_0$. The hidden layers are termed as $\partial$, and the number of hidden layers is referred to as $\partial_n$. In the first hidden layer, the vehicle is detected to establish communication. Here, the vehicle's number is detected with its distance between the neighbor and initial vehicle and provides the output to the second hidden layer. The input is given as the vehicle distance detection to provide assistance navigation to the forthcoming autonomous vehicle.

Eq. (8b) is used to derive the second hidden layer that describes the vehicle's detection for cooperative infrastructure and navigation of the autonomous vehicle. Here, the infrastructure and navigation of the current state of the vehicle are identified. This prediction is used for interaction and communication, and it is represented as $(f_0 + n_v) * (\Delta + v_0/\alpha + g_b)$. In this manner, the distance is calculated in the first hidden layer from this; the second hidden layer is responsible for providing the interaction and communication in a cooperative autonomous vehicle. In Figs. 5, the hidden layer process is illustrated.

By equating these two hidden layers, the weight is assigned to the incoming vehicle and provides the upcoming vehicle's assistance navigation. Here, the infrastructure and neighbor vehicle is detected; this

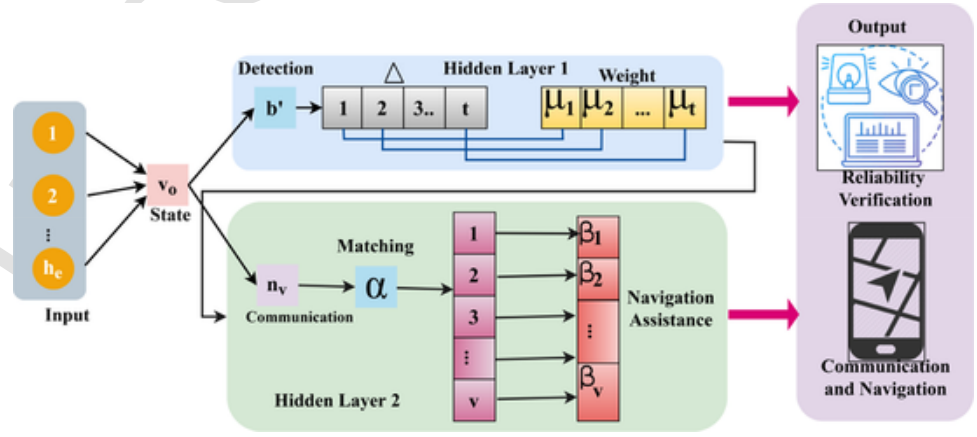



**Fig. 5.** Hidden layer process.

outage is decreased by computing the prediction between the vehicle's current and previous state. This cooperative computing is used in this autonomous vehicle to monitor the complexity and outage by deploying RNN learning. Here, the analysis time is decreased by making a decision that deploys the autonomous vehicle's assistance navigation. The following equation is used to evaluate the decision-making for navigation of the autonomous vehicle.

$$n_v = \left(\frac{1}{c_n}\right)\prod_{b'}^{c_n}\left(\alpha * \frac{l_i + c_0}{\mu}\right)\begin{cases}(m_n * \beta) - (u_x + i'r_t) + \Delta - k', \forall\ Dec\\ (\Delta - r_t) * \left[\left(\frac{y_w + \partial_n}{v_0}\right) + (f_0 + g_b)\right] - k', \end{cases}$$

The assistance navigation is provided to the autonomous vehicle that acquires the data from infrastructure and neighbor that deploys the cooperative computing. Here, the decision is made in the second derivation, where the first derivation is associated with the vehicles' communication and interaction. The decision support is provided using the ACDS method associated with RNN; in this, the outage and complexity are deceased. Thus the first derivation is computed by detecting the hidden layer processing in the neural state and produces assistance navigation, the analysis time is not minimized.

