Smart Home Secure Network using Decentralized Infrastructure and Machine Learning Techniques

Habib Yassin-Kazem
Department of Computer Engineering, Faculty of Engineering, Central Tehran Branch
Islamic Azad University
Tehran, Iran
enghabeb54@gmail.com

Imam Attarzadeh
Department of Computer Engineering, Faculty of Engineering, Central Tehran Branch
Islamic Azad University
Tehran, Iran
Iman.Attarzadeh@iauctb.ac.ir

***Abstract*— Security vulnerabilities in telecommunications networks have become an important issue due to the significant growth of gadgets for smart homes. and its connectivity via the Internet of Things (IoT) This research supports the smart home network learning engine using secure communications based on the blockchain system and evaluation layers based on cloud systems for determine their priorities and classify them into three kinds of coefficients (T): Avoid T. Smart T and Mod T. The learning engine uses a neural network to train and classify these types and the blockchain helps layer make more effective decisions. Key contributions of this study include implementing a secured blockchain layers for user authenticating and creating a ledger for the communication networks. Besides, using of a cloud-depend datas assessment layers, the development of the SI-depend teaching algorithm, and the complementarity of a neural engine for accurate classification are highlighted. The suggested algorithm excels the sequentially deep learning machine (RTS-DELM), data fusion techs., and IoT AL. technologies in affording electronic information engineering and improvement strategy analysis. This is achieved by reducing computational complication, false authentication rates, and quality parameters, ensuring a safty and effective smart home communication network that improves human life style.**

Keywords—Lunberg Model, Lunberg Model, Blockchain, Consensus Protocol, Dragonfly Algorithm, Smart Contract

I. INTRODUCTION

As a result of rapid technological progress, advanced technologies have introduced smart devices that can monitor home management and thus improve human lifestyle. These devices, known as smart home appliances, are connected to each other through Internet of Things (IoT) technology. This infrastructure allows devices, especially smart devices, to communicate and exchange information. From 2018 to 2022, the smart home industry witnessed a significant growth rate, with the annual number of smart home applications increasing from 500 million to 700 million devices [1].

The security and privacy of smart homes are crucial for data transmission. Five aspects are authentication, authorization, confidentiality, consolidation, and availability. A network that has a lot of connected devices may be more susceptible to security risks. To address this, a supervised approach to analyzing data generated by IoT networks can be beneficial. Swarm intelligences are suitable for handling Np-hard problem and feature extraction, while meta-heuristic techniques, such as population-based meta-heuristic algorithms, are efficient for multi-objective problems. Implementing a combination of these techniques can enhance the security and privacy of smart homes by ensuring data is securely transmitted and protected from potential threats. Additionally, continuous monitoring and updating of security protocols can help mitigate risks and safeguard the network from cyberattacks [2]. The dragonfly algorithm is a trustworthy method for selecting data that can spot patterns and trends in data sets, particularly when it comes to identifying anomalies and exceptional data. Deep learning and decentralized frameworks are presented, and the suggested paradigm is a noteworthy development in information engineering. It beats existing techniques like data fusion techniques, real-time serial profound learning machine systems (RTS-DELM), and Internet of Things artificial intelligence technologies. Furthermore, the proposed model also offers improved scalability and efficiency in processing large volumes of data. This makes it a valuable tool for organizations looking to enhance their data analytics capability and refined processes of making desision [4, 5, 6]. Using this technology lowers the possibility of illegal access and data breaches, making it a dependable alternative to institutions handling sensitive data [7, 8]. This study focuses on developing a learning engine integrated with this network communications, using a neural-based propagation engine to decide on smart transactions, Fig. 1 illustrates average transactions as well as transactions that should be banned.

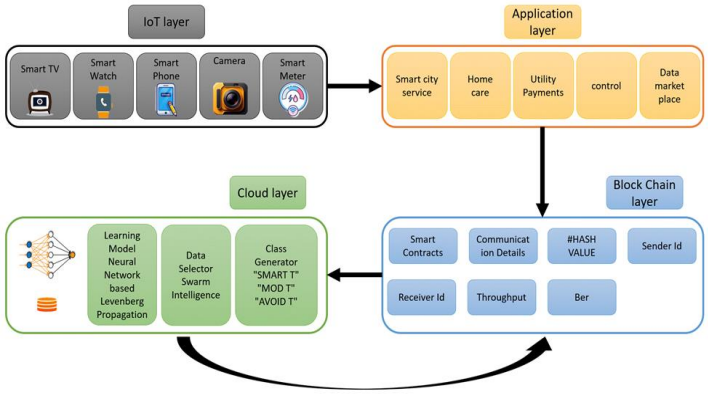

Fig. 1. Skeleton of Smart Home App.

As described in Fig. 1, the application architecture comprises four layers, with the IoT layer being the primary layer where users communicate through various devices. The application layer provides a best way for user to send and process requests, encompassing areas like home care, hospitals, utilities, data, and markets. Data layers are official for hoarding and managing vast amounts of information collected from the IoT devices, ensuring data integrity and security. The market layer analyzes trends and patterns in user behavior to provide valuable insights for businesses and organizations to make informed decisions. This data is accumulated through the blockchain layer, which creates a ledger of communication details and provides comprehensive information about transactions. Treatments are implemented across smart contracts, and layers of blockchain generate data related to quality-of-service parameters like operation speed and bit error rate [9, 10, 11]. "SMART T," "MOD T," and "AVO-T." Crowd-based ction algorithm data selections are integrated to reduce data replication, and the data is fed into a neural engine for structured learning. The layers of cloud assist layers of blockchain in transaction for processes to decision-making. By leveraging the combined capabilities of the blockchain and cloud layers, the system can optimize transaction efficiency and accuracy. This integrated approach ensures that transactions are executed seamlessly while maintaining high standards of quality and reliability.

In this work, using abbreviations RF for Random Forest, NB for Naive Bayes and P for proposed result. The contributions of this article are:

1. Introducing a new algorithm that combines blockchain technology and neural networks for secure and efficient smart home communication.
2. Implementing a cloud-based evaluation data layers to categorize and prioritize data into three main transaction types: Smart T, Mod T, and Avoid T.
3. Development of a neural network-based learning engine to train and classify these categories, helping the blockchain layer to make more effective decisions.
4. Increased security through a secure of layers blockchain for authentication users and a ledger for communications network.
5. Enhancement of SI-depend method for training and neural engine application for precise category classification and training.

(a) Data fusion technicians find that the suggested technique performs better than the sequential deep learning machine (RTS-DELM) system., and IoT AL. technology in providing (ectronic and engineering) informations, also to optimization design analysis. It achieves this by providing a lower average computational complexity, a more secure smart home communication network, and improvements in false authentication rates and quality parameters, thereby improving human lifestyles.

(b) Implementing a secure layers blockchain for authentication users and ledger creation for communications network further enhances security.

(c) Integrating a cloud-based evaluation layers data to separate and data processes create a ranking model based in three transaction categories, help better data management.

(d) The use and improvement of the SI-based algorithm improves the training accuracy in the cloud layer and leads to more accurate data analysis.

(e) Adopting a neural engine for training and classifying categories helps the layers blockckian to enhance decision-making processes, resulting in more efficient communication network management.

This paper provided an overview of researchs on enhancing smart home-based applications architecture, outlines proposed work integrating machine learning, blockchain technology, and crowd-based application architecture, presents empirical findings and discussion, and concludes with a conclusion in Section 5. The structure of the paper is comprehensive. The paper also includes a detailed analysis of the potential benefits and challenges of incorporating these technologies into smart home applications. Additionally, future research directions are suggested to further advance the field of smart home-based application architecture.

