Intelligent Automation & Soft Computing

Tech Science Press

DOI: 10.32604/iasc.2024.047080

ARTICLE

Machine Learning Empowered Security and Privacy Architecture for IoT Networks with the Integration of Blockchain

Sohaib Latif[1,*], M. Saad Bin Ilyas[1], Azhar Imran[2], Hamad Ali Abosaq[3], Abdulaziz Alzubaidi[4] and Vincent Karovič Jr.[5]

[1]Department of Computer Science, The University of Chenab, Gujrat, 50700, Pakistan

[2]Department of Creative Technologies, Air University, Islamabad, 42000, Pakistan

[3]Computer Science Department, College of Computer Science and Information Systems, Najran University, Najran, 66244, Saudi Arabia

[4]Department of Computer Science, Umm Alqura University, AlQunfudah, 28821, Saudi Arabia

[5]Department of Information Systems, Faculty of Management, Comenius University in Bratislava, Bratislava, 820 05, Slovakia

*Corresponding Author: Sohaib Latif. Email: sohaiblatif095@gmail.com

Received: 24 October 2023 Accepted: 04 January 2024 Published: 21 May 2024

ABSTRACT

The Internet of Things (IoT) is growing rapidly and impacting almost every aspect of our lives, from wearables and healthcare to security, traffic management, and fleet management systems. This has generated massive volumes of data and security, and data privacy risks are increasing with the advancement of technology and network connections. Traditional access control solutions are inadequate for establishing access control in IoT systems to provide data protection owing to their vulnerability to single-point OF failure. Additionally, conventional privacy preservation methods have high latency costs and overhead for resource-constrained devices. Previous machine learning approaches were also unable to detect denial-of-service (DoS) attacks. This study introduced a novel decentralized and secure framework for blockchain integration. To avoid single-point OF failure, an accredited access control scheme is incorporated, combining blockchain with local peers to record each transaction and verify the signature to access. Blockchain-based attribute-based cryptography is implemented to protect data storage privacy by generating threshold parameters, managing keys, and revoking users on the blockchain. An innovative contract-based DOS attack mitigation method is also incorporated to effectively validate devices with intelligent contracts as trusted or untrusted, preventing the server from becoming overwhelmed. The proposed framework effectively controls access, safeguards data privacy, and reduces the risk of cyberattacks. The results depict that the suggested framework outperforms the results in terms of accuracy, precision, sensitivity, recall, and F-measure at 96.9%, 98.43%, 98.8%, 98.43%, and 98.4%, respectively.

KEYWORDS

Machine learning; internet of things; blockchain; data privacy; security; Industry 4.0

This work is licensed under a Creative Commons Attribution 4.0 International License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

1 Introduction

Security threats in IoT network environments encompass a range of risks, including unauthorized access, where malicious actors gain entry to devices or networks, possibly leading to theft of data or service disruption. Data interception poses a danger as unauthorized entities eavesdrop on communication between IoT devices, risking data exposure and manipulation. Device tampering, whether physical or remote, can compromise device functionality, allowing for unauthorized control or data alteration. Denial of Service (DoS) attacks aim to overwhelm IoT devices or networks, causing disruption and operational inefficiencies. Man-in-the-Middle (MitM) attacks involve intercepting and altering communication, leading to unauthorized access and potential data manipulation. Device spoofing enables attackers to impersonate legitimate devices, risking unauthorized access and data manipulation. Insecure interfaces and APIs present vulnerabilities that could result in unauthorized access or manipulation of device settings. The lack of device updates and patching increases susceptibility to known exploits, while insufficient authentication and authorization mechanisms can lead to unauthorized access and data exposure. Physical security risks involve the compromise, tampering, or theft of IoT devices. Privacy concerns arise from improper handling of personal or sensitive data, and inadequate network security opens the door to unauthorized access, data exposure, and service disruption. Addressing these threats requires a comprehensive approach, including strong authentication, encryption, regular updates, and adherence to security best practices and standards.

The rise of IoT networks and services is sparked by the growing popularity of intelligent and smart services. The IoT computing and energy scarcity issue must be addressed immediately if services are to be secure and effective [1]. Several articles can be connected to IoT. These devices with sensors can detect, trigger, collect, store, and process data. IoT applications include smart traffic monitoring [2], smart homes [3], wearable devices [4], industry [5], and smart cities [6]. IoT-based applications thus become the core elements of our everyday life [7].

Even though the Internet of Things (IoT) can make people's lives safer, failing to protect user data and privacy can have some bad effects [8]. Cybercriminals may be able to reprogram these unsecured IoT systems and cause malfunction by other malicious individuals through this method. At the system level, security and privacy become important. Integrity, confidentiality, and authentication properties must be taken into consideration to create a safer Internet of Things solution [9]. Several prior methodologies are used to guarantee that entities and associated resources can legitimately access service providers during IoT networking and communication. The substance in this cycle may be an independent specialist or a real client, whose sole design is to safely get to the computerized resources [10]. Access to a wide range of additional security services, having confidentiality, integrity, access control, non-repudiation of digital envelopes, and privacy with anonymity, all require entity legitimacy [11]. It is necessary to carry out authentication with a high level of trust.

Digital identity has become an important aspect of blockchain technology, and projects like Sovrin and Hyperledger Indy are specifically designed to address this issue. Both Sovrin and Hyperledger Indy are open-source distributed ledger frameworks that provide tools and protocols for creating and managing digital identities in a secure and decentralized manner. Sovrin is focused on creating a utility for global public for self-sovereign identity (SSI) that allows individuals to control and own their digital identities without depending on third-party intermediaries. Sovrin aims to provide a decentralized, interoperable, and verifiable identity system that can be used across different applications and platforms. Sovrin's approach is based on a public blockchain, which allows for trust and transparency while still maintaining privacy and security. Hyperledger Indy, on the other hand, is a distributed ledger specifically designed for decentralized identity. It provides a set of interoperable standards

and protocols for creating and managing digital identities, which can be used in various applications, including identity verification, authentication, and authorization. Hyperledger Indy uses a blockchain model with a focus on privacy, security, and user control over their digital identities [12].