The second derivation is associated with the decision made from the data acquired from the infrastructure and neighbor of an autonomous vehicle. In this manner, periodic monitoring of vehicle is detected by deploying the hidden layer, and it is represented as $\left(\frac{y_w+\partial_n}{v_0}\right) + (f_0 + g_b)$ here the infrastructure and neighbor of the vehicle are identified with its data. Here, the vehicle's current and previous state is analyzed by evaluating the prediction process; the second derivation satisfies the decision-making approach. In this equation, the analysis time is decreased by satisfying the decision-making method associated with the ACDS. The detection of navigation assistance for the autonomous vehicle in cooperative computing, the following equation is calculated.

$$\beta = \sum_{k'}\left(\Delta * \frac{y_w}{p' + a_t}\right) + r_t(b') * v_0 - \left(v_0 + \frac{h_e * c_n}{\prod \partial_n}\right) + (f_0 + g_b) + n_v \quad (10)$$

The detection is estimated in the above Eq. (10); here, the monitoring of vehicle with the acquired data from the infrastructure and neighbor vehicle is identified to decreases the outage and complexity, and is represented as $\sum_{k'}\left(\Delta * \frac{y_w}{p'+a_t}\right)$. In RNN, the current and previous state of the neuron is identified that is represented as $r_t(b') * v_0$; the distance is calculated for the autonomous vehicle. Cooperative computing is used to improve the analysis of autonomous vehicles. These connectivity and navigation issues are sorted out by equating the above equation.

Here the detection is done by deploying the hidden layers. In this, the data is fetched from the infrastructure and neighbor vehicle, and it is denoted as $\left(v_0 + \frac{h_e * c_n}{\prod \partial_n}\right) + (f_0 + g_b)$. In this manner, assistance navigation is provided to the vehicle by utilizing the equation's decision-making method (9). For every vehicle identified from the roadside, the distance is calculated and evaluates the prediction and decision-making approach. Thus, RNN provides the vehicle's current state and results in better analysis time and decision-making support by deploying the ACDS method.

The inter-vehicles distance varies for detecting the data that is acquired from the infrastructure and neighboring vehicles. The detection of this data from these two sources varies for every instance of time. It calculates the distances between the vehicles. If the detection increases, then neighboring and infrastructure increase; comparing with a neighbor, infrastructure decreases (Fig. 6). Inter-vehicle distance is calculated for every instance for the number of vehicles that fetches the data (Fig. 7). It is associated with the interaction failure that deploys the detection of neighboring vehicles and infrastructure. If the inter-vehicle

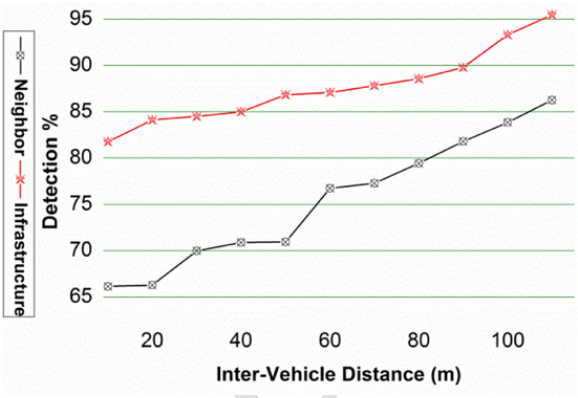



**Fig. 6.** Detection%.

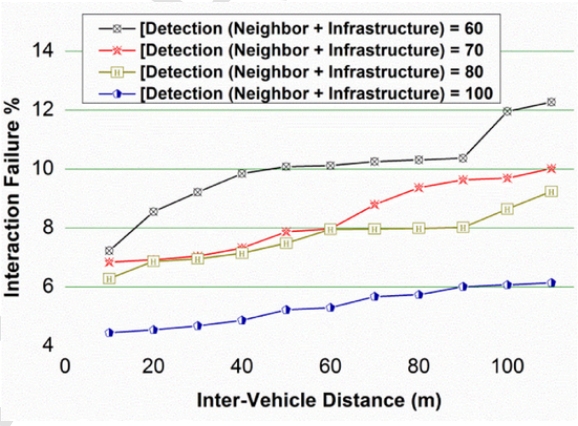



**Fig. 7.** Interaction failure% for inter-vehicle distance.

increases, then infrastructure of the vehicle increases, this shows higher detection. Compare to the detection value of 90, 60 shows higher infrastructures.