II. RELATED WORK

This review explores into recent research in smart home technologies, with a focus on peer-to-peer energy trading, blockchain-based network security models, and data security models. The authors explain the notion of peer-to-peer energy trading, which involves communication between networked devices via a routing topology. They also talk about a blockchain-based smart home network security architecture that employs a decentralised network and machine learning to optimise calculations and distributions in smart device interactions.

The authors present a data security model for smart homes using blockchain tech., which improves system security by documenting communications and transactions. They introduce an encrypted communication index called a hash value stored in an open-source ledger, which allows for the adjustment of operational phases. Furthermore, the model includes a consensus algorithm that ensures the integrity of data exchanges within the network. This approach enhances the overall security and efficiency of smart home systems by leveraging blockchain technology [12]. The authors evaluate a machine learning intelligence approach to reduce the costs of smart homes, focusing on energy consumption. They use a training and classification mechanism to gain insight into the system. They also introduce smart home networks developed using an occupancy detection model based on operable building automation technologies. The integration of machine learning intelligence allows for more accurate predictions and adjustments to optimize energy usage in real-time. This innovative approach not only reduces costs but also enhances the overall sustainability of smart home systems [7, 8]. The authors highlight the importance of security, power, and performance considerations for blockchain-based IoT frameworks and systems. They explore communication and the modelling of data transfer channels. Efficiency is the primary goal, with various optimisation techniques being implemented to cut energy usage and improve efficiency in smart homes and IoT devices.

One algorithm, inspired by the bat algorithm with inertia weight, optimizes energy consumption and increases comfort levels. Additionally, the authors delve into the integration of renewable energy sources to further enhance sustainability in smart home systems. They also emphasize the need for continuous monitoring and updates to ensure the security and efficiency of blockchain-based IoT frameworks [8, 10].

The authors propose the adoption of a communication protocol based on the Message Queuing Telemetry Transfer Protocol (MQTT) to enhance the performance of IoT devices. They recommend task management for the IoT, which relies on predictive optimization to improve energy efficiency and scalability in smart residential buildings. By implementing these optimization algorithms and communication protocols, smart homes can achieve significant reductions in energy consumption while maintaining high levels of comfort for residents. The integration of predictive task management further enhances the overall efficiency and scalability of IoT devices in residential buildings. In addition, the use of MQTT allows for real-time data transfer and communication between devices, enabling seamless integration and automation within smart homes. This holistic approach to IoT optimization not only benefits energy efficiency but also contributes to a more sustainable and convenient living environment for residents [10, 11]. The contributions and potential applications of this framework are summarized in Table 1.

TABLE I. ANALYSIS AND COMPARISON OF EXISTING METHODS

Author/Citation	Implemented Technology	Methodology	Findings
Alam et al. (2019) [2]	Smart home	Peer-to-peer energy trading with routing topology	Cost saving is not directly proportional to the increase in the usage of renewable resources
Tchagna Kouanou et al. (2022) [5]	Smart home data security using Blockchain technology	Blockchain interpretation was used to keep communication records	Enhancing security of the overall system via encrypted communication index
Mansouri et al. (2023) [8]	Hierarchical decentralized framework technology	Deep learning-based forecaster and risk-aware information gap decision theory was employed to design efficient smart homes	The smart prosumer's illustrated reduced energy requirements
Alzoubi et al. (2022) [11]	Machine learning technology	Involved bat optimization technique for reduced energy consumption of the smart home	Using machine learning for intelligent evaluation of energy consumption and finding the least used and highly used resources
Rivera et al. (2015) [12]	Automation technology	Built smart homes using interoperable automation using neural networks	Designed efficient smart homes with reduced energy consumption
Vanus et al. (2022) [17]	Occupancy detection for smart homes	Propagational neural networks	Developed an occupancy detection model and utilized the cloud for data centralization and monitoring purposes
Our proposed method	Machine learning technology and Blockchain	Real-Time Sequential Deep Extreme Learning Machine	It is the ease of obtaining facilities and the security of resources. There is no need for additional Authentication and data fusion techniques are also presented to optimize multi-sensor networks.

TABLE II. EVALUATION PARAMETERS

Author	Statistical Measure	Number of Collected packets	File size (Bytes)	Amount of Collected (Bytes)	Average Data Transfer Rate (B/s)
Alam et al (2019) (2)	Mean	4958	8,318,400	4,119,314	4.1
Vanus et al. (2022) [17]	Median	2048	1,200,000	1,167,360	6.5
Qamar et al. (2022) [13]	Median	1000	1,048,576	982,254	6.5
Kumar et al. (2022) [14]	Mean	50	10,111	3424	0.5
Khanpara et al. (2023) [15]	Mean	15,360	1,094,430	748,408	4.5
Malek et al. (2022) [18]	Mean	1000	32,000	15,814	6.2
Devassy et al. (2022) [19]	Mean	100	15,423	4846	0.6

III. METHODOLOGY

The suggested project seamlessly combines home smart design with a machine learning framework that incorporates Levenberg-based model systems to train and classify data generated by classes. This project is divided into two main parts: the blockchain layer and the cloud layer.

A. Blockchain layer

The proposed framework uses the blockchain layer to record user transactions and the utility layer for data hosting. Blockchain is a revolution. Technology can revolutionize various industries and sectors by replacing manual processes with automated ones, simplifying, accelerating, and strengthening transactions security. It eliminates the need for third-party intermediaries and provides numerous benefits in everyday life. By leveraging technologies of bolckchaine, the framework ensures transparency and immutability of user transactions, reducing the risk of fraud and manipulation. This innovative approach not only enhances efficiency but also promotes trust among users in a decentralized environment [14,15]. Blockchain technology has the potential to disrupt various industries by streamlining processes and reducing costs. Its decentralized nature also eliminates the need for intermediaries, making transactions faster and more secure. The most common cryptographic hash functions are SHA-1 and SHA-256, which plays an important role in securing numerous, websites and applications. Increasing the flexibility of blockchains. Firebase's blockchain architecture offers a range of features that can enhance the functionality and security of applications. By integrating these components into a project, Developers may take advantage of blockchain technology to construct more efficient and secure applications. [17,18]

The Firebase Config object contains various properties, such as API Key, AUTH Domain, Database URL, Projected,

Storage Bucket, AppId, and Measurement, which have unique values specific to a particular Firebase project. These properties are used by Firebase SDK to establish communication between the application and Firebase services. Additionally, developers can also utilize Firebase Authentication to easily authenticate users and manage user accounts within their applications [19,20]. This simplifies the process of implementing secure user authentication mechanisms without having to build them from scratch. The pseudocode specifies steps to initialized the firebase Config objects and set values for its charecterizations.

The Firebase config object begins with the following properties:

- API key
- Domain AUTH
- Database address
- Project ID
- Storage bin
- Application ID
- Measurement ID

The Api Key attribute values set to "AIzaSyD11_9I9_5yLJu0UCGa6SdiYFQTAiWoOe0".

AUTH domain attributes values set to "subhita-block-chain.firebaseapp.com".

Database URL attribute values set to "https://subhita-block-chain-default-rtdb.firebaseio.com" (accessed on 14 April 2023).

Project ID attribute values set to "subhita-block-chain".

The Storage Bucket property values set to "subhita-block-chain.appspot.com".

The appId values attribute set to "1:1038363801308: web: 338b2f2XXXX".

The measurements attribute values set to "G-38V0GXXX".

B. Cloud Layer

The layer cloud consists of three subsections: (Disaggregation-management) data and decision making integrated with training and classification, as shown below.

