Intrusion Detection System Using Machine Learning For Smart Home

|  |  |  |
| --- | --- | --- |
| Dr. S MANJULA  Asst. Prof. Dept of CSE SJCE JSS Science and Technology university  Mysore-570006,india. [thejasyashas@sjce.ac.in](mailto:thejasyashas@sjce.ac.in)  , | HARSHITH MR  M.Tech., Dept of CSE  SJCE, JSS Science and Technology university  , Mysore-570006,india.  [Harshith.hr436@gmail.com](mailto:Harshith.hr436@gmail.com) | MANOHAR SN  M.Tech., Dept of CSE, SJCE,  JSS Science and Technology university , Mysore-570006,india. [msn.nadig@gmail.com](mailto:msn.nadig@gmail.com) |

**Abstract : Security and privacy remain significant challenges in the Internet of Things (IoT) due to the large-scale deployment and distributed nature of IoT networks. Blockchain-based solutions offer decentralized security and privacy protection, making them a promising approach for securing smart home environments. This study proposes a private blockchain-based smart home network architecture for intrusion detection, enhanced by a Fused Real-Time Sequential Deep Extreme Learning Machine (RTS-DELM) system model. The research explores the implementation of RTS-DELM within blockchain-based smart home networks to detect malicious activities in real time. By leveraging data fusion and decision-level fusion techniques, this approach improves intrusion detection accuracy and network reliability. Additionally, key components and architectural features of the proposed smart home security framework are analyzed in detail. The Fused RTS-DELM technique achieves a high level of stability with a low error rate, ensuring efficient and accurate detection of intrusions within smart home networks. Simulation results demonstrate that the proposed model effectively optimizes smart home security by improving real-time monitoring and mitigating potential cyber threats. This research highlights the advantages of integrating blockchain technology with AI-driven intrusion detection to enhance the resilience of smart home networks against evolving security risks.**

**Keywords: Real-Time Sequential Deep Extreme Learning Machine, data fusion, blockchain, smart home security, intrusion detection system.**

1. INTRODUCTION

A smart home is connected to the Internet, allowing users to manage a variety of smart gadgets, each of which serves an important purpose in the home for the user and their family. The IoT is the foundation of an intelligent home network, connecting disparate intelligent devices such as smartphones, smart computers, and wearable devices. Citizens’ lives can be made easier and safer by making their homes more open and secure. The smart home provides useful resources such as monitoring habits and even safety tests, which have compelled consumers and system developers to conduct extensive research. Blockchain-type systems and unified “cloud-like” computing networks can be used to solve these problems. Blockchain was developed in 2008 by Satoshi Nakamoto and

includes a time-stamped set of malicious evidence documentation managed by a network of autonomous networks [1]. Blockchain architecture consists of a series of blocks linked together by simple cryptography. The three main concepts underlying the operation of blockchain technologies are inflexibility, decentralization, and transparency. The three roles have been remarkably effective, exposing them to a wide range of digital currency technologies, such as the functionality of mobile vehicles, mobile phones, and embedded systems. While the blockchain platform is secure and anonymous, there are some issues with its current implementation. For example, Sybil attacks by generations of false identities to manipulate the community have become more complex. Since standard methods only look at the signatures and do not operate on searching for various specific patterns, a robust intrusion detection system is essential to analyze the circumstances thoroughly. RTS-DELM is a machine learning technique used to analyze data. This machine learning program uses an automated dataflow framework to determine data flow to detect intrusions and attack patterns. To handle the continually emerging smart blockchain-based applications, it is important to create powerful and versatile algorithms. Machine learning is a method that includes computers that teach themselves using an intelligent algorithm. According to one argument, machine learning is one of the first use cases of Artificial Intelligence (AI). The theory of machine learning helps machines to solve tasks without being explicitly programmed. The major objective of this sort of study is to develop a realistic algorithm that will receive information from the input and forecast it, as well as altering the outputs using statistical analysis. By utilizing machine learning, one can process a massive amount of data and arrive at a judgment based on facts. Furthermore, we suggest that a smart home network architecture that will overcome the current problems related to the centralized security of home networks and will address future attacks on smart home networks. In the present study, an RTS-DELM

methodology is used to make smarter homes safer using

Internet of Things (IoT) powered sensors with enhanced efficiency. The key contributions to this research include a

comprehensive overview of technological innovations applicable to blockchain-based smart homes empowered by RTS-DELM and a new outlook on diverse implementations (e.g., smart home data sharing), assisted by the recent stages of technological advancement.

RTS-DELM enables the automation of data analytics procedures and the generation of real-time insights. The datasets that the RTS-DELM methodology can assess can be manipulated in smart home networks, which means that all inaccuracies can be eliminated. Networks require consistent data. Any data-related issues in the RTS-DELM system will be ignored. It contains a method for detecting and anticipating possible deception and other unlawful activities. The purpose of this article is to examine an RTS-DELM-based system model for the smart estimation of intrusion detection in smart home networks with the highest degree of reliability. In the training and testing of intrusion detection in smart home network optimization with RTS-DELM, the fused datasets NSL-KDD (123,323 data samples) and KDD CUP 99 (25,193 data samples) are analyzed so that every instance has specific and varied features. As a result, the analysis and comparison of the finest approaches take place in the same place..

The remainder of this article consists of the following parts. Section 2 contains survey papers of related studies. Section 3 background and related work that explains the underlying blockchain technologies and introduces an RTS-DELM solution for blockchain-centered mobile home and smart home application systems. Section 4 presents an approach to the proposed methodology. Section 5 addresses the research results and discussions addresses the conclusions o the study found from the details.

1. LITERATURE REVIEW

Blockchain is a current buzzword among smart home enthusiasts, and a range of research articles have been produced on the subject. In research exploring how blockchain technologies would be used in the smart city, S. Aggarwal et al.

[[2](https://pmc.ncbi.nlm.nih.gov/articles/PMC9227380/#B2-sensors-22-04522)] discussed many aspects of healthcare, including transaction assimilation, home healthcare, and investment sharing. Nonetheless, the application of blockchain technologies in the smart home has not been explored comprehensively in information analysis. In many ways, the blockchain can be used in the smart home sector. M. Andoni et al. [[3](https://pmc.ncbi.nlm.nih.gov/articles/PMC9227380/#B3-sensors-22-04522)] provided a

detailed study of different blockchain applications of a peer-to- peer resource sharing network. The study presents detailed information on the implementation and capabilities of various smart home networks, such as security challenges in the smart grid, big data analysis, Artificial Intelligence (AI), and payment systems. However, their study did not adequately account for smart house-related issues, such as smart home security and smart city financial planning.

Khan et al. [[4](https://pmc.ncbi.nlm.nih.gov/articles/PMC9227380/#B4-sensors-22-04522)] suggested a user-based blockchain structure to secure the connectivity of edge information in the Internet of Things. Z. Zhou et al. [[5](https://pmc.ncbi.nlm.nih.gov/articles/PMC9227380/#B5-sensors-22-04522)] researched blockchain technologies, contractual analysis, and distributed computing to transfer the control and performance of certain automobiles. J. Wu et al. [[6](https://pmc.ncbi.nlm.nih.gov/articles/PMC9227380/#B6-sensors-22-04522)] suggested a software-specified blockchain interface to recognize dynamic blockchain frameworks and proceeded to apply a consent function approach to virtual machines with an application-aware system that can extract and manage unique consensus resources.

Sivaraman et al. [[7](https://pmc.ncbi.nlm.nih.gov/articles/PMC9227380/#B7-sensors-22-04522)] examined security issues in the smart home networks and made constructive suggestions. It is necessary to monitor and validate the systems that have been approved with an algorithm server and run the smart home equipment also in the external internet world. Via the abolition of a requirement for recognizing users and banning data packets that are not originating from the internet, the current regulations cannot efficiently protect internal user data.