The weight is assigned to the varying vehicle that is associated with providing better assistance navigation. Here the assistance percentage varies from low to high, and the failure is identified for this estimation. If the navigation increases, the failure rate is deceased, whereas assistance is maximized; compared to the 12 failure rate, 6 shows a higher assistance percentage (Fig. 8). The weight varies for interaction failure percentage and the number of vehicles that range from high to low (Fig. 9). If the weight increases, the interaction failure varies for the number of vehicles on the roadside. If the number of vehicles increases, the in-

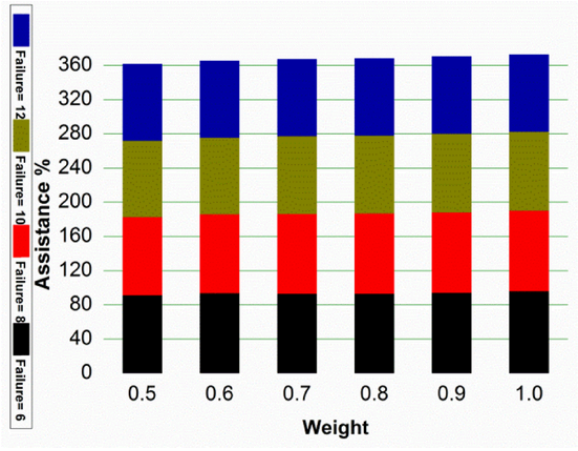



**Fig. 8.** Assistance% and

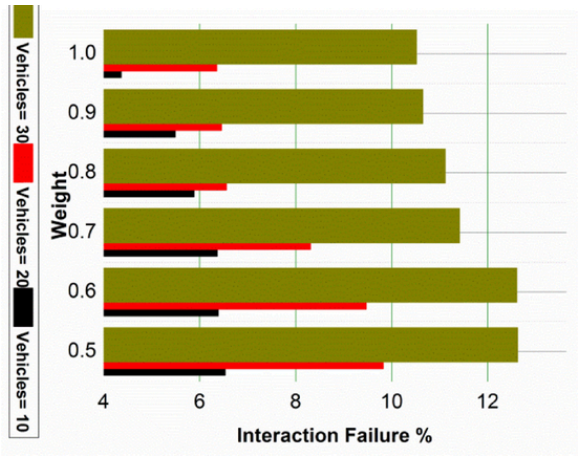



**Fig. 9.** Interaction failure% for weight.

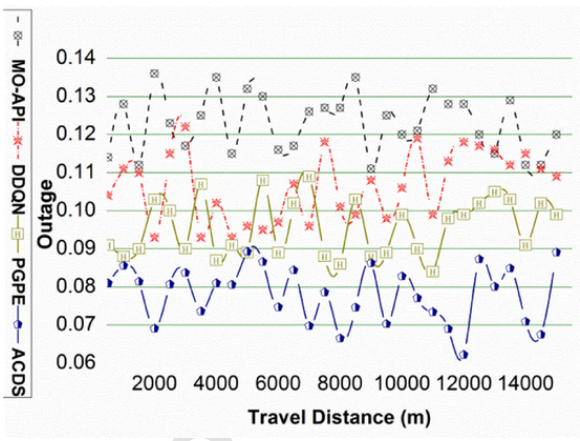



**Fig. 10.** Outage for travel distance and vehicles.

teraction failure increases, and vice versa, and in another case, if the weight increases, then failure decreases.

## 5. Discussion

This section discusses the performance of ACDS that is analyzed using experimental analysis. The experiments are performed using the OMNETT++ simulator, in which 30 vehicles are used in a region of 1000m* 400 m. The road segment is designed with one intersection and two lanes covering a 15,000 m two and fro. The inter-vehicle distance is measured between 10 and 110 m. The distance is covered using four infrastructures, each of which encloses 250 m of communication range. The metrics outage, complexity, navigation assistance, and accuracy are analyzed through comparisons. The metric navigation assistance is estimated based on the success rate of the decisions that identify the infrastructure location and movement direction. For comparative analysis, the existing MO-API [16], DDQN [18], and PGPE [22] methods are used.