1-Data Separation

As shown in Section 3.1, the blockchain layer collects and organizes data in a ledger. In this research, used the K-means clustering algorithm to segment the data followed by statistical analysis to classify them into distinct categories. Fig. 2 presents a visual illustration of this method.

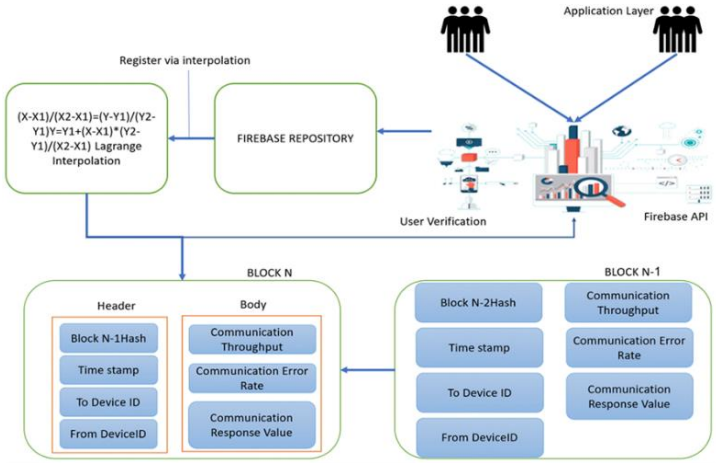

Fig. 2. Blockchain Layer and Their Produce

The collected data contaian three categories and the labeling process done by fuzzy logic. Algorithm 1 provides a visual representation of the disaggregation structures of data.

Algorithm 1: Data Separation Algorithm
1. Procedure 1: Data Segregation Procedure 2. Implement the data segregation process. 3. Input: Aggregated Data denoted as Ad 4. Begin 5. Utilize the k-means algorithm to segment Ad into three clusters, producing the cluster centroids in K_{cent} and the cluster indices in K_{index}. 6. Compute the Mean Squared Error (MSE_K) and Standard Deviation (STD_K) using Evaluated_MSE and STD (Ad, K_{index}).

Algorithm 1: Data Separation Algorithm
7. Set up the Mamdani Fuzzy Rule Set. 8. Assign the labels from K_index to GT (Ground Truth). 9. End Procedure

Algorithm 1 took the entire accumulated data as input and divided it into three separate categories as shown earlier. The detailed schematic of the operational model is shown in Fig. 3.

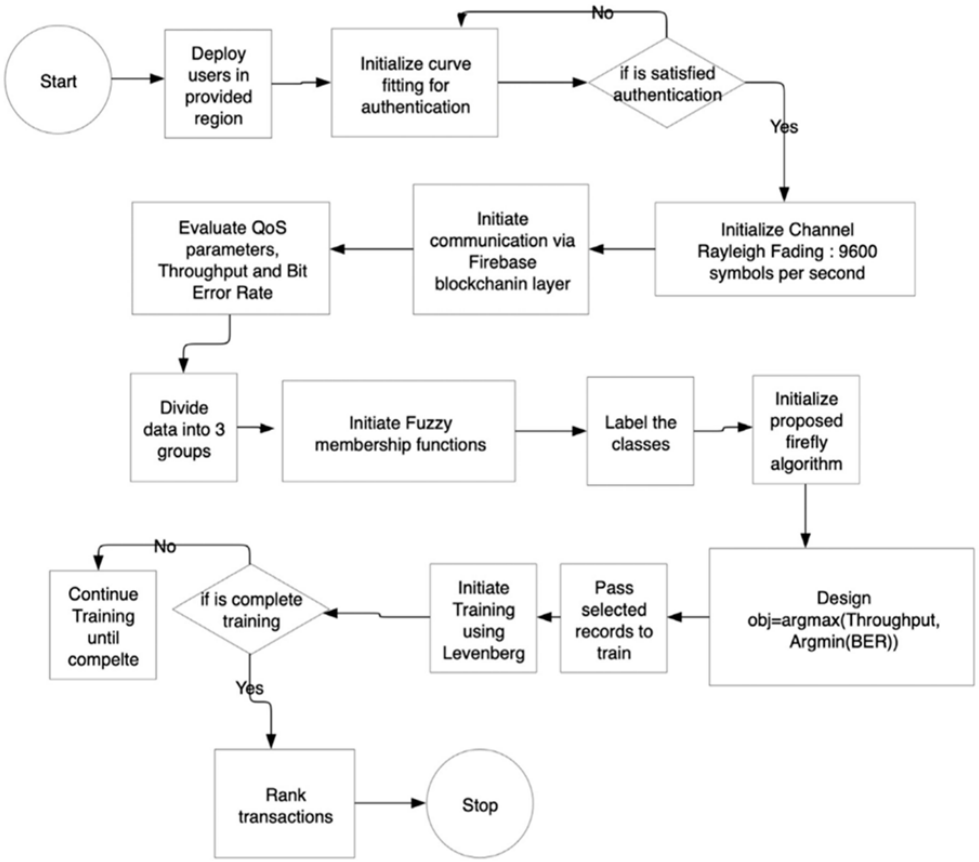

Fig. 3. Proposed Work Model

2- Data Selection for Ranking

The fuzzy inference engine produced a labeled dataset based on the evaluated quality of service (QoS) for transactions within the blockchain layer. In building a reputation system to strengthen the blockchain layers, this research used the dragonfly algorithm to select data based on class labels. The adoption of the dragonfly algorithm is in line with the previous discussions in the literature review outlined in Section 2.

The dragonfly algorithm is a highly efficient data selection method that detects patterns and trends in datasets, particularly outliers and unusual data. It divides the set datas into smaller subsets and iteratively selects the most optimal subset. This versatile algorithm, based on swarming principles, uses an attraction index to select and reject prey. The dragonfly algorithm is inspired by the hunting behavior of dragonflies, making it a unique and effective approach to data analysis [21, 22]. By mimicking the instincts of these insects, the algorithm can quickly adapt to changing data patterns and provide accurate results. It evaluates data points' proximity to the data set's center using Euclidean or Manhattan distances [23]. The dragonfly algorithm can handle both distance measures and factors in multiple dimensions during calculations. Its versatility makes it suitable for various dataset types. The algorithm's ability to adjust its attraction index allows it to efficiently filter out irrelevant data points and focus on those that are most relevant for analysis. This adaptability makes the dragonfly algorithm a valuable tool for researchers and analysts working with complex datasets [24].

AI calculations can be shown by equation (1). The fuzzy inferences engine provides a set labeled which results from the QoS service evaluation of transactions at the layers blockchain. To enhance system reputations for the layers blockchain, this research used the dragonfly algorithm to select a data record based on its class label. This selection method required the use of the dragonfly algorithm, as specified in previous research [25], to calculate the next state of the fly with (1):

$$x_i^{t+1} = x_i^t + \beta_0 e^{-\gamma r_{ij}^2} x_j^t - x_i^t + \alpha \quad (1)$$

In this scenario, $x_i^{(t+1)}$ signifies the subsequent state of a firefly, x_i^t denotes its current state, and α represents the randomization parameter within the range of 0 to 1. r_{ij} Denotes the distance between the positions x_i and x_j of two fireflies, where i and j are indices for the fireflies β. Denotes the attractive index, while γ indicates the change in the attraction index. Moreover, x_{gcd} represents the group centroid of the labeled route. The algorithm for the dragonfly approach is delineated in Algorithm 2.