Lee et al. [[8](https://pmc.ncbi.nlm.nih.gov/articles/PMC9227380/#B8-sensors-22-04522)] introduced an upgrade that handles software upgrades of embedded systems utilizing a blockchain, cryptographic certificates that are implemented with shared keys, and introduces encryption protocols utilizing a private key. A smart house has several tiny, embedded devices that are linked to each other. However, to utilize this mechanism, there are more components required than what is needed for a home.

1. BACKGROUND AND RELATED WORK

The operation of a blockchain is depicted in Figure 1. A block that reflects the desired transaction is produced once the transaction has been requested. The block is then distributed to all network nodes after that. The nodes then verify the transaction. The block is added to the current blockchain after receiving a reward for the proof of work. The transaction can then be designated as finished after this operation.

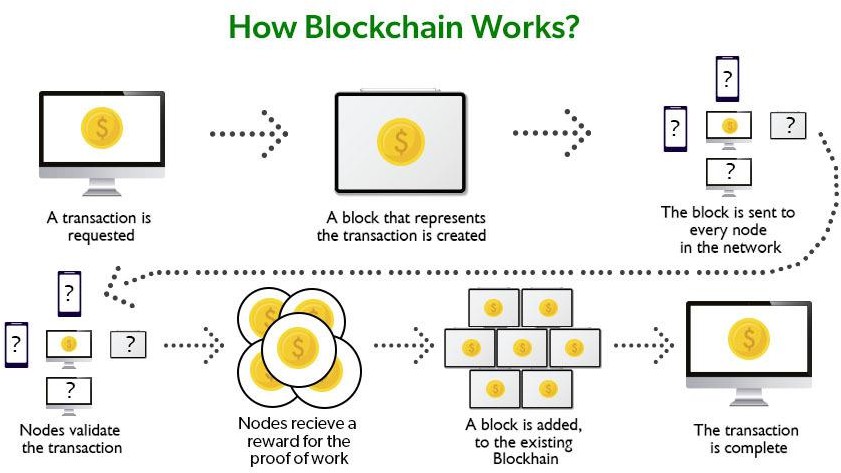


Figure 1 Working Process of Blockchain

* 1. Smart Home Network Security

Nowadays, with the help of smart home technology, it has become very easy to do various kinds of work, such as making a grocery list, and this method helps to monitor the access points of the house. Smart homes offer a variety of benefits through innovative equipment and can add value to the homeowner. The present age is highly dependent on technology, and it is very common for IoT devices to gain popularity [5]. The use of smart home devices protects homeowners from insecurity and ensures their security. Because of all the major security measures, this is their primary advantage. A simple and secured smart home framework is based on a refined version of the blockchain, known as the Consortium blockchain. Smart home devices use a kind of security automation via cameras to monitor the outside. A type of lock is also used to attach the buttons. In addition, if any irregular behavior can be detected in the home, special notifications are shown. Many use such devices to establish power over their family security and obtain transparent information about it. However, smart home devices might not always provide accurate and precise information. Like other devices, these devices allow hackers to use various tools to make threats and gain access by creating access points. Security vulnerabilities, in this case, can create promotions that homeowners will never know about and are unlikely to be unaware of. These threats can occur in various ways: malware infiltration, data theft, data leaks, death penalty failures, and denial of service. However, homeowners should explore other alternatives to promote greater security and take great care of their smart home systems to avoid facing such a dangerous digital environment.

Figure 2 shows how the user connects to a smart home. The smart home combines smart lights, smart locks, smart sockets, smart appliances, an alarm system, smartwatches, and smart TVs. The smart home connects with a cloud server, health care providers, entertainment providers, etc. The user's needs and

requirements can be fulfilled as soon as possible.

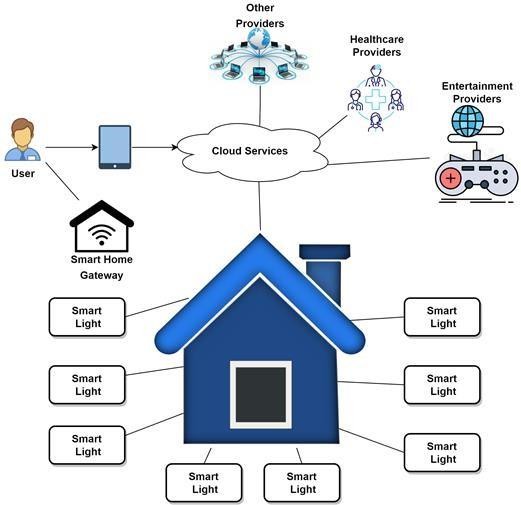


Figure 2. Smart Home Security

* 1. Related Work

Numerous IoT-based devices are linked together and centered on a smart home's gateways, as was explained in [8]. A gateway plays a big part in a smart home. However, due to its centralized structure, there may be security issues with certification availability and integrity. The authors suggested a blockchain- based gateway for smart homes to overcome the security flaws and protect the network from potential attackers. Gateway, device, and cloud are the three levels that make up the network.

The authors claim that in order to enhance decentralization and resolve problems associated with conventional centralized design, the blockchain will be integrated at the gateway layer, where data is stored and transferred in the form of blockchain blocks. Almost every user is familiar with and knowledgeable about their smart home devices. According to [4], Due to their constrained processing and storage capabilities, IoT-based devices like lightbulbs, door locks, and power switches have become increasingly vulnerable to security threats as the number of IoT devices used in smart homes has increased exponentially. By encouraging the adoption of blockchain technology and investigating some of the already suggested architectures for smart homes utilizing blockchain technology, Arif et al. aimed to investigate the security of smart homes.

nodes and the security transactions for smart homes, they included verification services made up of verification nodes to their model.

According to [5], security and privacy in IoT are two of the biggest challenges, mainly due to the massive scale and distribution nature of IoT-based networks. Decentralized security and privacy can be offered through blockchain-based methods. The majority of resource-constrained IoT devices cannot handle the delay, high energy use, and computing overhead needed. Authors in [5] presented a lightweight instantiation of blockchain specifically geared for utilization in IoT by eliminating the proof of work and the concept of coins. Table 1 summarises the advantages and disadvantages of securing smart homes with blockchain by analyzing papers by various authors.

Table 1 Relevant Studies on Advantages and Disadvantages of Securing Smart Homes with Blockchain

|  |  |  |  |
| --- | --- | --- | --- |
| Related Studies | Advantages | Disadvantages | Methodology |
| [1] | Blockchain can improve efficiency and speed, as it can complete time-consuming processes and automate them, maximizing efficiency. | Transparency is a huge issue in the present industry. The organizations tried to  implement more regulations and rules. With blockchain, smart homes can use a completely decentralized network, which does not require centralized authority and  improves the system's transparency. | Using an attribute-based access control system to authenticate users of smart homes and IoT devices allows for real-time communication between home users and a fully validating private blockchain node. |
| [2] | As a substitute for end-to-end encryption, blockchain is helpful in the development of a common security protocol.  Forming an uniform API  framework allows it to be used to secure private messages. | It is expensive, and network connectivity is one of the common issues the owners will encounter. The setup and configuration are too complex. | * The network is based on the Ethereum blockchain, and security, reaction speed, and accuracy are measured. * Ethereum is a decentralized, open- source blockchain that supports smart contracts. |
| [3] | One of the benefits of blockchain is its low cost. It allows data to be submitted peer-to-peer without  centralizing the controls. | Blockchain has a difficult process of  implementation, and scalability is an issue. | * The confidentiality and authentication issues are resolved by using the SHA2 encryption technique. * The integrity of the data kept in |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  | the gateway is maintained using blockchain technology.  - The design effectively shapes raw data to perform the data transformation algorithm. |
| [4] | Combining other technologies with blockchain can strengthen privacy agreements and enhance secure communications. | It needs huge storage; most of the blockchain consumes too much energy. | * Cloud computing and the consortium blockchain were combined. * To make smart homes safe and secure, the architecture for smart homes was designed to provide secrecy, integrity, scalability, and availability. |
| [5] | It is secure and encrypted by design with so many independent nodes to verify the updates to the chain before the updates. | It can be destroyed, so there is a requirement for a better way to handle  this. Whenever the data are updated, the nodes required are not ideal for the commercial blockchains needed for the network to be fast and secure. | Utilization of computing resources in a typical IoT environment (such as smart homes) and application of a Deep Extreme Learning Machine (DELM). |
| [6] | The block can be verified and inspected by all parties, which can help improve trust and  access to the data. | It has a high implementation cost.  Accessing the information stored by blockchain requires a private key, but the wallet will be in danger if it does not work. | Built a modified form of the Smart Home System (SHS). Following that, translate this concept to the consortium blockchain architecture. |
| [7] | Encryption with blockchain can help secure the IoT-based devices, making it impossible to overwrite existing data records. | Blockchain is highly energy-dependent, and it is not a distributed computing system. |  |

* 1. Problem Statement

The rapid increase in home devices on the market has raised numerous security problems [5]. This is due to such equipment's small power and storage, making people vulnerable to various cyber-attacks, including ransomware. This is why security solutions in the distribution among those devices have gained prominence as a required study field among academics due to their importance [16]. Following are some research questions that will be found in this research.