## 6. Outage

The outage for the proposed work decreases for varying travel distances, describing the vehicle's starting stage and the vehicle number. The outage occurs due to vehicles' non-connectivity; in this work, the data is fetched from both infrastructure and neighboring vehicles. The distance is calculated as $[(f_0+g_b)+(n_v-b')]*\frac{1}{c_n}$ here the number of vehicles is considered by acquiring the data from the infrastructure and neighboring vehicles. In this manner, communication is established between the initial vehicle and the neighboring vehicle. It is used to monitor the vehicle's position and speed on the roadside and forwards the data to the neighboring vehicle. By deploying this assistance, navigation is provided to the neighboring vehicle in this prediction is performed by mapping the initial and neighboring vehicle data. The resultant decreases in the outage in this proposed work for the varying vehicle appears on different time instances. Here, the outage is related to the disconnection of communication between the autonomous vehicle, and it is overcome by the ACDS method. In this manner, the communication is established between the autonomous vehicle, and it is represented as $\sum_{h_e}\left(n_v*\frac{i'}{u_x}\right)$. Here, to establish the communication link, the distance between the neighboring and initial vehicles is calculated and interacts (Fig. 10).

## 7. Complexity

The complexity decreases by varying vehicle and inter-vehicle distances; it identifies the neighboring vehicle on the roadside. If the outage is decreased, the complexity is reduced by equating $\left(\Delta*\frac{y_w}{p'+a_t}\right)*v_0+n_v$. This analysis is done to provide assistance navigation to the autonomous vehicle that deploys cooperative computing. Here, the periodic monitoring is done for the neighboring vehicle and addresses the complexity at different intervals. The outage and complexity are identified by deploying the prediction method associated with the current and previous state of the vehicle. The prediction is performed by formulating $\left(\frac{b'+h_e}{z_s}\right)-k'*(r_t-v_0)$ in this identification of inter-vehicle distance is calculated for the prediction. From the vehicle's previous state, the data is acquired and mapped with the current state of the autonomous vehicle and provides the resultant. In this, the state is referred to as a neuron state that deploys the RNN learning to monitor vehicles. Here, the neuron state is responsible for forwarding the data from one state to another, and it is related to the activation function that is denoted as $(c_e*b')*\left(\frac{o'+n_v}{\Delta+l_a}\right)$. The vehicles are identified and forward the data to the neighboring vehicle in this analysis; it provides better navigation for the forthcoming vehicle (Fig. 11).

## 8. Navigation assistances

In Fig. 12 the navigation assistance for the proposed work increases by varying travel distances and the number of vehicles. Here, the distance is calculated for every vehicle that is associated with the prediction and decision-making approach. The assistance navigation is provided to the autonomous vehicle in this infrastructure, and neighboring vehicle data is fetched for computation. If the navigation assistance is provided to the forthcoming vehicle, the connectivity between the autonomous vehicles is established. If there is better communication is established, then navigation assistance is improved, and it is computed as $\prod_{c_e}^{c_n}(h_e+\beta)*\left(\frac{g_b+f_0}{a_t}\right)*\Delta$. Here the neighboring and infrastructure are considered to acquire the data and forwards to the inter-vehicle. For this distance is calculated, the communication is established between the initial and neighboring vehicles. In this manner, the navigation assistance is associated with the prediction and decision-making method. The decision is made to improve the navigation assistance for the autonomous vehicle. By formulating $\sum k'+r_t(c_e)+u_x$ the previous state of the vehicle is considered to identify to establish communication between the autonomous vehicles. For every instance, the distance is calculated by the concerning prediction method; here, it is evaluated by assigning the neighboring and infrastructure data weights.