Algorithm 2: Dragonfly Algorithm

$Dragonflies = [K\_index, Ad]$
$Dragonflies\_AK = Dragonflies.QoS$ # Extract QoS parameters for each extracted class
$G = 10$ # Maximum Generation
$Dragonfly_{Score_{Chart}} = Zeros(V, G)$
Initialize
score chart with zeros, where V is the total number of
while G:
  for i in $range(1, Dragonflies)$:
    $S\_tp = Rand\_index(Dragonflies, 30\%)$ # Generate a 30% random swarm population to pair
    $Sp = Dragonflies[S\_tp]$ # Extract the population attribute set
    for j in $range(1, S\_tp)$:
      $x\_i\_t = x\_i\_t.QoS$ # Extract attained QoS
      $x\_j\_t = x\_j\_t.QoS$ # Extract attained QoS
      $AI\_L =$ Evaluate attraction value for local swarm
      $AI\_G =$ Evaluate group attraction value for global swarm
      $AI = (AI\_L + AI\_G) / 2$ # Evaluate the attraction index by taking the mean of local and global group
      $Dragonfly\_Score\_Chart[i, j] = AI$

The neural engine was used to rank dragonflies based on their training scores. After the training phase, 30 % of the dataset was thoroughly tested, and the classification scores were used to rank transitions. Neural networks, inspired by the human brain, are used in fields like picture and word identification, fraud revelation, and financial predictability. They have recently been applied to blockchain to strengthen security in smart homes. It is also utilized in the biological field to analyze genetic data and predict protein structures. The versatility of neural networks makes them a valuable tool in various industries for complex problem-solving and decision-making [26, 27]. This process allows the neural network to make accurate predictions on new, unseen data based on the patterns it has learned. The ability to classify data into specific categories makes neural networks a valuable tool in various industries for complex problem-solving and decision-making. [28, 29, 30]

Fig. 4 explains using of four parameters in the proposed approach: sender ID, receiver ID, evaluated operation, and BER. After completing the training phase, the neural network is ready for classification tasks. Four parameters (sender ID, receiver ID, evaluated operation, and BER) are used as input for the Lönberg model, configured with two layers and 12 active neurons per layer. Neurons propagate according to the minimum gradient, typically stabilizing between 5 and 15 cycles on average. The Lönberg model then uses these ground truth values to fine-tune the neural network's weights and biases, improving its accuracy in classification tasks. This iterative process allows for more precise decision-making based on the neural network's learning from the data records. Classification the highest probability was selected. This method of fine-tuning the neural network based on ground truth values helps to minimize errors and increase the overall performance of the classification system. By selecting the classification with the highest probability, the system can make more confident and accurate decisions. [28, 29, 30]

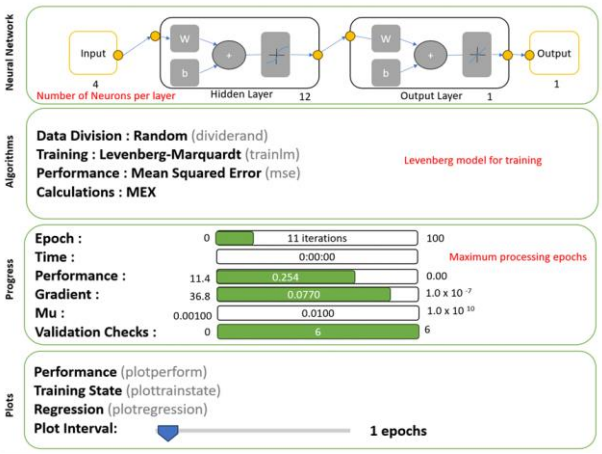

Fig. 4. Neural Network Structure

C. Proposed Framework

The SH-Block CC architecture, as proposed, utilizes the potential of computing cloud and technology of blockchain to achieve efficiency, scalability, and availability in the pursuit of friendly home smart environmentally. Consisting of four key components – home smart layers, network blockchain, layers services – the architecture and computing cloud, are explained in Fig. 5.

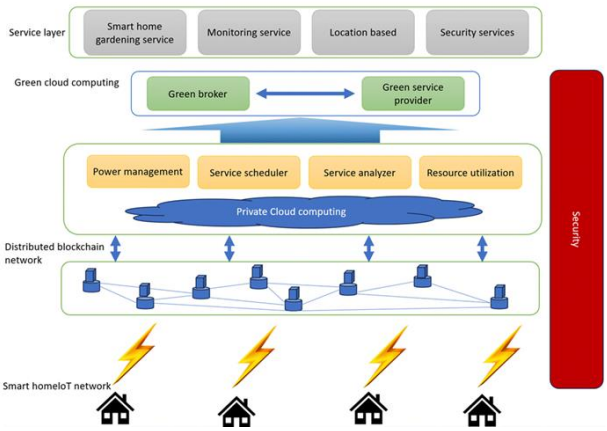

Fig. 5. Proposed Smart Home Architecture

1- Smart home layer

The smart house refers to a residential equipped house with devices of smart and subsystem, including security systems, control mechanisms, home cinema, etc. These devices have sensors that facilitate communication through a centralized program. Data of sensor connected to the cloud infrastructure along with related services. Data from Internet of Things (IoT) networks is received by a cloud platform that integrates it with other device data as well as transaction data. Efficient home services are often required by multiple smart home networks, usually provided by service providers.

2- Distributed blockchain layer

Blockchain technology has recently attracted the attention of stakeholders in various industries. This interest stems from the fact that blockchain enables applications to be managed in a decentralized manner, bypassing the need for a trusted intermediary as previously required. Blockchain, which serves as a distributed ledger, records multiple transactions efficiently and reliably across the entire chain without relying on a central host. A comparable approach can be adopted using decentralized service contracts. By providing a distributed peer-to-peer network, blockchain technology facilitates interactions between untrusted individuals without the need for intermediaries.

3- Blockchain in distributed cloud storage

Decentralization and Trust: Blockchain introduces a decentralized framework where transactions are validated without relying on a central authority. To ensure trust in the blockchain network, consensus among network nodes is required to confirm transactions.

Advanced Privacy: Each user in the blockchain maintains their own key, ensuring privacy. User data is stored encrypted in the digital currency system, addressing various privacy concerns.

Efficient use of resources and high quality: Blockchain facilitates the use of resources through its distributed architecture. For example, when a smart contract executes an algorithm that requires resources such as encryption functions, the program allocates computer resources based on the demand of the smart contracts. The payment is automatically processed after the function is completed. In principle, blockchain adoption can increase quality of service by enabling resource usage tracking.

4- Blockchain transaction management in smart home

The system of home smart manages all devices through transactions and stores them locally on the blockchain. These transactions can be performed over local device communications or between overlapping nodes, with each transaction designed to specific functions such as storage, access, monitoring, configuration, and deletion. The Diffie-Hellman algorithm creates a shared key used by all transactions. In addition to adding a new device, data access involves two distinct methods: local access and cloud access. Both methods ensure secure data transfer through encryption and authentication protocols. This dual approach allows for flexibility and efficiency in managing data access across different platforms. In local data storage, the device needs authentication in local memory and sends a request to nodes to verify permission to store data. If authorization is deemed valid, a key is shared between the device and local storage, enabling direct storage of data in local storage. For cloud data storage, identical blocks associated with unique identifiers are used for verification purposes. After successful authentication, user data packets are stored in blocks in a first-in, first-out (FIFO) sequence, allowing service providers to effectively access data and provide intelligent services. This process ensures secure and efficient storage of data, whether it be on local devices or in the cloud. By utilizing authentication and verification methods, users can trust that their data is being stored safely and accessed appropriately.