* + 1. Is it feasible to leverage blockchain protocols to establish security architecture for smart products and home connections from a technical standpoint?
    2. How do existing network architectures react to resource unavailability when subjected to the blockchain-based protection implementation described in the linked paper?
    3. How will applying the conceptual methodology for users and suppliers affect the security (consumers' network resilience and dependability) of the networks of both service providers and consumers.

` 4.PROPOSED METHODOLOGY

4.1 Background

In the year 2008, Satoshi Nakamoto invented the blockchain. A blockchain-based peer-to-peer payments system can eradicate intermediaries and double-spends by using a primary cryptocurrency (e.g., bitcoins). It is a centralized method where any information block is validated by SHA-256 (Secure Hash Algorithm) using a former hash block. The block contains a large amount of transaction stored data such as the block number of the previous block hash, transaction data, a nonce, and time stamps. The timestamp contains a constant parameter, but a nonce parameter is randomly generated. The miner (computer module) has control over the static (block) and dynamic (timestamp and nonce) portions of an information

chain and calculates the leading number of zeros required to form the header of the block.

Figure 3 highlights the smart home network centered on the private blockchain network. The platform includes four layers:

a layer of data sources connecting to the network and emitting user information, a private blockchain network layer empowered with RTS-DELM that unleashes predictive analysis against thousands of files, a client node with smart home system data, and a collection of home devices to simulate the data.

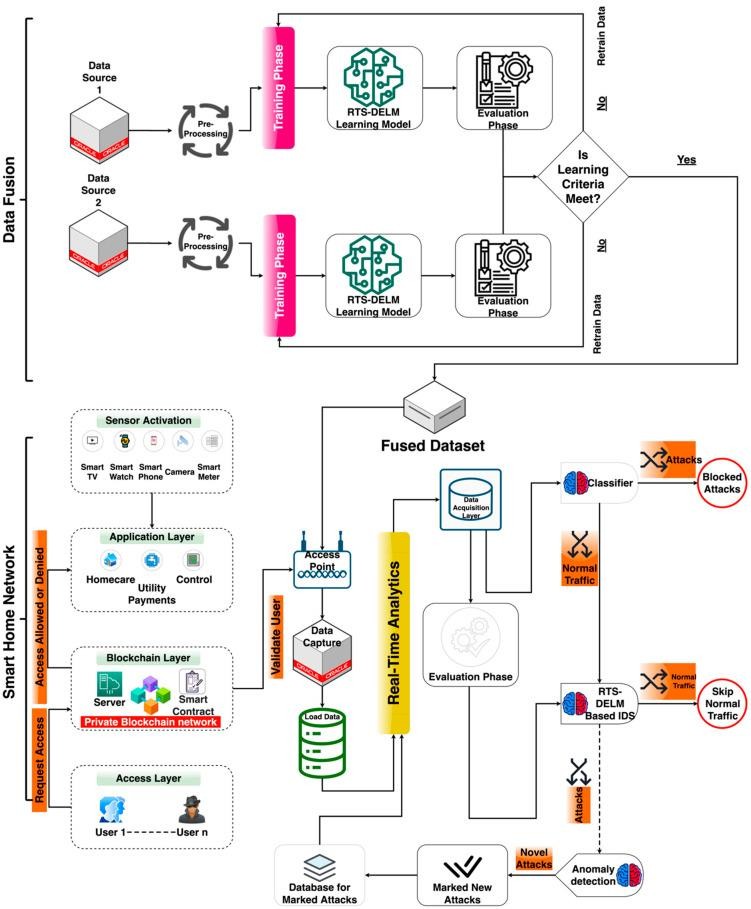


Figure.3. A Proposed Blockchain-Based Smart Home Network.

* 1. Integration Data Fusion Technique in Blockchain-Based Smart Home

Data fusion approaches incorporate information from various sensors to obtain more accurate observations than could be accomplished by using a single, separate sensor. Information extraction is the practice of extracting information from different and probably interconnected sources and integrating it in a way that will get the most impactful outcomes. For example, a series of network security sensors are in operation in a security framework. It is impossible to achieve a wide- angle, all-encompassing image of the overall security state of a dynamic system of the security system. Furthermore, devices that are spread over an extensive range can be challenging to manage effectively. To increase the efficiency of the model and provide analysis with an entire system protection condition, it is also essential to effectively and intelligently fuse the outcomes of these sensors.

In comparison, several data sources can offer more consistent reliability because the information itself comes from various sources. Consequently, data fusion approaches by integrating information from various data sources can produce more reliable and stable results than those obtained by a single information source. In this manner, the NSL-KDD [5] and KDD CUP 99 [4] datasets were used to evaluate the suggested system’s performance—these datasets were utilized to perform data fusion. Each data collection specifies a unique link that corresponds to a sequence of packets that flow between the provider and target locations in the fused data collection according to a predefined protocol. This data collection has 41 characteristics per record. Six distinct fields and 35 continuous fields compose these features.

* 1. Integration of Real-Time Sequential Deep Extreme Learning Machine in Blockchain-based Smart Home.

Listed below are the advantages when RTS-DELM is implemented;

* + - User authentication, as a means to legitimately access and make transactions on the blockchain network.
    - Blockchain offers a high degree of trust and protection. Blockchain applications incorporate real-time transaction mechanisms into smart contracts to ensure that the contractual commitments, which were already negotiated, are fulfilled.
    - Blockchain is a reliable way to incorporate an incentive-based mechanism to enable consumers and users to make a data contribution. In addition, this big data would help to refine the RTS-DELM model.

The usage of blockchain-based systems can be rendered smarter by the use of RTS-DELM computational technology. The confidentiality of data can be enhanced when utilizing the RTS- DELM distributed blockchain technology. RTS-DELM can also be used to increase the pace at which comprehension is achieved by exchanging further knowledge, thereby improving understanding. It offers the framework and network structure to develop a decentralized blockchain application. In this article, we analyze the RTS-DELM deployment architecture, which is an advanced system. The proper use of this technology will be to collect intelligence from different information resources, such as sensors, mobile devices, and IoT systems. Knowledge derived by utilizing these techniques is used for smart apps. The blockchain is the central structural feature of smart apps. Nonetheless, for analysis, the RTS-DELM method may be used to evaluate and forecast real-time data. The blockchain also processes all the data that might be required from the RTS- DELM model.

Data errors such as duplication, missing data parameters, glitches, and noise are reduced when making data for research. Knowledge is transmitted through the blockchain, and the minimization of data-related issues can be solved in the RTS- DELM framework. The RTS-DELM technique can function well where only a limited portion of a data set is needed. The architecture provides a wide variety of implementations in various areas, such as fraud detection and prevention. The blockchain infrastructure focuses on the edge of the Internet of Things (IoT) and comprises three main elements: blockchain layer, knowledge architecture, smart contracts, and the RTS- DELM framework. In the proposed RTS-DELM system, vast quantities of hidden layers, hidden neurons, and several activating mechanisms have been employed to optimize the privacy and protection of smart homes. There are three separate steps in analyzing the data in the proposed method: the data acquisition, preprocessing, and assessment stages. The evaluation layer was made up of two sub-layers: the prediction and performance layer. For analysis, accurate data are obtained from sensors and actuators. Then, the data are given as raw data and used by the collection layer. A comprehensive technique for data cleaning and preparing has been implemented to remove discrepancies in the preprocessing layer. The RTS-DELM was employed to maximize the home network protection by preventing disruptive or invasive applications.