## 9. Accuracy

The accuracy is improved if the autonomous vehicle communicates and interacts reliably promptly. For this accuracy level calculation, the

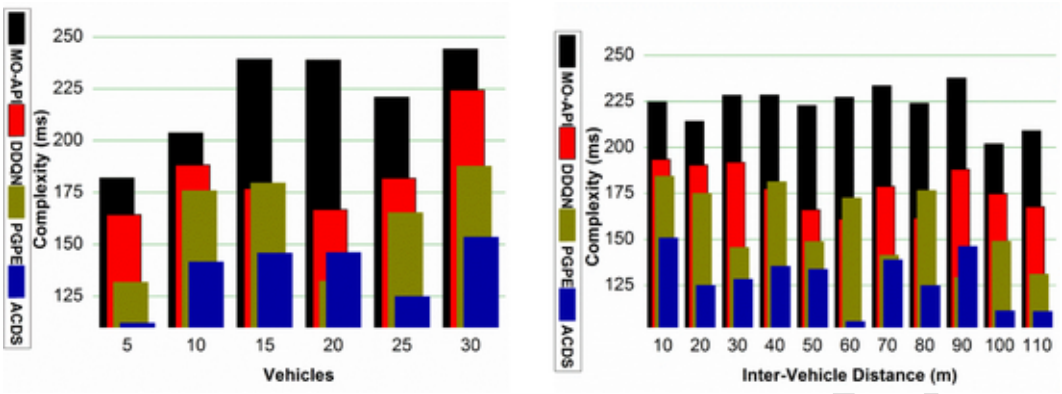



**Fig. 11.** Complexity for vehicles and inter-vehicle distance.

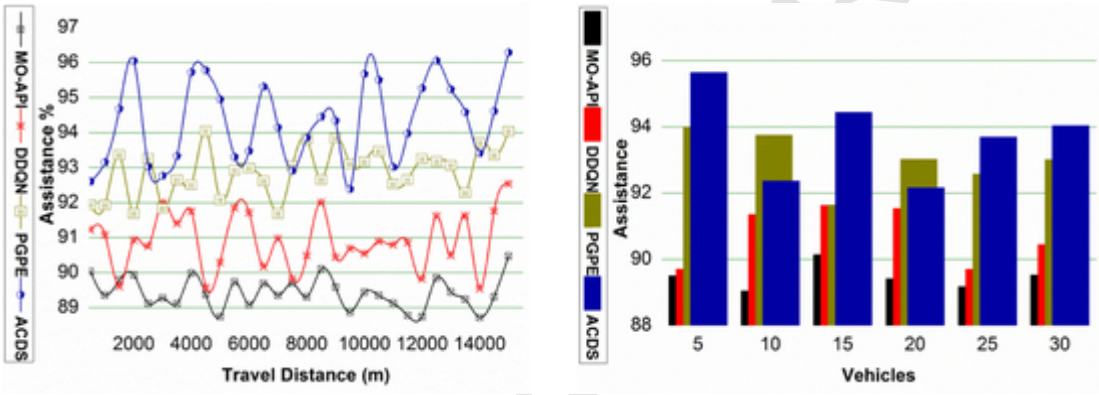



**Fig. 12.** Navigation assistance for travel distance and vehicles.

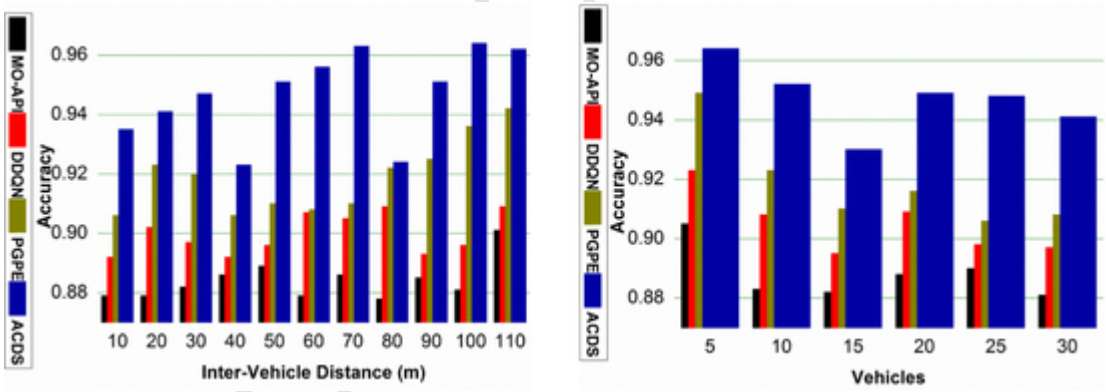



**Fig. 13.** Accuracy for inter-vehicle distance and vehicles.

activation function is important to assign the weight. The data fetched from infrastructure and neighboring vehicles are associated with the hidden layers evaluation. In this work, two hidden layers are used that monitor and identify the complexity and outage and improve the accuracy level for the number of vehicles. By equating $(c_n + h_e/u_x)$ the distance is calculated for better communication, and the prediction is associated with the neuron state. Here the decision-making is performed for the assistance navigation that provides the cooperative interaction. Cooperative computing is used for the autonomous vehicle that is used to improve the connectivity among the vehicles. These hidden layers are responsible for providing efficient navigation for the forthcoming vehicles on the roadside. The accuracy level is identified by calculating the number of vehicles divided by its prediction and decision-making for navigation. By estimating this, the accuracy level is improved for varying vehicles, and it is associated with the communication and interaction of the autonomous vehicle. Here the accuracy is maintained on time that improves the connectivity and assistance navigation among the vehicles (Fig. 13).

## 10. Comparative analysis summary

In Table 1, the summary of the analysis for travel distance is presented.

**Table 1**
Summary of the analysis for travel distance.

| Metrics | MO-API | DDQN | PGPE | ACDS |
|---|---|---|---|---|
| Outage% | 0.120 | 0.109 | 0.099 | 0.0891 |
| Assistance% | 90.473 | 92.544 | 94.039 | 96.29 |