In summary, a home smart consists of different types of Internets of Things devices connected through a network. Local device management is facilitated by blockchain, with symmetric key encryption used for local transactions. Each home smart has a local ledger that processes all local transactions and overlaps with smart home transactions. This ledger ensures transparency and security in data storage and access within the smart home ecosystem. Additionally, regular updates and maintenance of the blockchain technology are crucial to ensuring continued protection of user data.

5- Overlapping network

The networks overlays are networks computer consisting of multiple nodes that are connected through virtual links and another network is built on top of them. Given the abundance of nodes in the overlapping network that ensures scalability and reduces overhead, the cluster head is determined for each cluster using a clustering algorithm, as described in Abbas and Yunus. The management of the entire network is overseen by a public blockchain. Therefore, as shown in Fig. 6, cluster heads are also known as overlay block managers (OBM). Overlay block managers are responsible for all cluster heads (CH) in the networks overlay, including handling multi-signed transactions from storage cloud and transactions acesses. Unlike Bitcoin mining, each CH independently decides whether to keep or discard a new block based on its relationship with the partner transactions. Consequently, this can lead to distinct versions of the blockchain for each CH.

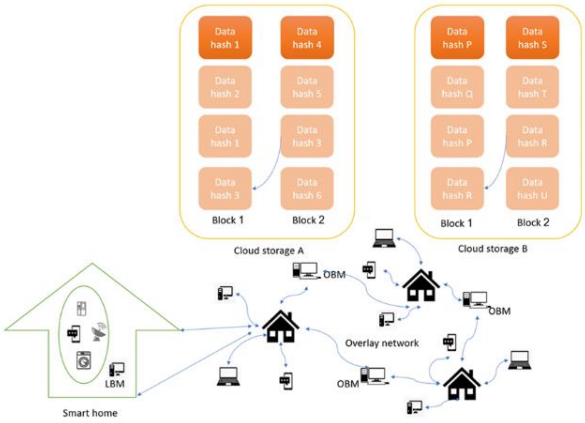

Fig. 6. Overview of the Overlay Network Connecting the Smart Home, Obm, And Cloud Storage

The overlay network is a peer-to-peer network that uses asymmetric encryption, digital signatures, and digital hash functions for transactions. The network's integrity is based on the Public Key Infrastructure (PKI), with each node maintaining its public key. A certificate authority verifies the node's public key through a self-signed certificate. To initiate a transaction, the transaction node generates an emergency transaction with a certificate verified by the Overlay Block Manager (OBM). The OBM verifies transactions by verifying the signatures of transaction participants with their public respective keys. All valid transactions are stored in a

predefined block, and the OBM verifies the existence of previous transactions in the public blockchain. Each OBM has a list of three elements: the requester's public key, a list of public keys of smart homes connected to the cluster with access rights, and the transactions history sent to other OBMs. This system ensures that only authorized participants can engage in transactions within the network. Additionally, the history of transactions allows for transparency and accountability in the blockchain ecosystem.

6- Transaction access for IoT device

Decentralized access to Internet of Things (IoT) data is achieved through a consortium blockchain network, where a user manages access control and secures data entry requests. The user connects to the consortium network through the client application and shares IoT data with the local blockchain administrator. A local blockchain, also known as a private blockchain or sidechain, is formed by grouping IoT devices for specific use cases. Users can own their side-chain networks, each tasked with ensuring secure IoT data logs. Sidechaining eliminates the need for validation on other sidechains. The validation node appends the requester's public key to the whitelist in the consortium network. The encrypted Interplanetary File System (IPFS) hash is decrypted using the private key, ensuring data privacy and integrity. A well-defined agreement governing the consortium blockchain reduces the risk of illegal access to transactions. This secure process ensures that only authorized users can access and validate transactions on the sidechains, maintaining the integrity of the network. Additionally, regular audits and monitoring of the consortium blockchain further enhance security measures and prevent unauthorized activities, as shown in Fig. 7.

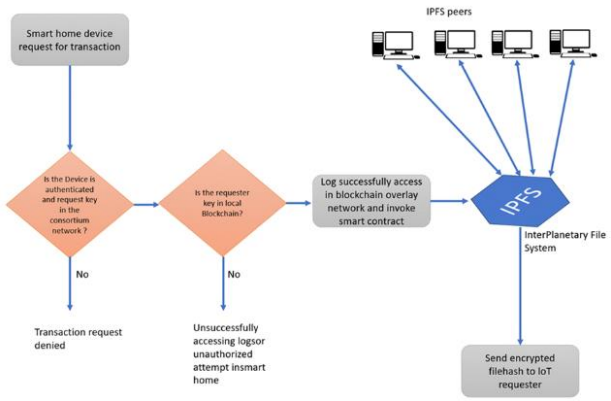

Fig. 7. Method For Iot Device Access Request Transaction

7- Cloud layers

The cloud layers refer to the software architecture in which the computing, storage, network and other resources required to provide Internet services over the Internet are provided. This model is based on the fact that the resources required to run a software or online service are made available in a virtual and shared manner so that users do not need to invest in hardware and software infrastructure and can pay the usage fee. Do References.

8- Green broker and CSP

Green Broker plays a pivotal role in increasing the energy efficiency of cloud services by carefully selecting service providers for users while managing customer requests in an environmentally friendly manner in SaaS, PaaS and IaaS domains. Each broker has a public listing detailing service cost history, carbon emissions, access times, and other relevant information, along with tools such as a work schedule, job selector, and carbon emissions calculator. Basically, the provision of green cloud services depends on three key elements:

- Third party: Maintains a carbon footprint inventory that shows the energy efficiency of its cloud services.
- Users: Choose the most eco-friendly cloud providers.
- Providers: facilitate the deployment of the most efficient carbon neutral clouds.

By moving their operations to the cloud, companies can reduce their carbon footprint by at least 30% per user.

Multi-tenancy and data centers:

The advent of virtualization and remote access in cloud computing has greatly expanded the scope of multi-tenancy architecture. For example, a SaaS provider can host an application instance on a single database instance and grant web access to different clients, ensuring data isolation for each tenant while maintaining confidentiality. Multi-tenancy is cost-effective by distributing software development and maintenance costs.

When it comes to cloud data center efficiency, the main focus is on energy consumption. Implementing efficient technologies in data centers increases energy efficiency and offers countless benefits such as load balancing across multiple servers in different locations. With its virtual services and accurate accounting, cloud computing facilitates unified access and exchange of services between data centers.

9- Cloud topological structure

This arrangement is similar to a typical cloud structure in a home smart. However, what sets it apart is the integration of the home smart as a form of infrastructure, along with the integration of middleware in the cloud platform to expand access to resources of home smart. In this framework, the smart home acts as a virtual node in the gateway. The nodes in the cluster form the components of the smart home cloud, and their distinctions are based solely on the types of services they provide. The gateway takes over the control of all services and thus makes them accessible to devices outside the home environment. The main goal of smart home connecting automation to the cloud is to create an intelligent environment that connects home devices. This integration also facilitates the development and deployment of third-party devices, while simultaneously seeking external resources and guidance for household items to use them.

10- Green cloud computing

Power Management: The purpose of this model is to maintain efficient power management in data centers. Its focal point is resource optimization, with the aim of reducing the energy consumption of servers or data center spaces. As a result, reducing the number of connected devices translates into reduced energy consumption in the data center. Service Scheduling: In the context of smart homes, multiple interconnected buildings and cities, this model coordinates the allocation of requests to virtual machines (VMs) and determines the optimal allocation of resources for these virtual machines. Additionally, it dynamically adjusts the number of virtual machines based on fluctuating demand levels. Service Analyzer: Tasked with interpreting and scrutinizing incoming service requests, this component determines whether to accept or reject smart home service

requests. Consequently, continuous monitoring of the current load and energy status of the smart home is essential, facilitated by VM managers and green brokers. Resource Analyst: This aspect expertly manages the availability of smart home services to end users and strives to optimize cloud computing performance by minimizing energy consumption, reducing e-waste, and utilizing heterogeneous and geographically dispersed resources to meet demand. Increase the growing number of smart home consumers.