Device authentication is one of the key prerequisites for ensuring IoT security, which can help to regulate IoT entities access and verification of their identity. It is hard to safeguard privacy and security without confidence in the connectivity and functionality of IoT entities [13]. Attackers may use any compromised IoT device to interrupt the system's regular operation and do significant harm. End-to-end encryption techniques are often used to ensure authenticity and secrecy [14–16]. On the other hand, IoT devices often only support a few extremely lightweight cryptographic methods and have constrained battery and processing resources. Thus, these approaches run the risk of compromising the system's security [17].

According to [18], secure device pairing is a crucial method for creating encrypted channels for data processing and transmission as well as for IoT device authentication. Users are frequently requested to participate in the pairing cycle by using standard device authentication methods, such as providing a password or keeping the paired devices close to one another. Due to budget and space constraints, the majority of IoT devices do not have the user interface faces needed for authentication interactions. Furthermore, traditional human-in-loop device pairing approaches become inapplicable as the number of devices keeps growing [19–21]. Digital Signature Algorithms (DSA) based on Elliptic Curves are frequently used for authentication [22,23]. Most DSAs use a variety of hashing and public key cryptography algorithms (LAVANYA and NATARAJAN 2017). Message digest (MD5) and SHA family versions are the most widely used hashing algorithms [24]. Certain hashing methods require additional calculations, which can strain the resources of the device. It has been demonstrated that the stream cipher-based hashing algorithms BLAKE and BLAKE2, when applied to resource-constrained IoT devices, significantly reduce energy consumption and computational expenses [20].

IoT devices are vulnerable to physical, side-channel, and cloning attacks since they are easily accessed and physically exposed. In order to solve these problems, IoT device manufacturers are thinking about incorporating security measures in next-generation IoT devices. Researchers are creating new, lightweight security mechanisms for Internet of Things applications. One of the inherent security features of Internet of Things devices is Physical Unclonable Functions (PUFs), commonly referred to as physical one-way functions. PUFs are new primitives that take secrets out of the complex physical characteristics of integrated circuits rather than storing them in digital memory. Because a PUF is based on a random variation that happens during the integrated circuit fabrication process, it is very difficult to forecast or discern its secret [25,26] Key generation and user authentication have been the main uses of PUFs in security [27]. The source of the data, however, cannot be ascertained using these techniques. The location from where the data were obtained cannot be guaranteed, but the combination of a PUF and the sensor reading approach can successfully prove the validity and identification of the IoT device generating the data [28,29]

Blockchain is a distributed, open, and transparent ledger that efficiently and permanently records transactions between two parties ("IThings 2016 Organizing Committee" 2016). Unless a new consensus is reached, the data on the blockchain cannot be altered once it has been recorded. It is anticipated that the Internet of Things (IoT) and blockchain technology will increase trust and decrease overall overhead for IoT systems [30]. For billions of connected objects to achieve distributed trust through it, it can assist the Internet of Things in establishing a decentralized, credible, and publicly verifiable database. As a result, this work proposes a novel decentralized and secure method that incorporates blockchain to address the security risks and privacy concerns associated with IoT devices.

This paper mainly focuses on the integration of blockchain with IoT systems for data access, control from cyber-attacks, and privacy. To avoid a single-point OF failure, the blockchain transaction and signature verification have been performed through the blockchain.

The following is the arrangement of the remaining part of the paper: The most recent research is presented in Section 2; The proposed method's in-depth description can be found in Section 3; The outcomes of implementation are discussed in Section 4; The paper concludes with Section 5.

2 Literature Survey

A secure authentication technique for a hierarchical Internet of Things network (HIoTN) was developed [31]. In HIoTN, nodes are organized hierarchically, including sensor nodes, gateway nodes, and cluster head nodes. For such a network, they have suggested a three-factor remote user authentication technique called the user authentication key management protocol (UAKMP). UAKMP uses a smart card, a password, and personal biometric entities to provide three-tier user authentication. In a real-time environment, they were unable to attain the same level of performance with resource-constrained devices, despite simulations demonstrating that UAKMP defends against known assaults.

Techniques for two-tier authentication based on devices were proposed by [32–34]. They were able to look into the trade-offs between malicious node detection and spectrum management by using this setup. However, they could extend their system to real-time sensing, network access control, and end-to-end latency reduction by developing a joint spectrum allocation and topology control. Reference [35] expressed worries about the security and privacy of the data when it is sent across an unreliable channel. The researchers also discovered that not all IoT use cases could be supported by present systems due to their high computation and communication overheads. The authors developed a novel, privacy-preserving user authentication method for the Internet of Things to address the issues. To authenticate the entities, the strategy employs XOR, fuzzy extractors, a one-way hash function, and biometrics, among other techniques. The approach combines biometrics and smart cards to confirm the entities' legitimacy. Although the technique has benefits, it consumes a lot of energy due to the size and quantity of messages transmitted during the verification process.