**Table 2**
Summary of the analysis for Vehicles.

| Metrics | MO-API | DDQN | PGPE | ACDS |
|---|---|---|---|---|
| **Outage%** | 0.136 | 0.124 | 0.102 | 0.0868 |
| **Assistance%** | 89.522 | 90.441 | 93.006 | 94.031 |
| **Accuracy** | 0.881 | 0.897 | 0.908 | 0.941 |
| **Complexity (ms)** | 244.115 | 224.345 | 187.735 | 153.443 |

**Table 3**
Summary of the analysis for Inter-Vehicle Distance.

| Metrics | MO-API | DDQN | PGPE | ACDS |
|---|---|---|---|---|
| **Accuracy** | 0.901 | 0.909 | 0.942 | 0.962 |
| **Complexity (ms)** | 209.073 | 167.649 | 130.982 | 110.735 |

For the travel distance, the proposed ACDS reduces outage by 6.02% and improves the assistance by 11.8%.

In Table 2, the summary of the analysis for Vehicles is presented.

From Table 2, it is seen that the proposed method achieves 10.16% less outage, 9.12% high assistance, 13.7% high accuracy, and 9.95% less complexity.

In Table 3, the summary of the analysis for Inter-Vehicle Distance is presented.

ACDS achieves 13.4% high accuracy and 11.59% less complexity for different inter-vehicle distance.

## 11. Conclusion

Instantaneous decision-making improves the quality of navigation assistance in an autonomous vehicle scenario. The problems with connectivity and interaction between the vehicles and infrastructure units have to be resolved along the AV travel time. For providing this feature, assisted cooperative decision-support is discussed in this article. The proposed method identifies the interaction reliability by identifying neighbors and infrastructures based on distance and assistance ratio. The process of decision-making is supported by neural learning that identifies the interaction process's reliability throughout the travel time. In this process, the multiple connection issues are identified and mitigated by assigning the trailing neighbor or in-range infrastructure to assist the AV. Both the radial inputs are analyzed using cooperative navigation support to improve accuracy by controlling complexity and outage.