Cryptographic hash functions connect blocks via cryptography. A home server computer could be viewed as a miner to validate new transactions and introduce new blocks. In contrast, intelligent contracts follow predefined rules to make decentralized transactions easier and quicker. There are diverse consensus models for blockchains, such as proprietary, public, and federated, but private blockchains are more effective when used in smart homes.

The deployment layer can provide interoperability between smart home devices and blockchain networks. The paper tackles wireless home technology, interoperability in the home, connectivity control, electronic billing of networks and municipal resources, and healthcare. Consequently, the access layer serves to interact with devices at the intersection layers such as at the individual level, the customer level (mainly for tech companies, including for marketing and use in retail), as well as for the corporate level as the topmost “layer” of the smart home, which primarily influences entities to take opportunity of the blockchain smart home ecosystem, which is a huge market.

With smart appliances, smart technology, and smart upgrades, smart home architecture is the tip of the iceberg; it is going to be a cornerstone of the smart home for smart households. Living in a smart home environment includes having a smart scan of one’s home with rooms, locking doors, smart devices that trigger conditions, and more. Through the functions provided with the smart home, the user can regulate remote electricity, set off alarms, watch and secure their home with video monitoring, and control their vehicle, among several more applications. A user-friendly, custom-integrated framework that would enable the homeowner to enable it on request should be introduced to increase the seamless activity of smart homes and detect any disruptive behaviors by hackers. For an IoT system, the user’s permission authorization can be listed in a collection of IoT system control records, a specified set of IoT system owner records, or a specified set of IoT system owner list records. Many sources that preserve trustworthy information must store those pieces of information to withstand the assaults of hostile attackers.

To explain how blockchains will contribute to secure access, we present the following explanation.

* + - First, the consumer must decide the access level and add it to the home service computer. For example, at the highest level, the homeowner (Admin) is allowed, while teenagers, youths, visiting relatives, and adolescents need mid-level permission.
    - For a user who has access to the smart home and is using applications inside, Figure 4 shows how blockchain facilitates secure entry.
    - Relatives and visitors have relatively poor access permits. When processing a request from the client, the home server checks security access to repositories. Upon receiving an order from the customer, the home server transmits the encrypted username and password to the blockchain layer.
    - For various users and implementations, a blockchain regulation header contains a set of authorization rules.

The part of the block data used for applying control policies and services is the policy header.

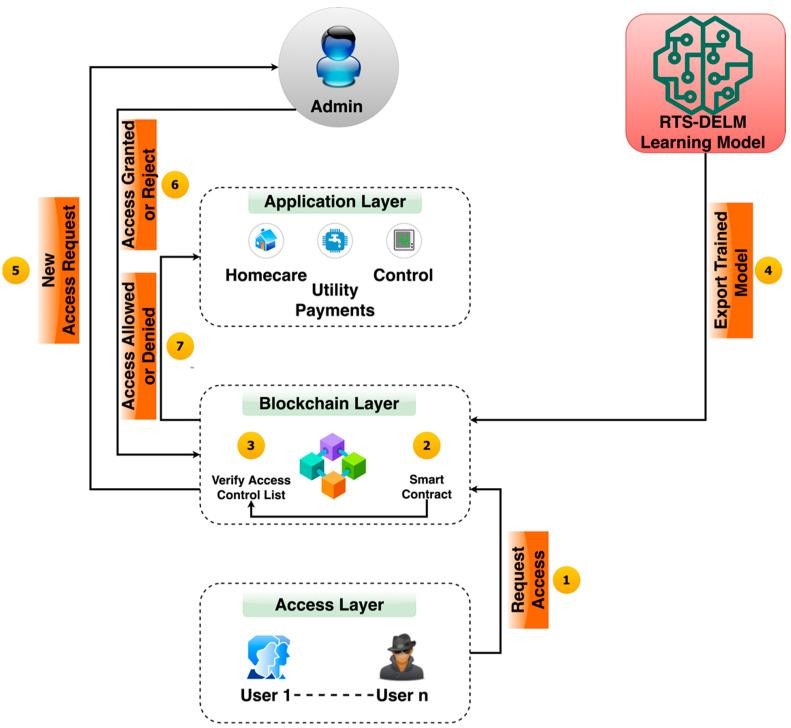
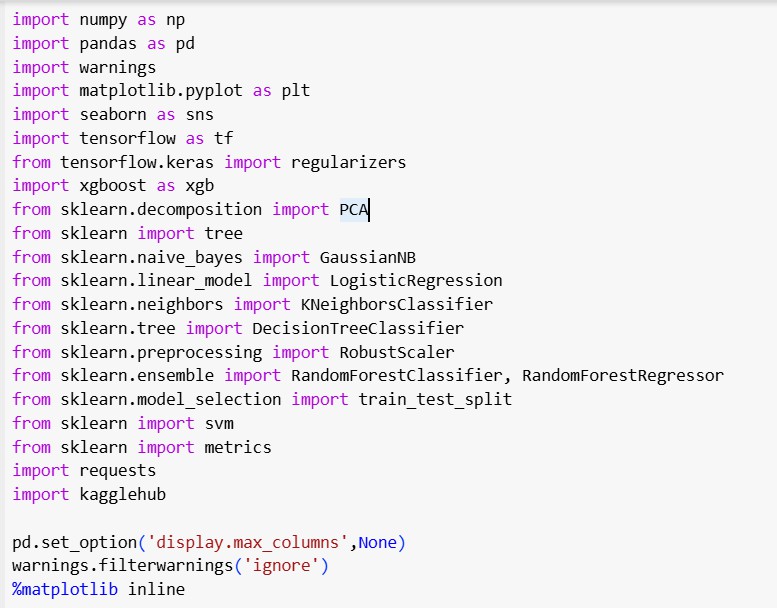


Figure.4. Proposed blockchain-based smart home management system.

The administrator checks the new user’s request and then accepts or rejects the access request. When the information is incorporated into the blockchain, miners take action depending on the policy specifics added to the header. This mechanism is successful in combatting malicious attackers.

* 1. Real-Time Sequential Deep Extreme Learning Machine.

RTS-DELM combines a variety of hidden layers, multiple hidden neurons, and a variety of different activation functions to provide the ideal solution for improving smart home networks. The proposed technique comprises three different phases: gathering the data, reviewing it, and presenting it. We have two sub-layers in the application layer (there are also additional layers in-between), where one is for estimation and the other layer is for assessment. While experimenting, data were collected from sensors for observational investigation. The data obtained through the data collecting mechanism were then made available as input to the data collection mechanism.

Until final processing, many data processing techniques were used to eliminate anomalies from the results. Finally, the RTS- DELM algorithm was utilized to improve smart home networks to prevent disruptive or intrusive behavior.

The RTS-DELM method applies to a wide variety of smart home applications. To maintain the requisite detection accuracy, a significant fraction of sensor readings is frequently required. RTS-DELM addresses a variety of network access concerns through the use of integrated routing and security measures. However, given that 80% of a network’s energy is used during data transmission and reception, data reduction and function abstraction approaches may help to reduce processing time and increase the endurance of neural networks. However, excessive compression will increase energy expenditures. Within smart home networks, RTS-DELM enables more efficient data compression. As a result, intelligent home networks require real-time networking solutions for security, scheduling, monitoring, clustering nodes, data aggregation, and fault diagnostics. The RTS-DELM design enables smart home networks to react smoothly to their changing environments.