References [36,37] discussed several scenarios where Wireless Sensor Networks (WSN) and the Internet of Things (IoT) are integrated to accomplish particular tasks. The authors created a new security procedure in response to the potential for an unauthorized user to access a sensor node. The authors created an authentication procedure for IoT networks based on Elliptic Curve Cryptography (ECC) to get over the lack of user anonymity and other flaws in the current protocols. Their suggested solution used XOR, a fuzzy extractor, a one-way hash, and biometrics to accomplish the authentication aim. The authors asserted that their method was firmly based on the formal security analysis performed with the random oracle model. After analysis, the scheme is run through the Network Simulator (NS3) to see how the method performs in the WSN-IoT context. The plan has advantages and disadvantages, but it has not been proven to withstand potential MITM assaults in the future, which could destroy the protocol. Due to the absence of a nonce and ciphering techniques, the system also fails to guarantee the confidentiality of all shared data and the freshness of messages.

Reference [38] has demonstrated how important WSNs are for gathering data from remote areas. Since the channel was open, communication was challenging, and the author emphasized the necessity of robust security measures to preserve integrity and secrecy. In WSN, it becomes difficult because of the limited resources of the compute nodes. The shortcomings of the current methods have been addressed by the development of a novel protocol for key exchange and mutual authentication. With

all of its security characteristics, the technique still lacks identity anonymity and overall privacy. The method's overall hashing consumption and high message overhead stress the system in addition to the security measures.

According to study by [39], most internet-connected devices are vulnerable to unsecured channels, which makes privacy vulnerable. As lightweight hashing techniques for IoT user authentication, a modified elliptic curve digital signature system (ECDSA) and a customized BLAKE2b hashing algorithm have been presented. The writers have compromised security to cut down on the amount of money spent on computing and communication. Because the protocol's resilience to most anonymous attacks was not confirmed, the scheme's reaction to attacks was extremely unpredictable.

While earlier techniques are more effective in establishing security in an IoT context, in a real-time scenario with resource-constrained devices, neither the end-to-end delay nor performance can be improved. Despite the benefits that become apparent, the system consumes a lot of energy due to the size and amount of messages delivered during the authentication process. The overview of previous work is discussed in Table 1.

Table 1: Overview of previous work

Authors	Journal	Purpose	Methodology	Results
Kumar et al. 2022 [33]	IEEE Transactions on Intelligent Transportation Systems	Utilizes blockchain to create a decentralized and secure network for data storage and sharing among vehicles and infrastructure.	Deep learning models are used to analyze the data collected from different sources and provide insights for decision-making.	The proposed framework is evaluated using a case study involving vehicle-to-vehicle communication and intersection management. The results show that the framework is effective in preserving privacy and ensuring security while providing efficient communication and decision-making.
Kumar et al. 2023 [34]	Journal of Parallel and Distributed Computing	Utilizes a blockchain-based decentralized network to securely store and share patient data among different healthcare providers.	Deep learning models are used to analyze the data and provide insights for decision-making.	To ensure the privacy and security of patient data, the framework uses encryption techniques to protect the data and prevent unauthorized access. Proposes a novel consensus mechanism based on deep learning to achieve consensus among the nodes in the blockchain network.

(Continued)

Table 1 (continued)

Authors	Journal	Purpose	Methodology	Results
Kumar et al. 2023 [35]	IEEE Communications Magazine	A blockchain-based decentralized network to securely store and share network configuration data among different devices.	Deep learning models are used to analyze the data and provide insights for decision-making.	To ensure the security of network communication, the framework uses a combination of encryption techniques and blockchain-based consensus mechanisms. The authors propose a novel consensus mechanism based on deep learning to achieve consensus among the nodes in the blockchain network.
Kumar et al. 2022 [36]	IEEE Global Communications Conference	Blockchain technology is used to create a decentralized and secure network for storing and sharing patient data among different healthcare providers.	AI-based predictive models to analyze patient data and provide personalized healthcare recommendations.	To ensure the privacy and security of patient data, the framework uses a combination of encryption techniques and blockchain-based consensus mechanisms. The authors propose a novel consensus mechanism based on Proof of Reputation (PoR) to achieve consensus among the nodes in the blockchain network.
Kumar et al. 2022 [37]	IEEE Transactions on Network Science and Engineering	Utilizes a blockchain-based decentralized network to securely store and share data among different devices in the network.	Deep learning models are used to analyze the data and provide insights for decision-making.	To ensure the security of communication, the framework uses a combination of encryption techniques and blockchain-based consensus mechanisms. The authors propose a novel consensus mechanism based on deep learning to achieve consensus among the nodes in the blockchain network.

(Continued)

Table 1 (continued)

Authors	Journal	Purpose	Methodology	Results
Kumar, et al. 2020 [38]	Journal of Ambient Intelligence and Humanized Computing	Utilizes a fog computing-based approach to distribute the detection and decision-making process among multiple fog nodes. The fog nodes are responsible for collecting and analyzing network traffic data from different IoT devices in the network.	Proposes a novel feature selection technique based on the mutual information-based filter method to reduce the number of features and improve the accuracy of the IDS.	To ensure the security of IoT networks, the proposed system uses a combination of machine learning algorithms, such as support vector machines, random forests, and neural networks, to detect and classify different types of attacks. The ensemble of these machine learning models is used to improve the overall accuracy and robustness of the IDS.

3 Novel Decentralized Scalable Framework

IoT has been rapidly developing in recent years due to the rise in the number of intelligent gadgets. With the use of existing network infrastructure, it successfully connects the physical world to the Internet to enable data sharing between intelligent devices. The dynamic and large-scale network topology, on the other hand, presents cyber security challenges and complications to IoT systems. However, these solutions offer decentralized security and anonymity. Additionally, data privacy preservation is one of the main concerns regarding IoT devices. Due to the computation burden, IoT devices need to manage a huge number of keys with previous techniques. Consequently, DoS is the major challenge on IoT networks, since it can overwhelm the server of the system. Despite numerous research attempts to identify DDoS assaults using machine learning techniques, there is a lack of a systematic strategy to avoid commonly entrenched problems like colinearity and duplication. Thus to cope with the aforementioned issues, a novel Decentralized and Secured Framework has been proposed in this work with a decentralized, reliable, and scalable blockchain, which is illustrated in Fig. 1.