11- Cloud smart home

It envisions a smart home that seamlessly integrates with a cloud to leverage additional information and services. While the cloud architecture differs from conventional models, it extends its functions to provide convenient and efficient home services for consumer digital electronics, ensuring readiness for future needs. The key components that facilitate home automation are simple and adaptable for future demands:

(a) Infrastructure component: It consists of a set of physical and virtual resources designed for cloud services that are managed through computing, storage, and extended network capabilities. These resources are tailored to meet the needs of large-scale operations.

(b) Platform: combining resources alongside a security management module. The resource detection module monitors system processes and implements resource virtualization. Simultaneously, the security management module enhances cloud security, which includes reliability, authentication, data scrutiny and reconfiguration. A PaaS-based cloud serves as a convenient platform for service providers to deploy smart home consumer-tailored offerings.

(c) Service layer: Facilitating interaction between service providers and smart home users, with primary emphasis on service applications through the application programming interface (API) provided by the cloud platform. Users access services or applications provided by smart home clouds, enterprise public clouds, or other third-party clouds, enhancing connectivity and performance.

12- Process flow

The security approach in the networks of home smart start with Algorithm 1, which verifies the client's authentication at the home gateway and checks the query packet qi for validity against the database. The gateway then processes the request and responds to the client. If the query packet is part of a new stream, Algorithm 2 is invoked for further examination and analysis. After receiving the new stream, press packet qi, which is checked in the detection mechanism, to determine if its signature matches any known attack database. If no match is found, the qi feature for the traffic is extracted using the MCA25 triangular area map (TAM) mechanism. This feature is then used to classify the traffic as either normal or potentially malicious. The classification result is sent back to the home gateway for appropriate action, ensuring network security and integrity. The chi-square anomaly pattern is investigated using MCA detection methods to extract correlation features between traffic. Packets are sent to the information security analyzer for further analysis. A data flow diagram (DFD) identifies vulnerabilities through vulnerability templates. If no vulnerabilities are detected, the packet is simply redirected to the home network. The information security analyzer also logs the incident for future reference and analysis, ensuring a comprehensive record of potential threats. Additionally, the system may automatically generate reports on the frequency and severity of detected vulnerabilities to aid in ongoing network protection efforts... This allows for proactive monitoring and response to any suspicious activity, enhancing the overall security of the home network. By regularly updating firmware and disabling unnecessary UPnP features, users can further reduce the risk of potential vulnerabilities in their network.

13- Profile generation

This module introduces an anomaly detector based on a typical profile, which uses thresholds from validated network traffic records to evaluate incoming traffic. The detection mechanism uses the latest knowledge base and a common scheme involving various security services. The protection services mitigate attacks, while the data detection service examines activity data from applications, devices, and smart home networks to identify anomalies. The response service, reinforced by a defense mechanism, ensures the smart home remains unharmed from attacks. These services are equipped with dynamic algorithms and robust inter-service communication to strengthen defense against potential threats. Overall, the comprehensive security system in place continuously monitors and analyzes all incoming and outgoing traffic to safeguard the smart home network. By combining cutting-edge technology with proactive measures, the system effectively prevents and responds to any potential security breaches in real time.

The response service executes actionable commands to remediate system vulnerabilities and shares behavioral insights with detection and protection services. The active security system (ASSYST) counters distributed denial of service (DDoS) attacks at the router level, powered by real-time traffic analysis from an external intrusion detection system (IDS), which detects potential attacks and generates appropriate responses. By leveraging real-time data and automated responses, ASSYST can quickly identify and neutralize threats before they can cause significant damage to the network. This integrated approach ensures a comprehensive defense strategy that adapts to evolving threats in real-time.

IV. RESULTS AND DISCUSSION

Google Collaborate and MATLAB Simulation were used in the development of the suggested smart home network concept. Quality of service (QoS) and other quantitative metrics, such as total computational complication, false detection rates, accuracy, recall, f-measure, and classification precision, were assessed using a blockchain ledger. To accomplish this, the researchers ran 20,000 simulations using a particular system model to gather the bit error rate (BER) and speed of each simulation, which were then input into the learning process. After testing the suggested approach for over a thousand iterations, the average convergence to the global optimum was found to be reasonably close to the global optimum. Table 4 offers specifics about the system specs and cloud computing and blockchain technologies, whereas Table 3 covers the system specifications and system model. The results indicated that the proposed approach using blockchain ledger technology was effective in optimizing system performance. Additionally, the study highlighted the potential of integrating cloud computing and blockchain technologies to improve system efficiency and reliability.

TABLE III. SYSTEM INFORMATION

System specificationsmn	
Number of data centers	2
Number of PMs to handle	10
Cloud Type	Xen
Blockchain Type	Firebase

TABLE IV. ORDINAL MEASURES OF SYSTEM AND SYSTEM MODEL

System Information	
RAM	4 GB
Processor	Intel core i3 530
Memory	DDR3
HD Capacity	500 GB
System Model Information	
Number of Users	50-500
Simulation Area	4000 m2
Channel of Communication	Rayleigh channel
Interpolation measurement	Lagrange interpolation
Channel Capacity	96,000 symbols per second
Channel gain	0.0023 units
Evaluation Parameters	Throughput, BER

The quality of service (QoS) was the primary focus of the comparison between the suggested approach and two cutting-edge algorithms. It was assessed using several classifiers based on quantitative criteria. After processing the transaction data, the training and classification model divided them into three categories: Avoid T, Mod T, and Smart T. After that, the neural network was taught to identify patterns in the information linked to every category, allowing it to categorize new objects. A network's computational complexity can rise dramatically as its device and transaction count rise. Furthermore, mining on proof-of-work (PoW) blockchains can become quite computationally intensive, which presents a problem for IoT devices with limited resources. Table 5 displays the precise computational complexity figures and contrasts them with other cutting-edge methods created for comparable environments. For example, Mod T has a computational complexity of O (n log n), while Smart T has a complexity of O (n^2). These figures highlight the efficiency of Mod T in handling larger amounts of data compared to Smart T.