In real-time, an RTS-DELM algorithm based on Deep Extreme Learning Machine (DELM) examines the data sequence. The DELM may be used in a variety of applications and domains to forecast health problems, assess energy consumption, inventory services, and specify transportation activities. The RTS-DELM may be used to categorize and regressively dedicate data in a variety of ways since it is intuitive and efficient at keeping up with the intricacy of frameworks. An extreme learning computer is a feed-forward neural network architecture that ensures that feedback can only shift one direction through those various layers, but “back-propagation” through the initial neural network can be consistently modified without error in the initial training process, where information passes through the initial neural network and advances in reverse through the corresponding error rate of achieving high precision at low errors. The weights in the model are constant throughout the validation phase of the system, in which the validated model is imported, the real data are predicted, and the precision of the model improves. There are several hidden layers and at least one output layer in the RTS-DELM model, as well as an input layer. Following conditioning, the framework is transported to the cloud for online use, and it is then utilized for validation services throughout the cloud during the validation process, as shown in the following diagram. In the assessment layer, the Mean Square Error (MSE) was examined to enhance smart home networks

and other connected devices. Figure.5. Implementation of the Proposed Model

1. RESEARCH RESULTS AND DISCUSSIONS

The Fused RTS-DELM method was applied to the fused dataset in this research. The findings were distributed randomly between the training collection (126,238 samples) and the test/validation set (15% of the tests) (22,278 records). The data were evaluated in advance of their intended usage to ensure that they were error-free. The RTS-DELM method needed to know if its machines had been affected by ransomware or other cyber threats. Following that, we examined several neurons, including the activation of buried layers and numerous types of active activities. In research designed to determine performance, we successfully evaluated the production of RTS-DELM. To assess the RTS-DELM algorithm’s performance, we used a variety of statistical measures that explained the result.

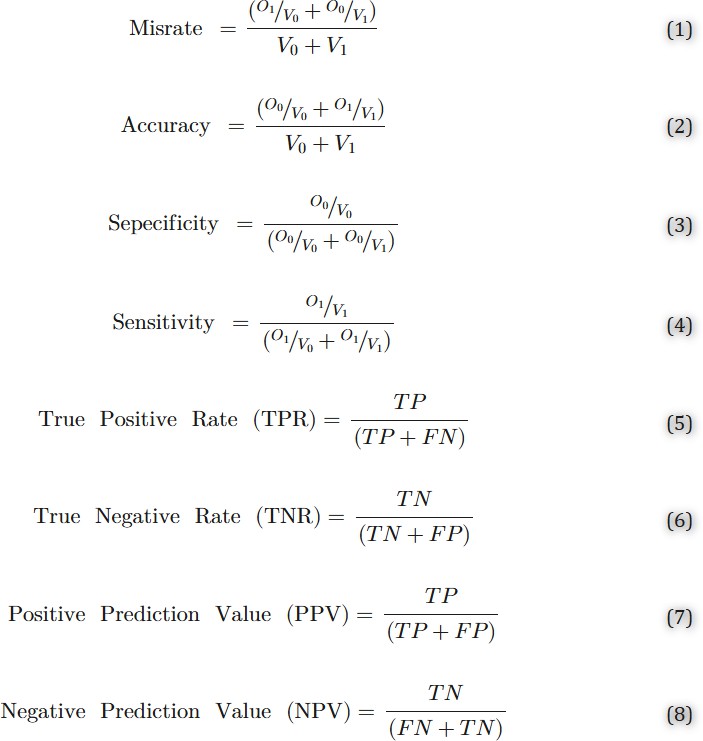


Table 1 shows the suggested RTS-DELM-based decentralized smart home network framework to predict intrusion detection during the training level. Throughout the training, a total of 126,238 recordings were used, divided into 65,495 and 60,743 normal and assault records, respectively. As a consequence, it is seen that the forecasting system properly anticipates 64,185 attack records of normal groups without a genuine attack while forecasting 1310 attack records incorrectly. In comparison,

60,743 records are obtained in the event of an attack, of which 58,707 are appropriately predicted as an attack and 2036 are incorrectly forecasted as a regular activity while the attack occurs.

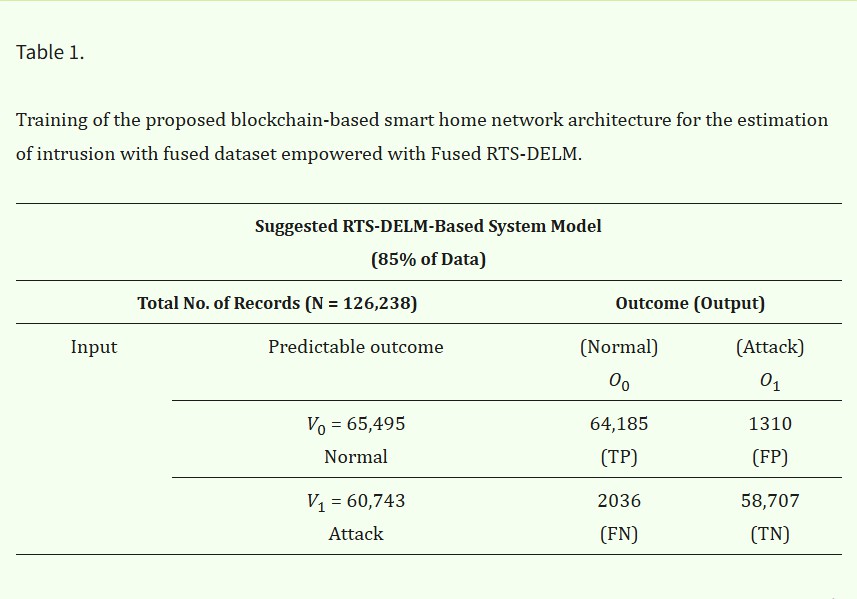


Table 2 shows the suggested RTS-DELM-based decentralized smart home network framework to predict intrusion detection during validation level. Throughout the validation, a total of 22,278 records were used, divided into 11,558 normal and 10,720 assault records. It is seen that 11,072 records of normal class with no attack identified are properly predicted, whereas 486 records are forecasted falsely as having an attack, despite the absence of a genuine assault. In the event of a cyber-attack, 10,154 of the 10,720 data points collected were properly predicted as invasions, whereas 566 were incorrectly predicted as normal activities throughout the attack.

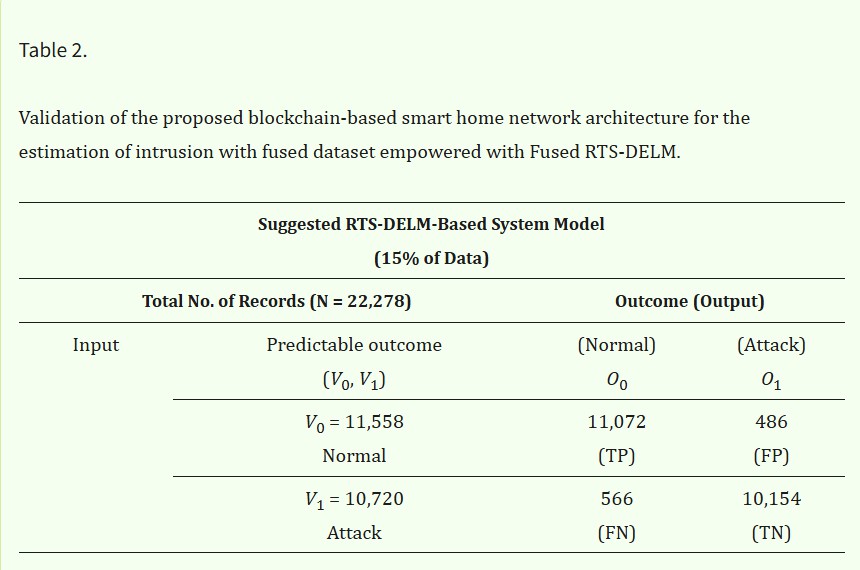


Figure 5 shows the assessment of the proposed RTS-DELM- based decentralized smart home network framework in terms of accuracy and the misclassification rate at the training and validation levels. It was proven that the proposed RTS-DELM- based decentralized smart home network system achieves a combined accuracy and misclassification rate of 97.35% and 2.65%, respectively, during training. Additionally, during validation, the proposed RTS-DELM decentralized smart home network system achieves a combined accuracy and misclassification rate of 95.28% and 4.72%, respectively.