The above figure shows the block diagram of our proposed framework in which the users as well as the nodes/devices registered initially with the certification authority. Initially, to mitigate the single-point OF failure, an Accredit access control scheme is included to interpret the variation of accredits. Attribute-based cryptography through blockchain is employed in addition to achieving data availability and integrity. Finally, a smart contract-based DoS attack mitigation technique has been preventing the server from DoS attacks. In the following sections, the researchers propose an approach that is further described below.

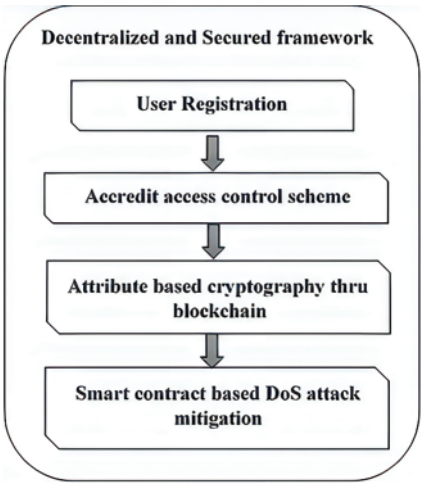

Figure 1: Proposed framework's block diagram

3.1 Registration with Certification Authority

Actors: Actors in an IoT network including blockchain can be divided into two categories: consumers and producers of data. Devices that use data, such actuators or controllers, are known as data consumers, whereas data producers are devices that make data, like sensors or smart meters. Actors can exchange data securely and transparently by communicating with one another via a variety of protocols, including constrained application protocol (CoAP) and message queuing telemetry transport (MQTT). Data transactions are also logged on the blockchain network.

Anchor: Anchors are used in blockchain-based Internet of Things networks to give an unchangeable and impenetrable record of the blockchain's status at a given moment in time. The process of creating an anchor involves hashing the most recent blocks' block headers on the blockchain network and storing the hash on a different, more secure network, such Ethereum or Bitcoin. In order to guarantee the integrity and validity of the data on the blockchain network, this offers a high degree of security and tamper resistance.

Local peers: In a blockchain-based IoT network, local peers play a critical role in ensuring the security and efficiency of the network. Local peers can be organized into clusters or sub-networks based on geographical or logical proximity and can communicate with each other to validate and authenticate data transactions. Local peers can also act as gateways between the IoT network and the blockchain network, which helps to ensure that data is transmitted securely and efficiently. In addition, local peers can participate in the consensus process of the blockchain network, which involves validating transactions and creating new blocks. This helps to ensure that the network is secure, transparent, and efficient.

First, the users participating in this communication as well as the sensor nodes/devices are registered by the framework to guarantee security. At this point, a master is created who acts as a certification authority (CA). To be a part of the system, every IoT device needs to be registered with both the local peer (LP) and the CA. The Certification Authority Server is a fully reliable organization capable of managing several credential-certifying designs. It is a crucial component of the system since no other entity in a blockchain network has the authority to provide certifications, signatures, or keys. Both the certificates for user registration and all administrative certificates are created by it. All

user apps obtain their encryption keys and signatures from CA. Additionally, it permits TLS-secured communication between every blockchain element, as well as credential validation, signature creation, and verification.

However, access control is not directly under its authority. Devices and apps must use that solution, and many of them only need it for signature verification. Local Peer only supports IoT devices that are organizational in nature. Moreover, secondary LP can engage in application scenarios where local transaction consensus requires the participation of multiple peers. A copy of the ledger is additionally maintained by secondary LP. Every gadget needs to register on LP. It employs CA to certify each device and keeps track of users, their credentials, and smart contracts. Blocks can only be read and written into the ledger by LP. In order to facilitate inter-organizational transactions, it is also in charge of connecting with the anchor peer.

In this architecture, IoT nodes can be part of the blockchain layer, acting as nodes that validate and process data transactions. Alternatively, IoT nodes can communicate with the blockchain layer through a gateway or a local peer, which acts as a bridge between the IoT layer and the blockchain layer. The gateway or local peer can be responsible for converting the data into a format that is compatible with the blockchain network and transmitting the data to the blockchain layer for storage and processing.

The CA is responsible for generating various certificates, such as eCert, TLS CA, public-private keys, and signatures, and distributing them to the device. After that, it registers with LP, which confirms the identity of the requester from CA. LP saves all device credentials (like CA certificates, TLS, and signatures) for later verification during the verification step. IoT devices that have been authorized can join the regional Blockchain network as a result of this procedure. The worldwide Blockchain network, where LP registers devices with the anchor peer, will also be a part of the IoT device. As a response to a device registration request, the CA produces and maintains signatures and cryptographic materials (such as certificates) (only if accepted). When the device D_i is linked to LP, the device's registration ID changes to *PeerID.DeviceID*, which is utilized in further transactions. The registration process has been depicted in Fig. 2 as well as Algorithm 1.