TABLE V. COMPUTATION COMPLEXITY

Total Test Samples	Fused Real-Time Sequentail Deep Extreme Learning Machine System [3]	Data Fusion Technique [11]	Internet of Things Information Electronic Engineering and Optimization Schemes [17]	Proposed Technique
500	0.85991282	0.8780829	0.84910773	0.76528091
1000	2.11021973	1.9531654	2.04723132	1.87965372
1500	1.78525512	1.7024945	1.82948338	1.67876619
2000	2.05459249	2.1310947	2.19553898	2.03360384
2500	3.74510098	3.6378217	3.52360793	3.46864933
3000	3.34175878	3.4041558	3.48210032	3.26647149
3500	4.86868341	5.0819671	4.60406431	4.44362262
4000	4.22346545	4.2047017	4.47550357	4.06799277
4500	4.91378696	4.7681754	5.12593208	4.50671531
5000	6.0492668	6.4493703	6.17813064	5.77015973

The middle value of the "Proposed Computational Complication" column about the middles of the other columns indicates that the suggested method in this study had a lower average computational complexity than other algorithms. This improvement in computational complexity suggests that the proposed algorithm may be more efficient and effective in handling large datasets or complex computations. Further research and testing could provide more insights into the practical applications and benefits of this algorithm in various scenarios. Depending on how many test samples are used, the suggested algorithm's improvement over other algorithms vary in percentage. For instance, the suggested technique demonstrated an 11.1 % reduction in computational complexity with 500 test samples at 0.765. Nevertheless, the percentage improvement during the current research was just 7.07 % with 5000 test samples. The lowering of the proposed computational complexity values with increased test samples indicates that the proposed algorithm's effective data selection is responsible for its enhanced performance. Together with a set of algorithms, the suggested method was also assessed for false authentication rates. Fig. 8's authentication rate displays the total number of false positives that occurred during user authentication. This evaluation helps provide a comprehensive understanding of the algorithm's performance across different sample sizes. The results suggest that the algorithm's efficiency in data selection plays a crucial role in improving computational complexity and reducing false authentication rates. When compared to other methods, the suggested approach in this investigation displayed fewer incorrect authentication samples. The improvement numbers, which show a decrease in misauthentication in comparison to all other algorithms, clearly demonstrate this superiority. For instance, the suggested method recorded 18 erroneous authentications in the entire test sample size of 500, but the succeeding approach recorded 19 incorrect authentications. This leads to a 5.26 % improvement in the suggested algorithm. Similar to this, the suggested approach improved by 6.49 % with 173 false authentications compared to 185 false authentications for the other algorithm with a total test sample size 5000.01. Furthermore, the suggested method was assessed for qualitative criteria; Table 6 offers a detailed qualitative analysis. The qualitative analysis revealed that users found the suggested method to be more user-friendly and intuitive compared to the alternative algorithm. Additionally, participants reported higher satisfaction levels with the suggested approach in terms of ease of use and overall experience.

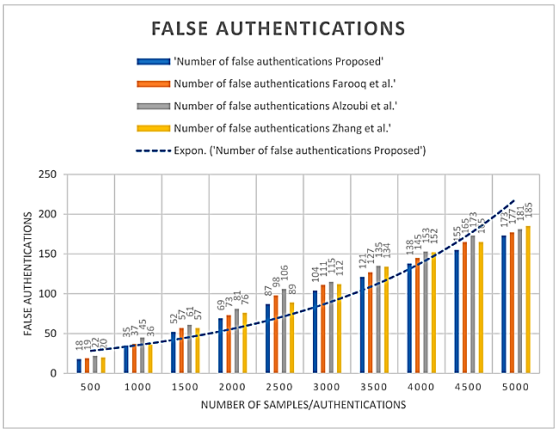

Fig. 8. Number Of False Authentications Reported in Farooq Et Al. [3], Al-Dhoubi Et Al. [11] And Zhang Et Al. [21]

TABLE VI. QUANTITATIVE PARAMETER EVALUATION

Precision				Recall			F-Measure		
Total test Samples	**RF**	**NB**	**P**	**RF**	**NB**	**P**	**RF**	**NB**	**P**
500	0.96	0.98	0.98	0.89	0.97	0.97	0.93	0.97	0.98
1000	0.97	0.97	0.97	0.93	0.99	0.99	0.95	0.98	0.98
1500	0.96	0.96	0.97	0.94	0.96	0.96	0.95	0.96	0.96
2000	0.97	0.97	0.97	0.93	0.99	0.99	0.95	0.98	0.98
2500	0.96	0.95	0.96	0.99	0.99	0.99	0.97	0.97	0.97
3000	0.98	0.98	0.98	0.94	1	1	0.96	0.99	0.99
3500	0.97	0.97	0.97	0.91	0.99	0.99	0.94	0.98	0.98
4000	0.98	0.98	0.99	0.95	0.98	0.98	0.96	0.98	0.98
4500	0.95	0.95	0.96	0.95	0.99	0.99	0.95	0.97	0.97
5000	0.93	0.96	0.98	0.93	0.92	0.95	0.93	0.92	0.97

The accuracy performance of the suggested approach was excellent, with an average accuracy of 0.97 to 0.98. Although the accuracy ratings of the NB and RF approaches were generally comparable, the RF method demonstrated reduced accuracy for certain test sample sizes, particularly for bigger samples. The suggested approach fared well in terms of memory as well, with an average score between 0.98 and 0.99. The suggested approach received somewhat higher marks than the NB and RF procedures, despite the latter producing good outcomes. Overall, the suggested approach showed consistent high performance across various metrics. It outperformed the NB and RF methods in accuracy and memory usage, making it a strong contender for data analysis tasks. The suggested approach often yielded good results in the F-measure metric, with an average score between 0.96 and 0.99. Although the F-measure scores obtained from the NB and RF approaches were generally comparable, in certain instances, the RF method yielded lower results, particularly when dealing with larger test sample sizes. Furthermore, the suggested approach demonstrated great accuracy when tested for false authentication prediction. A comparison of the suggested work and current approaches in terms of false authentication prediction is shown in Fig. 9. The accuracy of the suggested technique was 96.54 %, which is somewhat better than that of Farooq (95.28 %) and Alzoubi (92 %), indicating that the suggested strategy is successful in networks of home smart. Additionally, the suggested approach outperformed both Farooq and Alzoubi in terms of false authentication prediction, highlighting its effectiveness in enhancing security measures for networks of home smart. This demonstrates the potential for the suggested technique to be a valuable tool in ensuring secure access control within smart home environments.

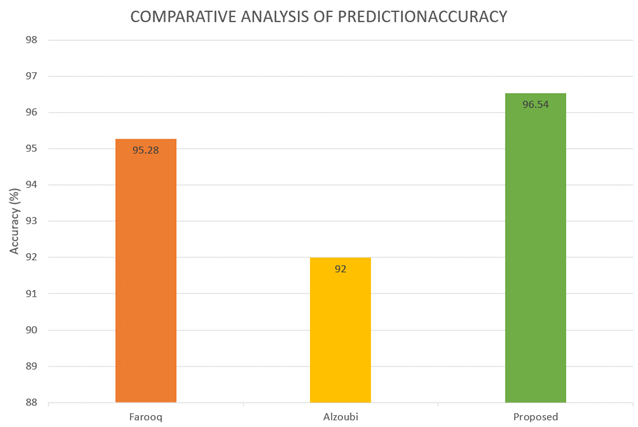

Fig. 9. Accuracy Comparison

The proposed method effectively reduced the computational complexity and thus improved the capacity of the network to handle larger data volumes. In addition, the network can integrate additional real-time data sets aimed at meeting similar demands.

V. CONCLUSIONS

This research paper presents a new framework that integrates IoT, layers of blockchain, computing cloud, and A.I. techniques to create an active and secured network communications. The substructure contains a front of the user, ledger generation, assessment data, and decision-making techniques. It highlights the secured implementation of a blockchain layers, a cloud-depend datas assessment layers, and the active uses of an AI-depend algorithms. An advanced dragonfly algorithm is presented to increase communication efficiency and security. The algorithm shows an average computational complication 3.5439, a significant enhancement 10.1399 % compared to the existing algorithms 3.9439. Algorithm's performance is due to its effective election of data. On a false authentication analysis, the proposed algorithm exhibited a maximum improvement percentage of 6.489 % compared to previous works. The approach also showed a large forecast precision 96.5439 to false authentication detection, demonstrating its effectiveness in ensuring security in networks of home smart. The research suggests future opportunities to integrate this tech. with other techns, like 4-5G and developed computing, to create most secured and effective communication network. The suggested architecture is promising for various applications in houses, clinic fields, markets and urabn life. Furthermore, the scalability of the algorithm allows for its implementation in large-scale networks without compromising performance. Overall, the findings highlight the potential of this approach to significantly enhance security measures in various IoT environments.