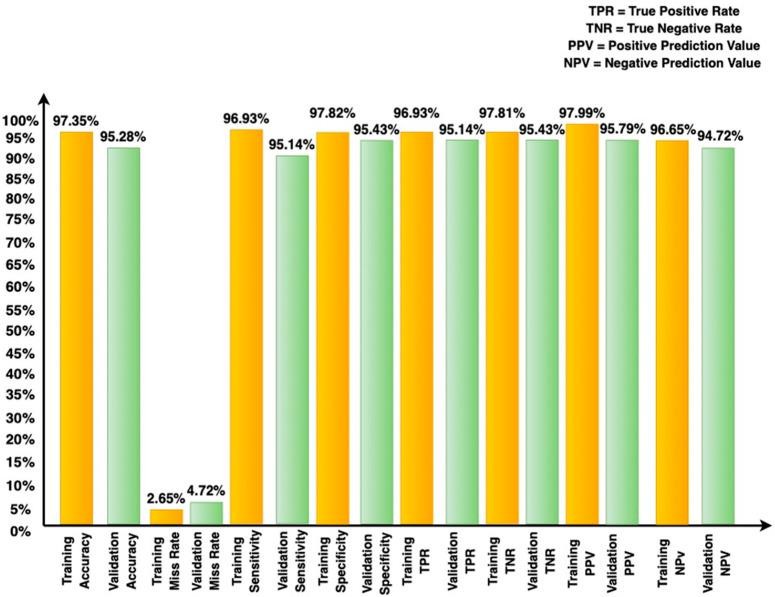


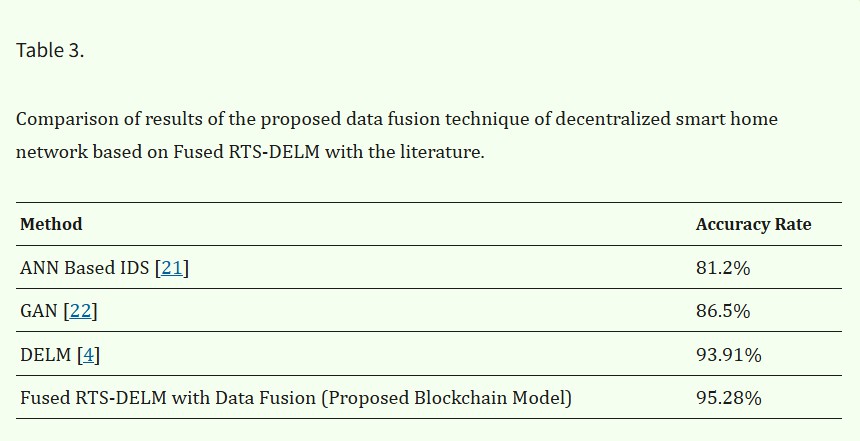
Figure.5. Different statistical measures for the proposed blockchain-based smart home network architecture for the estimation of intrusion with fused dataset during validation and training.

Figure 5 illustrates the proposed blockchain-based smart home network security system’s effectiveness in various statistical parameters during the training and validation phases using the Fused RTS-DELM proposed framework. This demonstrates unequivocally that the suggested method generates accuracy and misclassification rates of 97.35% and 2.65%, respectively, during training. During validation, the suggested system achieves an accuracy rate of 95.28% and a misclassification rate of 4.72%. Additionally, it demonstrates the performance of the system model in terms of sensitivity, specificity, and true positive rate. (TPR), true negative rate (TNR), positive

predicted value (PPV), and negative predicted value (NPV) during the training and validation phases.

We evaluated the dependability of our technique on the reliability of other published algorithms in the literature; in addition, as shown in [Table 3,](https://pmc.ncbi.nlm.nih.gov/articles/PMC9227380/#sensors-22-04522-t003) the suggested framework achieves much higher accuracy by reducing the error rate. In terms of accuracy, the proposed RTS-DELM framework outperforms existing algorithms already in use, such as the Artificial Neural Network-based Intrusion Detection System

[[21](https://pmc.ncbi.nlm.nih.gov/articles/PMC9227380/#B21-sensors-22-04522)] and Generative Adversarial Networks (GANs) [[22](https://pmc.ncbi.nlm.nih.gov/articles/PMC9227380/#B22-sensors-22-04522)] and Deep Extreme Learning Machine (DELM) [[4](https://pmc.ncbi.nlm.nih.gov/articles/PMC9227380/#B4-sensors-22-04522)]. When compared to the DELM technique, the suggested RTS-DELM method achieves higher efficiency on the fused dataset because of the enhanced accuracy achieved [[4](https://pmc.ncbi.nlm.nih.gov/articles/PMC9227380/#B4-sensors-22-04522)]. In [[21](https://pmc.ncbi.nlm.nih.gov/articles/PMC9227380/#B21-sensors-22-04522)], the authors suggested an Artificial Neural Network-based Intrusion Detection System, and, in this method, the researchers achieved 81.2% precision. In [[22](https://pmc.ncbi.nlm.nih.gov/articles/PMC9227380/#B22-sensors-22-04522)], the researchers suggested Generative Adversarial Networks (GANs), and in this method, the researchers achieved 86.5% accuracy. Finally, in the DELM approach without data fusion, 93.91% accuracy was achieved [[4](https://pmc.ncbi.nlm.nih.gov/articles/PMC9227380/#B4-sensors-22-04522)]. In this study, the RTS-DELM system achieved an accuracy of 95.28%, which is greater than prior attempts, demonstrating its efficacy and demonstrating that the system performance is improved by employing the data fusion technique. The suggested RTS- DELM paradigm provides a much higher return on investment than existing methods. As a result, the RTS-DELM paradigm that has been proposed gives a viable solution to the aforementioned issue.



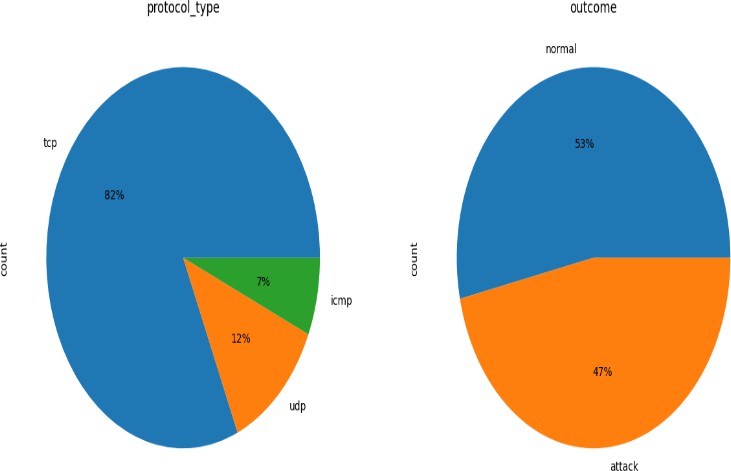


Figure.6. The Average Outcome of the Smart Home Terminal Device's Signature Method Examination

The applicability of the authentication protocol in a smart home context is first examined. The equipment of the smart home simulation environment, as per the concept suggested in this work, comprises a smart electronic endpoint unit and a home gateway host. The minimum group authentication scheme is uplinked on these systems, and the simulation findings are shown in the figure below. The ordinate in Figure 13 represents the mean time spent in various stages of the system during the operation of 82%, 7%, 12%instances, respectively, and the distance between A, B, and C symbolizes the 3 phases of signature verification, signature generation, and key generation in the authentication protocol.