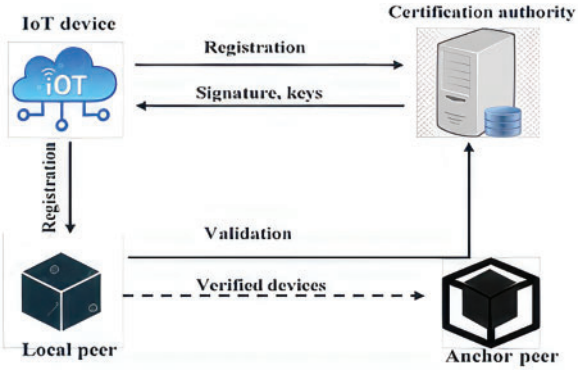

Figure 2: Registration process

Algorithm 1: Registration Process

Input: Device id, $D_i = (D_1, D_2, \ldots D_n)$

Output: *PeerID.DeviceID*

(Continued)

Algorithm 1 (continued)

Assign *device id* $\leftarrow D_i$
Assign *PeerID* $\leftarrow LP$
Request for certificate authentication
if (D_i *(certificates)*)
then
    $D_i \rightarrow LP(sign(D_i), D_i)$
    if $LP(sign(D_i))$ **then**
        Device D_i is registered with *LP*
        return *LP*. D_i
    else
        D_i certificate is not valid
    end if
else
    Cancel request
end if

Only when a device has been registered with both the certification authority as well as a local peer can it perform any transaction or communication in the blockchain. Then the message authentication has been taking place in this work, which is described in the next section.

3.2 Accredit Access Control Scheme

Traditional access control solutions are not suited for creating access control in IoT systems to offer data security because of their challenging access management and loss of legitimacy due to consolidation. Single-point of failure, as well as data manipulation, play a big role in compromising security and privacy in IoT devices. To handle this, blockchain technology can record the allocation of accredits in an IoT system to simplify access control and minimize single-point OF failure. The certification authorities are referred to as the accrediting authorities that collaborate to establish a transparent and trustworthy ledger of "transactions." The information in the block cannot be modified after it has been recorded, and anybody may ask the blockchain at a certain moment. To apply for an accredit α each device utilizes its address and ID. To create an address, the keys provided by the CA have been utilized. The public key as well as the ID are hashed and then encoded by the Base58Check encoding to create the address.

$$Address = Base58Check\left[H_2\left(K_{pub} \parallel ID\right)\right] \tag{1}$$

A pair of public and private keys are associated with each certification authority. The private key is used to sign the transactions and the public key is used to produce its address AA. The accrediting authority with which the device communicates will check if the applicant is capable of holding this accredit, α. The accrediting authority will produce the following transaction if the device passes the verification:

$$A_{add} \xrightarrow{\alpha} Address \tag{2}$$

The accrediting authority then signs the transaction's hash and timestamp with its private key as below:

$$sign\left(K_{pri}\right)\left[H_1\left(A_{add} \xrightarrow{\alpha} Address \parallel timestamp\right)\right] \tag{3}$$

The accrediting authority stores the transaction, including the date and signature, in its transaction pool at the end. These consortium nodes will select a block builder regularly. Its responsibility is to broadcast a block to the other consortium nodes for consensus that contains every transaction in its transaction pool. The blockmaker calculates the Merkle root of the transactions and arranges them according to their timestamps. The Merkle root, the creation date of this block, and the hash of the preceding block header are all contained in the block header.

The access control protocol between two users has been presented in Fig. 3. User 1 sent a communication demand to user 2 with its unique identity ID_1 and generated a session key K_{ses} with user 2 using the standard identity-based authentication and key agreement protocol. K_{ses}, utilizing any symmetric key method, ensures the security of the subsequent communication between user 1 and user 2. Then user 2 offers a random number R as well as an access policy P_{acc} that specifies who is allowed to connect with user 2.

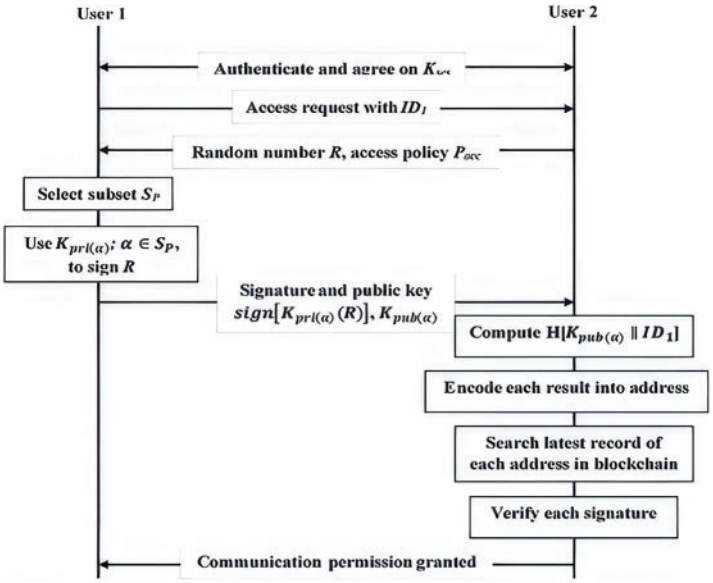

Figure 3: Access control protocol between two users

User 1 picks a contented subset S_P of the policy and signs the random number R with each secret key whose associated address has been assigned the matched accredit α. The fulfilled subset of characteristics, as well as each signature and public key pair $sign\left[K_{pub(\alpha)}(R)\right]$; $K_{pub(\alpha)}$; $\alpha \in S_P$, is then returned to user 2 via user 1. To retrieve the appropriate address, user 2 hashes the $K_{pri(\alpha)} \| ID_1$ and encodes the result using Base58 Check encoding. Then user 2 looks for the most recent relevant record for this address on the blockchain. If this address has the claimed accredit α, user 2 verifies the signature $sign\left[K_{pri(\alpha)}(R)\right]$ using the public key $K_{pub(\alpha)}$ by computing:

$$Ver_{K_{pub(\alpha)}}\left\{sign\left[K_{pri(\alpha)}(R)\right]\right\} = R \tag{4}$$

If that is the case, it is clear that user 1 owns this address and the property associated with it. Finally, user 2 verifies that the characteristics supplied comply with the access policy user 2 defined. user 2 will grant user 1's request to view user 2 data if user 1 holds enough characteristics that meet user 2's access rules. Using the generated session key Kses, the process of transmitting the data could also be encrypted.