## 12. Future work

In the future, the proposed decision-making method is planned to be coupled with critical handoff schemes. This would help to improve the accuracy of identifying precise infrastructure in the direction of movement. Therefore, the problem of misguided navigation support and interference in densely populated vehicle scenario is achieved with much more reduced outages.

## Declaration of Competing Interest

None.

## References

[1] D. Zhou, Z. Ma, J. Sun, Autonomous vehicles' turning motion planning for conflict areas at mixed-flow intersections, IEEE Trans. Intell. Veh. 5 (2) (2020) 204–216.
[2] S.A. Cohen, D. Hopkins, Autonomous vehicles and the future of urban tourism, Ann. Tour. Res. 74 (2019) 33–42.
[3] S. Rafael, L.P. Correia, D. Lopes, J. Bandeira, M.C. Coelho, M. Andrade, A.I. Miranda, Autonomous vehicles opportunities for cities air quality, Sci. Total Environ. 712 (2020) 136546.
[4] S. Chen, Z. Jian, Y. Huang, Y. Chen, Z. Zhou, N. Zheng, Autonomous driving: cognitive construction and situation understanding, Sci. China Inf. Sci. 62 (8) (2019).
[5] D. Yang, X. Jiao, K. Jiang, Z. Cao, Driving space for autonomous vehicles, Autom. Innov. 2 (4) (2019) 241–253.
[6] J. Yang, T. Chen, B. Payne, P. Guo, Y. Zhang, J. Guo, Generating routes for autonomous driving in vehicle-to-infrastructure communications, Digit. Commun. Netw. (2020).
[7] M.W. Levin, E. Wong, B. Nault-Maurer, A. Khani, Parking infrastructure design for repositioning autonomous vehicles, Transport. Res. Part C 120 (2020) 102838.
[8] A. Sarker, C. Qiu, H. Shen, Connectivity maintenance for next-generation decentralized vehicle platoon networks, IEEE/ACM Trans. Netw. 28 (4) (2020) 1449–1462.
[9] I.W. Damaj, D.K. Serhal, L.A. Hamandi, R.N. Zantout, H.T. Mouftah, Connected and autonomous electric vehicles: quality of Experience survey and taxonomy, Veh. Commun. (2020) 100312.
[10] M.W. Levin, A. Khani, Dynamic transit lanes for connected and autonomous vehicles, Public Transport 10 (3) (2018) 399–426.
[11] X. Gu, Y. Han, J. Yu, A novel lane-changing decision model for autonomous vehicles based on deep autoencoder network and XGBoost, IEEE Access 8 (2020) 9846–9863.
[12] M. Teixeira, P.M. D'Orey, Z. Kokkinogenis, Simulating collective decision-making for autonomous vehicles coordination enabled by vehicular networks: a computational social choice perspective, Simul. Modell. Pract. Theory 98 (2020) 101983.
[13] M. Peters, M. Saar-Tsechansky, W. Ketter, S.A. Williamson, P. Groot, T. Heskes, A scalable preference model for autonomous decision-making, Mach. Learn. 107 (6) (2018) 1039–1068.
[14] F. Alam, R. Mehmood, I. Katib, S.M. Altowaijri, A. Albeshri, TAAWUN: a Decision Fusion and Feature Specific Road Detection Approach for Connected Autonomous Vehicles, Mobile Networks and Applications, 2019.
[15] Y. Liu, X. Wang, L. Li, S. Cheng, Z. Chen, A novel lane change decision-making model of autonomous vehicle based on support vector machine, IEEE Access 7 (2019) 26543–26550.
[16] X. Xu, L. Zuo, X. Li, L. Qian, J. Ren, Z. Sun, A reinforcement learning approach to autonomous decision making of intelligent vehicles on highways, IEEE Trans. Syst. Man Cybern. (2019) 1–14.
[17] C.-. J. Hoel, K. Driggs-Campbell, K. Wolff, L. Laine, M.J. Kochenderfer, Combining planning and deep reinforcement learning in tactical decision making for autonomous driving, IEEE Trans. Intell. Veh. 5 (2) (2020) 294–305.
[18] J. Liao, T. Liu, X. Tang, X. Mu, B. Huang, D. Cao, Decision-making strategy on highway for autonomous vehicles using deep reinforcement learning, IEEE Access 8 (2020) 177804–177814.