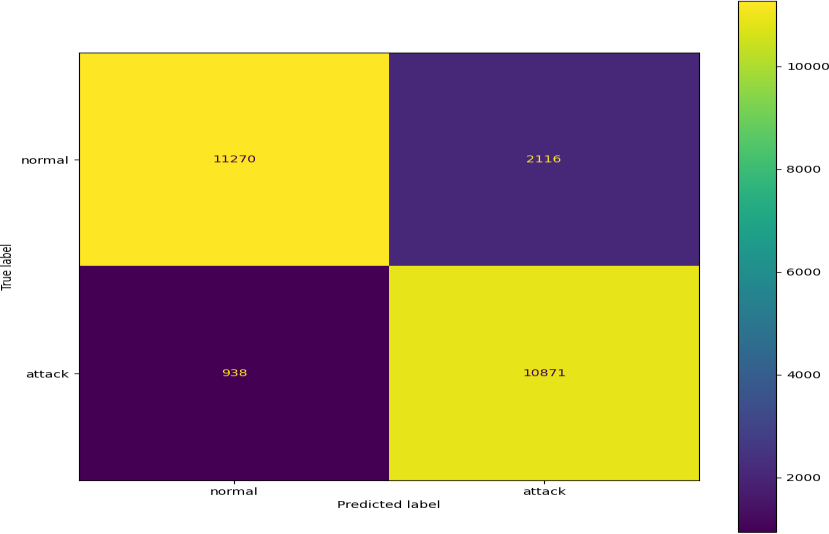
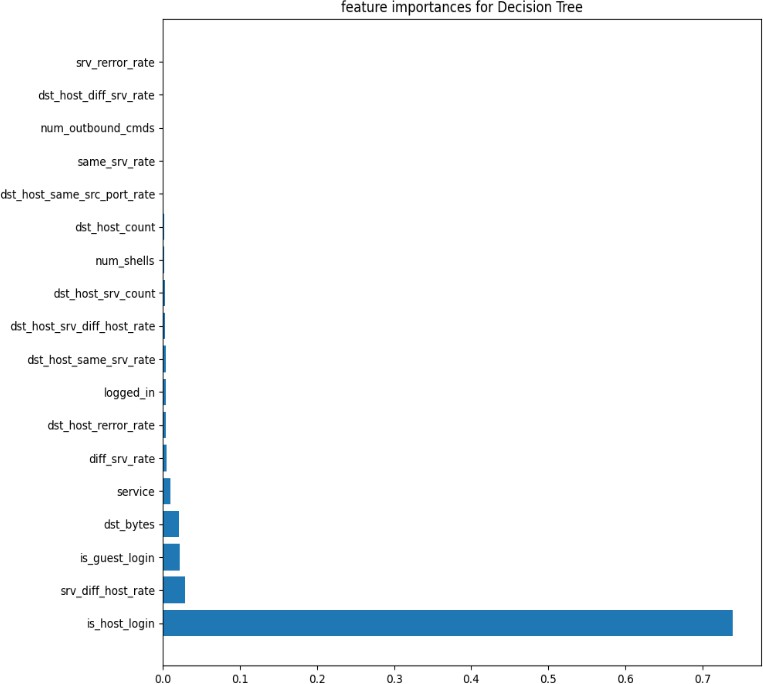


Figure.8.

Figure.7.Feature Importance For Decision tree

Decision trees in machine learning (ML) are used to structure algorithms. A decision tree algorithm helps split dataset features with a cost function. Through a process called pruning, the trees are grown before being optimized to remove branches that use irrelevant features. Parameters like decision tree depth can be set to lower the risk of an overly complex tree or overfitting.

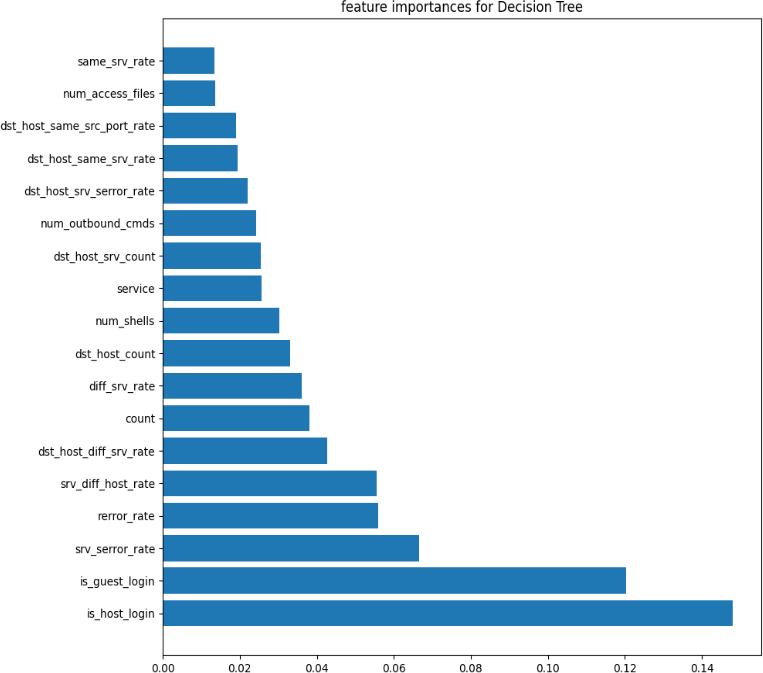
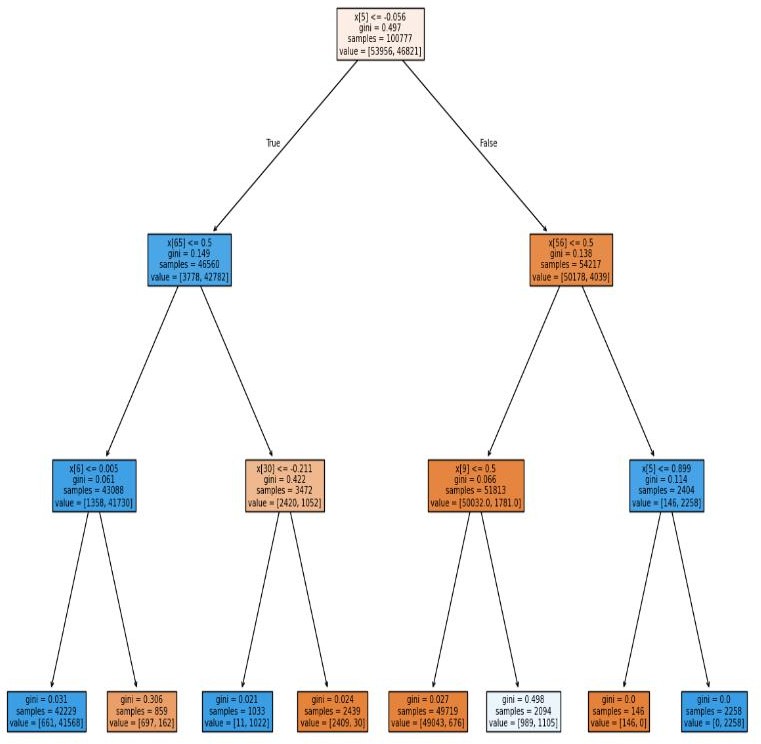
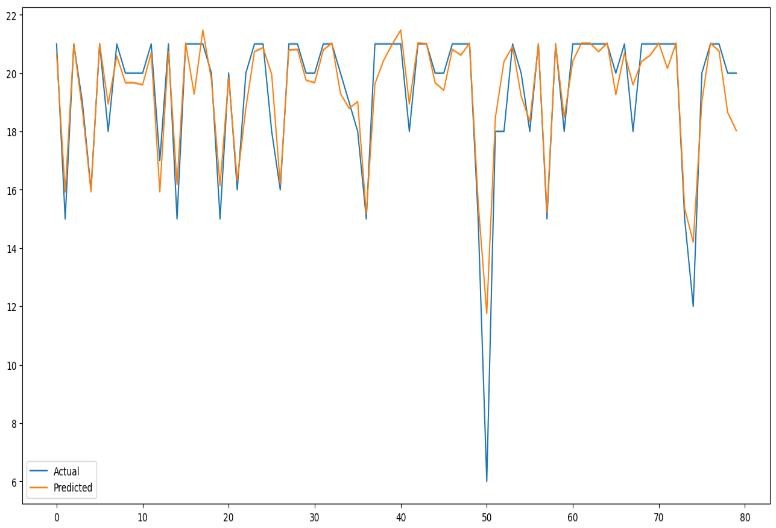