Accredit distribution needs to be scalable and dynamic to enforce effective access control. The system must be able to revoke accreditations that have expired or are no longer held by a specific user promptly for attributes to better define identities. To revoke a user's accreditation, the accreditation authority may initiate a new transaction using this attribute:

$$A_{add} \overset{\alpha}{\leftarrow} Address \tag{5}$$

Then, with the other consortium nodes, re-execute the consensus process. The new block containing this revocation transaction will be added to the blockchain once they reach a new consensus. When user 2 searches the blockchain for the address of that accredit α the most recent associated record is its revocation, not its earlier authorization. This allows for an effective and efficient revocation of characteristics. Thus this provides highly effective access control in which, once registered, it is impossible to change the information in the blocks, and anybody may query the blockchain as needed at any time, greatly reducing free space issues and effectively improving privacy in IoT.

3.3 Attribute-Based Cryptography through Blockchain

As IoT devices have limited power, cloud storage is one of the most efficient methods to handle data. However, a slew of security and privacy concerns emerge, including unauthorized data access, data manipulation, and data leakage. Conventional blockchain-based methods offer decentralized security and anonymity, but they consume a lot of energy and have high latency, making them unsuitable for the majority of IoT devices with limited resources. Despite being effective for data security, attribute-based encryption suffers from a computationally intensive decryption procedure and requires managing a large number of keys in the Internet of Things. Therefore, the blockchain has been incorporated into attribute-based cryptography to ensure data integrity and confidentiality. A decentralized blockchain system that produces threshold parameters, manages keys and revokes users takes the role of the traditional centralized server. The blockchain handles all revocation duties, thus ciphertext re-encryption and key updates are no longer necessary. Additionally, users can produce partial tokens using the coalition blockchain. Furthermore, the cloud server in our method not only stores the enormous encrypted data but also conducts search and pre-decryption for users who only need one exponentiation in the group $\mathcal{G}$ to fully decrypt.

The access structure has been utilized for encryption, where several parties must collaborate to get a resource. Consider the set of parties, $\mathcal{P} = \{\mathcal{P}_1, \ldots \mathcal{P}_n\}$. The collection $\mathbb{A} \subseteq 2^{\{\mathcal{P}_1, \ldots \mathcal{P}_n\}}$ was monotone if $\forall\, \mathbb{B}, \mathbb{C}$: if $\mathbb{B} \in \mathbb{A}$ and $\mathbb{B} \subseteq \mathbb{C}$ then $\mathbb{C} \in \mathbb{A}$. The collection $\mathbb{A}$ of non-empty subsets of $\{\mathcal{P}_1, \ldots \mathcal{P}_n\}$, such as $\mathbb{A} \subseteq 2^{\{\mathcal{P}_1, \ldots \mathcal{P}_n\}}$ is an access structure. Authorized sets are those that are in $\mathbb{A}$, whereas unauthorized sets are those that are not in $\mathbb{A}$. The encryption has been performed by the data owners. The global public key K_G, access structure $(\mathcal{D}, \delta)$ of size $l \times n$, time stamp t, user data as well as the symmetric key (K_{sym}) are used as input.

Step 1: To acquire the ciphertext CT_{sym}, encrypt the data with the key K_{sym}.

Step 2: Randomly select a secret element s and a set of numbers $v_2, \ldots v_n$ from $\mathbb{Z}_p$.

Step 3: Construct a vector $\vec{v} = (s, v_2, \ldots v_n)^T$.

Step 4: Compute the security parameter $\zeta_i = \mathcal{D}_i.\vec{v}$.

Step 5: Randomly select $\varphi_1, \ldots \varphi_l$ for the computation of cipher text as follows:

$$\left.\begin{array}{l} \mathcal{C}_0 = e\left(g,g\right)^{\alpha s}.K_{sym} \\ \mathcal{C}_1 = g^s \\ \mathcal{C}_2 = F_2\left(t\right)^s \\ \mathcal{C}_{3,i} = \omega^{\zeta_i}.\upsilon^{\varphi_i} \\ \mathcal{C}_{4,i} = F_1\left(Att_{\delta(i)}\right)^{-\zeta_i} \\ \mathcal{C}_{5,i} = g^{\zeta_i} \end{array}\right\} \tag{6}$$

The cipher text output $CT = \left[\left(\mathcal{D},\delta\right), t, \mathcal{C}_0, \mathcal{C}_1, \mathcal{C}_2, \left\{\mathcal{C}_{3,i}, \mathcal{C}_{4,i}, \mathcal{C}_{5,i}\right\}_{i\in l}\right]$ as well as CT_{sym}. Then the cipher text as well as symmetric CT are sent to the cloud for storage.