[19] O.S. Oubbati, N. Chaib, A. Lakas, P. Lorenz, A. Rachedi, UAV-assisted supporting services connectivity in urban VANETs, IEEE Trans. Veh. Technol. 68 (4) (2019) 3944–3951.
[20] K. Jiang, D. Yang, C. Liu, T. Zhang, Z. Xiao, A flexible multi-layer map model designed for lane-level route planning in autonomous vehicles, Engineering 5 (2) (2019) 305–318.
[21] S.A. Fayazi, A. Vahidi, A. Luckow, A Vehicle-in-the-Loop (VIL) verification of an all-autonomous intersection control scheme, Transport. Res. Part C 107 (2019) 193–210.
[22] A. Likmeta, A.M. Metelli, A. Tirinzoni, R. Giol, M. Restelli, D. Romano, Combining reinforcement learning with rule-based controllers for transparent and general decision-making in autonomous driving, Rob. Auton. Syst. 131 (2020) 103568.
[23] Z. Peng, N. Gu, Y. Zhang, Y. Liu, D. Wang, L. Liu, Path-guided time-varying formation control with collision avoidance and connectivity preservation of under-actuated autonomous surface vehicles subject to unknown input gains, Ocean Eng. 191 (2019) 106501.
[24] M.W. Levin, A combinatorial dynamic network trajectory reservation algorithm for connected autonomous vehicles, Netw. Spat. Econ. 19 (1) (2018) 27–55.
[25] C. Sur, UCRLF: unified constrained reinforcement learning framework for phase-aware architectures for autonomous vehicle signaling and trajectory optimization, Evol. Intell. 12 (4) (2019) 689–712.
[26] Y. Fu, C. Li, F.R. Yu, T.H. Luan, Y. Zhang, A decision-making strategy for vehicle autonomous braking in emergency via deep reinforcement learning, IEEE Trans. Veh. Technol. 69 (6) (2020) 5876–5888.
[27] J.-. B. Receveur, S. Victor, P. Melchior, Autonomous car decision making and trajectory tracking based on genetic algorithms and fractional potential fields, Intell. Serv. Rob. 13 (2) (2020) 315–330.
[28] R. Dutta, L. Sun, D. Pack, A decentralized formation and network connectivity tracking controller for multiple unmanned systems, IEEE Trans. Control Syst. Technol. 26 (6) (2018) 2206–2213.

**Dr.G. Amudha**, B.E, M.E, Ph.D., pursued her Bachelors of Engineering (CSE) in the year 2002 from Periyar University and Master of Engineering in Computer Science and Engineering in the year 2007 from Anna University, Chennai. She bagged Ninth University Rank in M.E(CSE). She has completed her Ph.D., in the area of Wireless Sensor Networks from Anna University, Chennai in the year 2019. She has 18 years of working experience in the teaching profession. She is coordinating Cyber Security centre of Excellence activities. She obtained IBM - DB2, Tivoli, and RAD value-added certifications. She bagged more than ten NPTEL certificates in the domain of Internet of Things and Network Security. Her areas of interest are Cryptography and Network Security, Compiler Design, and Sensor Networks. She has guided eight Master of Engineering projects. She was associated as Co-coordinator with AICTE Sponsored Faculty Development Programme on "Provision of Urban Amenities in Rural Areas" and National Level Conference RING 2015. She has published eleven research papers in journals and conferences. She was invited as a Guest Speaker in Anna University Sponsored Faculty Development Training Programme. She is been awarded as Motivational Learner by NPTEL. She also bagged CEH certification. She has completed several online courses in course related to security domain. She has attended four ATAL Faculty development program in the domain cyber security and wearable devices.