Figure.9.Importance For Decision Tree

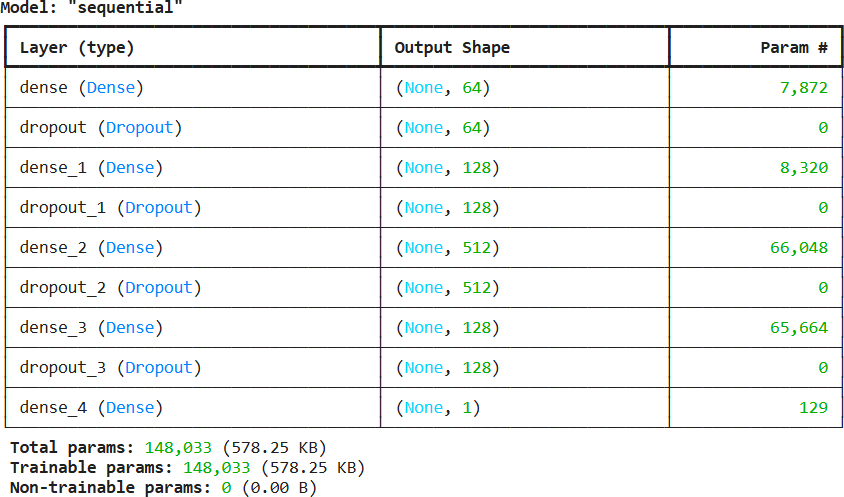




Decision trees are used to solve classification problems and categorize objects depending on their learning features. They can also be used for regression problems or as a method to predict continuous outcomes from unforeseen data.

guidelines are used for equipment and service discovery smart home systems. Every host represents a real-world home outfitted with smart home technology.

The time taken by the smart home devices performing each cycle of the authentication protocol is visible in Figures 13 and 14, suggesting that the authentication scheme has high stability and is within the appropriate time range of real application situations. Figure 15 depicts the overall mean time spent on each of the two devices' three stages. Figure 15 shows that the authentication technique suggested in this work performs well in meeting security features and computation complexity. As a result, based on simulations in the previous chapter, the minimum authenticated key agreement method described in this work may match the acceptance criteria of smart home contexts and have a promising application possibility. The simulation platform is then used to create a smart home authentication mechanism based on blockchain to demonstrate the feasibility of the proposed concept. This section will cover the operational specifics, including blockchain and a smart home ecosystem. The system's efficiency is then assessed via simulated experiments.



1. CONCLUSIONS AND FUTURE WORK

In this study, the idea of a smart contract in blockchain technology is employed to validate the user’s identity for accessibility to centralized smart home services. The most significant benefit of this research is the demonstration of how easy it is to receive facilities and how secure the resources are. There is no need to have redundant authentication because no

other third-party users can access smart home systems, even if another user tries to access an already used resource. Intrusion detection in smart homes, especially in the context of assessment and prediction, remains a key concern. In the meantime, recent advances in the blockchain and machine learning sectors have demonstrated tremendous promise to accomplish these aims. Discussing the need for an efficient approach, this study provided a compact and efficient mechanism for intrusion prevention. An RTS-DELM approach was developed, and also data fusion techniques were presented to optimize multi-sensor networks. Numerous measures were used to assess the feasibility of the proposal. The consistency of RTS-DELM findings showed that the proposed method is more successful than others. The suggested RTS-DELM solution obtained an exceptionally high rate of success, showing 95.28% accuracy. The findings obtained are encouraging, and we will continue to investigate more applications for the device through the deployment of more datasets and varying frameworks. Blockchain technology can establish new doors for cutting edge smart home systems. Nevertheless, some difficulties must be addressed before blockchain is widely adopted in the smart home infrastructure. Developing an interoperable system is difficult due to many blockchain systems' varied file formats and transaction runtimes. Information security is a big problem, and it is linked to three states: data leaving the source, data in motion, and data arriving at the target device. Another challenge when designing an interoperable framework is the different consensus processes used by independent blockchain systems. Transporting data from one blockchain to another is necessary to create a smooth application development environment. Smart home blockchain technology to reduce processing time Blockchain for smart homes that are flexible: Whenever the quantity of devices in the system rises, the scalability of the smart home blockchain falls considerably. This is because the multiplication of nodes increases the danger of data inconsistency owing to varying throughput. Centralized systems may be retained since homeowners seek a smooth service with the least hardware expense. A typical blockchain's heavyweight hardware architecture is a strain for a small smart home network, where devices have limited resources. As a result, lightweight blockchain technology necessitates increased acceptance and longterm durability and scalability. Considerable research has attempted to provide lightweight frameworks by incorporating shared overlay networks, cluster heads, data structures for block headers, etc. Nevertheless, such research yields only a modest decrease in storage and is based on security assumptions. These assumptions result from a lack of comprehensive testing to guarantee vulnerability in real- world settings.

The proposed system for the smart house network environment has to be improved further to solve the following specifications:

* Mutability and Ongoing Access Control: given the volatility of a smart home IoT ecosystem, access monitoring is needed to manage and regulate access even after it has been granted, and often users require a quick modification. Furthermore, access limits must be used as a consumable, non-refundable quantity of accessibility to some services. For example, the available time for children to use the PlayStation on holiday needs monitoring, and access should be withdrawn promptly (ongoing control) if it is depleted (mutability).
* Conflicts: users may not have policy disagreements since the proposed platform does not include any unfavorable policies; rather, it uses restrictive allocations to prevent a position from being granted certain privileges. Nevertheless, it is conceivable for administrator agendas to conflict. Various users, for example, set the smart thermostat to varying temperature settings. Because customers anticipated discrepancies to be handled autonomously based on a survey of access control demands in a smart home, it is strongly advised that a policy mediation mechanism be implemented into a smart home's access control scheme.

1. REFERENCES
2. Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. Decentralized Bus. Rev. 2008;10:21260. [Google Scholar]
3. Aggarwal S., Chaudhary R., Aujla G.S., Kumar N., Choo K.K.R., Zomaya A.Y. Blockchain for smart communities: Applications, challenges and opportunities. J. Netw. Comput. Appl. 2019;144:13–48. doi: 10.1016/j.jnca.2019.06.018. [DOI] [Google Scholar]
4. Andoni M., Robu V., Flynn D., Abram S., Geach D., Jenkins D., McCallum P., Peacock A. Blockchain technology in the energy sector: A systematic review of challenges and opportunities. Renew. Sustain. Energy Rev. 2019;100:143–174. doi: 10.1016/j.rser.2018.10.014. [DOI]

[Google Scholar]

1. Khan M.A., Abbas S., Rehman A., Saeed Y., Zeb A., Uddin M.I., Nasser N., Ali A. A machine learning approach for blockchain-based smart home networks security. IEEE Netw. 2020;35:223–229. doi: 10.1109/MNET.011.2000514. [DOI] [Google Scholar]
2. Zhou Z., Wang B., Dong M., Ota K. Secure and efficient vehicle-to-grid energy trading in cyber physical systems: Integration of blockchain and edge computing. IEEE Trans. Syst. Man Cybern. Syst. 2019;50:43–57. doi: 10.1109/TSMC.2019.2896323. [DOI] [Google Scholar]
3. Wu J., Dong M., Ota K., Li J., Yang W. Application-aware consensus management for software-defined intelligent blockchain in IoT. IEEE Netw. 2020;34:69–75. doi: 10.1109/MNET.001.1900179. [DOI] [Google

Scholar]

1. Lee B., Malik S., Wi S., Lee J.H. International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness. Springer; Cham, Switzerland: 2016. Firmware verification of embedded devices based on a blockchain; pp. 52–61. [Google Scholar].
2. Lee B., Malik S., Wi S., Lee J.H. International Conference on Heterogeneous Networking for Quality, Reliability, Security and

Robustness. Springer; Cham, Switzerland: 2016. Firmware verification of embedded devices based on a blockchain; pp. 52–61. [Google Scholar]