For the decryption of data in the cloud, a token has been generated by both the data user as well as blockchain. The user token generation has been fully performed by the data user. Where the random number r has been selected from $\mathbb{Z}_p$. The user token has been computed as

$$Tk_{user} = \left(g^{\alpha/\gamma}\right)^{\beta+r} \tag{7}$$

Then the hashing of keywords has been computed and sent both the user token and keyword hash to the blockchain for blockchain token generation. The verifiable secret sharing protocol with parameters (m,n) has been utilized for blockchain token generation. Initially, the parameter $\left\{a_j\right\}_{j\in ID}$ is broadcasted to the consensus nodes. Each node broadcast $\left\{g^{\gamma.a_{j,i}}, F_1\left(Att_j\right)^{a_{j,i}}\right\}_{j\in ID}$ based on its secret shares $\left\{a_j\right\}_{j\in ID}$. More than m consensus nodes are involved in generating the blockchain token for the user.

$$\begin{aligned} Tk_{BC_1} &= Tk_{user}.\left(g^{\alpha/\gamma}\right)^{H(KW)} \\ Tk_{BC_1} &= \left(g^{\alpha/\gamma}\right)^{(\beta+r+H(KW))} \end{aligned} \tag{8}$$

$$\begin{aligned} Tk_{BC_{2,j}} &= Tk_{user}.\prod_{i=1}^{m}\left(F_1\left(Att_j\right)^{a_{j,i}}\right)^{L(i)} \\ Tk_{BC_{2,j}} &= \left(g^{\alpha/\gamma}\right)^{(\beta+r)}.F_1(Att_j)^{a_j} \end{aligned} \tag{9}$$

$$\begin{aligned} Tk_{BC_{3,j}} &= \prod_{i=1}^{m}\left(g^{\gamma.a_{j,i}}\right)^{L(i)} \\ Tk_{BC_{3,j}} &= g^{\gamma.aj} \end{aligned} \tag{10}$$

Then the tokens are sent to the cloud from the blockchain, which is utilized for the decryption of data in the cloud. The decryption has been performed partially in the cloud then the complete decryption has been performed by the data user. The partial decryption by the cloud has been performed as

$$\frac{\prod_i\left[e\left(\mathcal{C}_{3,i}, Tk_2\right)e\left(\mathcal{C}_{4,i}, Tk_{4,\delta(i)}\right)e\left(\mathcal{C}_{5,i}, Tk_{5,\delta(i)}\right)\right]^{c_i}}{e\left(\mathcal{C}_2, Tk_3\right)^{-1}e\left(\mathcal{C}_1, Tk_1\right)} = CT'_{cloud} \tag{11}$$

The partially decrypted data by the cloud as mentioned in Eq. (11), is provided to the data users. They completely decrypted the data using their private key (K_{pri}). The computation for decryption is

given as

$$K_{sym} = \mathcal{C}_0 . \left(CT'_{cloud}\right)^{1/\beta}$$
$$= \frac{e\,(g,g)^{\alpha s} . K_{sym}}{\left(e\left(g, K_{pri}{}^{\alpha}\right)^{s}\right)^{1/\beta}}$$
$$= \frac{e\,(g,g)^{\alpha s} . K_{sym}}{e\,(g,g^{\alpha})^{s}} \tag{12}$$

To retrieve the plaintext, the data user uses the symmetric algorithm using a symmetric key. This method fails if the symmetric key is incorrect. Otherwise, the user can receive the desired information. Thus the proposed cryptographic method has assured the privacy of the data stored in the cloud.

3.4 Smart Contract-Based DoS Attack Mitigation

Many IoT devices are susceptible to a variety of cyberattacks because they lack the memory and computational complexity of modern computer systems. One of the most important risks to the IoT is denial of service (DoS) attacks. The attacker wants to disrupt operations by overloading the servers with data traffic. The enemy can take control of IoT devices and force them to send any amount of data to the DoS attack target.

Despite numerous research attempts to identify DDoS assaults using machine learning techniques, there is a lack of a systematic strategy to avoid commonly entrenched problems like colinearity and duplication. Thus to mitigate the DoS attack in IoT devices, a smart contract-based validation has been performed to validate the devices as trusted or untrusted with blockchain. Based on a list of permitted devices stored in the blockchain's smart contract, the contract will approve each device. The contract examines a list of authorized device addresses when a device requests a function and only gives access if the device's address is on the list. If the device cannot gain access or is not on the list, all data communications and interactions with it will be deleted and ruled invalid.

When one or more devices transmit abnormally large amounts of data to a server, they overload it and use its resources, resulting in the DoS issue. Such attacks can be avoided by using the resource limit property of the blockchain, which assures that once the limit is reached, no further resources can be utilized. To prevent the system from becoming overloaded, a resource limit is set for each transaction processed by the proposed smart contract. Let us take an example of N IoT devices which have a resource limit of RL_i. The maximum bandwidth of the server is BW, then

$$\sum_{i=1}^{N} RL_i \leq BW \tag{13}$$

According to Eq. (13), even if all devices begin simultaneously delivering data at the limits of their resources, the server bandwidth will not be depleted. In addition, any DoS attack that aims to exhaust server resources must first exhaust the resources of the malicious device until they are exhausted. The malicious device's activity—in terms of packets sent to the server—will stop once the resource limit is reached, preventing the server from becoming overloaded. Each device's limit is set when it registers in the blockchain, and it can be set as desired. As a result, the servers are effectively protected from denial-of-service attacks by the proposed method.

4 Results

This section gives a thorough explanation of the implementation outcomes and the performance of our suggested framework. It also includes a comparison analysis to make sure that our suggested framework outperforms the already-used IoT security solutions.

4.1 System Specifications

The system requirements for the proposed framework's implementation in the Python platform are provided below:

Platform: Python

OS: Windows 8

Processor: Intel Core i5

RAM: 8 GB RAM

4.2 Simulation Outputs and Performance Evaluation

In this section, the simulation outputs of the proposed framework as well as the performance evaluation metrics are presented. Accuracy, precision, recall, sensitivity, F-measure, execution time, encryption time, and decryption time have all been used to measure the proposed framework's performance.