REFERENCES

[1] 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.

[2] 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.

[3] Sivaraman V., Gharakheili H.H., Vishwanath A., Boreli R., Mehani O. Network-level security and privacy control for smarthome IoT devices. In Proceedings of the 2015 IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Abu Dhabi, United Arab Emirates, 19–21 October 2015, pp. 163–167.

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

[5] Panwar N., Sharma S., Mehrotra S., Krzywiecki Ł., Venkatasubramanian N. Smart home survey on security and privacy. arXiv 2019, arXiv:1904.05476.

[6] Khan, M.A.; Ghazal, T.M.; Lee, S.W.; Rehman, A. Data Fusion-based machine learning architecture for intrusion detection. Comput. Mater. Contin. 2022, 70, 3399–3413.

[7] Hsu, Y.L.; Chou, P.H.; Chang, H.C.; Lin, S.L.; Yang, S.C.; Su, H.Y.; Chang, C.C.; Cheng, Y.S.; Kuo, Y.C. Design and implementation of a smart home system using multisensor data fusion technology. Sensors 2017, 17, 1631

[8] Le Nguyen, B.; Lydia, E.L.; Elhoseny, M.; Pustokhina, I.; Pustokhin, D.A.; Selim, M.M.; Nguyen, G.N.; Shankar, K. Privacy preserving blockchain technique to achieve secure and reliable sharing of IoT data. Comput. Mater. Contin. 2020, 65, 87–107.

[9] Wang, J.; Chen, W.; Wang, L.; Sherratt, R.S.; Alfarraj, O.; Tolba, A. Data secure storage mechanism of sensor networks based on blockchain. Comput. Mater. Contin. 2020, 65, 2365–2384.

[10] Bordel, B.; Alcarria, R.; Martin, D.; Sanchez-Picot, A. Trust provision in the internet of things using transversal blockchain networks. Intell. Autom. Soft Comput. 2019, 25, 155–170.

[11] Ra, G.J.; Roh, C.H.; Lee, I.Y. A key recovery system based on password-protected secret sharing in a permissioned blockchain. Comput. Mater. Contin. 2020, 65, 153–170.

[12] Singh, S.K.; Azzaoui, A.E.; Kim, T.W.; Pan, Y.; Park, J.H. DeepBlockScheme: A deep learning-based blockchain driven scheme for secure smart city. Hum. Cent. Comput. Inf. Sci. 2021, 11, 12.

[13] Zhang, J.; Zhong, S.; Wang, J.; Yu, X.; Alfarraj, O. A storage optimization scheme for blockchain transaction databases. Comput. Syst. Sci. Eng. 2021, 36, 521–535.

[14] Salim, M.M.; Shanmuganathan, V.; Loia, V.; Park, J.H. Deep learning enabled secure IoT handover authentication for blockchain networks. Hum. Cent. Comput. Inf. Sci. 2021, 11, 21.

[15] Dhanabal, L.; Shantharajah, S.P. A study on NSL-KDD dataset for intrusion detection system based on classification algorithms. Int. J. Adv. Res. Comput. Commun. Eng. 2015, 4, 446–452.

[16] Tavallaee, M.; Bagheri, E.; Lu, W.; Ghorbani, A.A. A detailed analysis of the KDD CUP 99 data set. In Proceedings of the 2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications, Ottawa, ON, Canada, 8–10 July 2009; pp. 1–6.

[17] Ingre, B.; Yadav, A. Performance analysis of NSL-KDD dataset using ANN. In Proceedings of the 2015 International Conference on Signal Processing and Communication Engineering Systems, Guntur, India, 2–3 January 2015; pp. 92–96.

[18] Alshinina, R.; Elleithy, K. A highly accurate machine learning approach for developing wireless sensor network middleware. In Proceedings of the 2018 Wireless Telecommunications Symposium (WTS), Phoenix, AZ, USA, 17–20 April 2018; pp. 1–7.

[19] Gandam, A.; Sidhu, J.S.; Verma, S.; Jhanjhi, N.Z.; Nayyar, A.; Abouhawwash, M.; Nam, Y. An efficient post-processing adaptive filtering technique to rectifying the flickering effects. PLoS ONE 2021, 16, e0250959

[20] Ghosh, G.; Kavita; Anand, D.; Verma, S.; Rawat, D.B.; Shafi, J.; Marszałek, Z.; Woźniak, M. Secure Surveillance Systems Using Partial-Regeneration-Based Non-Dominated Optimization and 5D-Chaotic Map. Symmetry 2021, 13, 1447

[21] Singh, D.; Verma, S.; Singla, J. A Neuro-fuzzy based Medical Intelligent System for the Diagnosis of Hepatitis B. In Proceedings of the 2021 2nd International Conference on Computation, Automation and Knowledge Management (ICCAKM), Dubai, United Arab Emirates, 19–21 January 2021; pp. 107–111.

[22] Dash, S.; Verma, S.; Kavita; Jhanjhi, N.Z.; Masud, M.; Baz, M. Curvelet Transform Based on Edge Preserving Filter for Retinal Blood Vessel Segmentation. Comput. Mater. Contin. 2022, 71, 2459–2476.

[23] EL-Hasnony, I.M.; Elhoseny, M.; Hassan, M.K. Intelligent Neighborhood Indexing Sequence Model for Healthcare Data Encoding. J. Intell. Syst. Internet Things 2019, 15–25.

[24] Singh, D.; Verma, S.; Singla, J. A Comprehensive Review of Intelligent Medical Diagnostic Systems. In Proceedings of the 2020 4th International Conference on Trends in Electronics and Informatics (ICOEI) (48184), Tirunelveli, India, 15–17 June 2020; pp. 977–981.

[25] Ghosh, G.; Kavita; Verma, S.; Jhanjhi, N.Z.; Talib, M.N. Secure Surveillance System Using Chaotic Image Encryption Technique. IOP Conf. Ser. Mater. Sci. Eng. 2020, 993, 012062.

[26] Ramisetty, S.; Kavita; Varma, S. The Amalgamative Sharp Wireless Sensor Networks Routing and with Enhanced Machine Learning. J. Comput. Theor. Nanosci. 2019, 16, 3766–3769.

[27] Saracevic, M.; Wang, N.; Zukorlic, E.E.; Becirovic, S. New Model of Sustainable Supply Chain Finance Based on Blockchain Technology. Am. J. Bus. Oper. Res. 2021, 3, 61–76.

[28] Mafarja, M.; Heidari, A.A.; Faris, H.; Mirjalili, S.; Aljarah, I. Dragonfly Algorithm: Theory, Literature Review, and Application in Feature Selection. Stud. Comput. Intell. 2020, 811, 47–67.

[29] Ravi, N.; Verma, S.; Kavita; Zaman, N.Z.; Talib, M.N. Securing VANET Using Blockchain Technology. J. Phys. Conf. Ser. 2021, 1979, 012035.

[30] Gupta, V. Ideas on ad hoc networks and power aware networks. IJFRCSCE 2018, 4, 2554–4248.

[31] Maseleno, A. Design of Optimal Machine Learning based Cybersecurity Intrusion Detection Systems. J. Cybersecur. Inf. Manag. 2019, 32–43

[32] Elsharkawy, M.; Al Masri, A.N. A Novel Image Encryption with Deep Learning Model for Secure Content based Image Retrieval. J. Cybersecur. Inf. Manag. 2019, 54–64.