In this work, initially, several IoT devices are registered in the blockchain. To do this, initially, a decentralized blockchain has been created. Each block has a separate hash function to securely store the data, which is shown in Fig. 4.

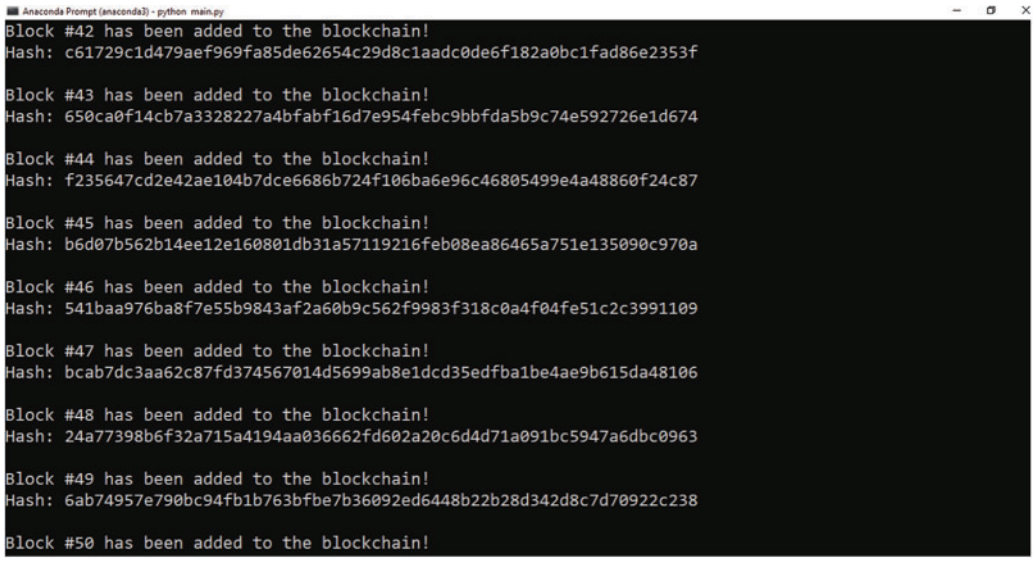

Figure 4: Generated hash of each IoT device in the blockchain

Once the blocks are created with different hash functions, those hashes are validated to whether each hash is identical or not. The validation of blocks with their hashes in the blockchain is depicted in Fig. 5.

Figure 5: Validation of hashes in the blockchain

Once the blocks are created in the blockchain, the IoT devices are registered in each block through the registration process via certification authority and local peer. The registration of IoT devices is depicted in Fig. 6.

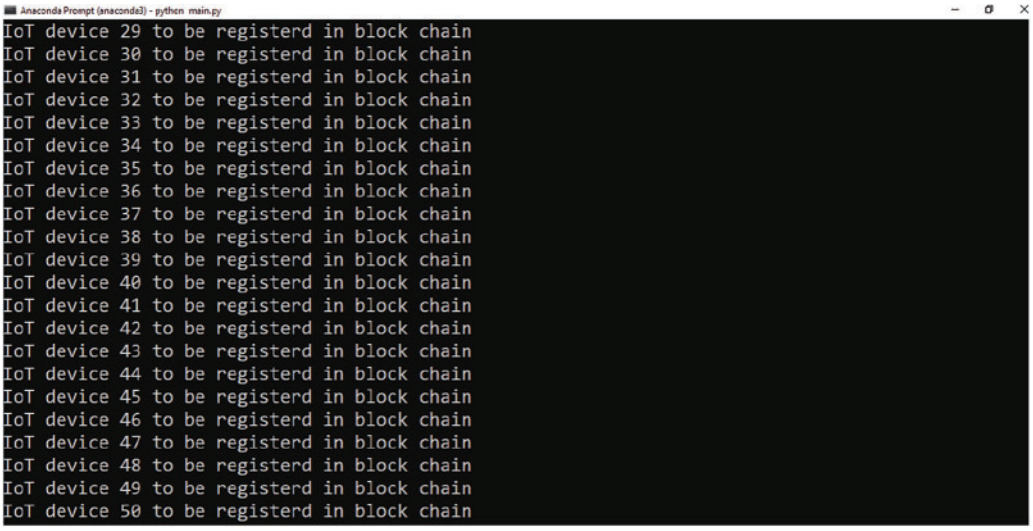

Figure 6: Registration of IoT devices

The proposed framework utilizes attribute-based cryptography through blockchain to maintain the privacy of the data through encryption and decryption of data in the blockchain. The proposed technique efficiently encrypts the data by constructing a vector with a secret element, which cannot be intruded upon by anyone. Fig. 7 states the encrypted data of sample data.

Figure 7: Encrypted data

The proposed framework utilizes attribute-based cryptography through blockchain to maintain the privacy of the data through encryption and decryption of data in the blockchain. The proposed work efficiently decrypts the encrypted data partially by cloud and remaining by the user with minimal time, which is presented in Fig. 8.

Figure 8: Decrypted data

Fig. 9 states the execution time that is simulation time of the implemented proposed framework. The execution time was computed with a varying number of IoT devices connected and registered with the blockchain. The execution time took a minimum of 0.1965 s with 10 IoT devices and a maximum of 0.2076 s with 50 IoT devices.

The proposed framework employs attribute-based cryptography in conjunction with blockchain to provide data privacy by encrypting and decrypting data in the blockchain. The presented technique efficiently encrypts the data with lower time consumption, which is depicted in Fig. 10. The encryption

time has increased with the increasing amount of data size. The 10 bytes of data have been encrypted within 72.3 ms similarly, the 50 bytes of data have been encrypted within 73.8 ms alone.

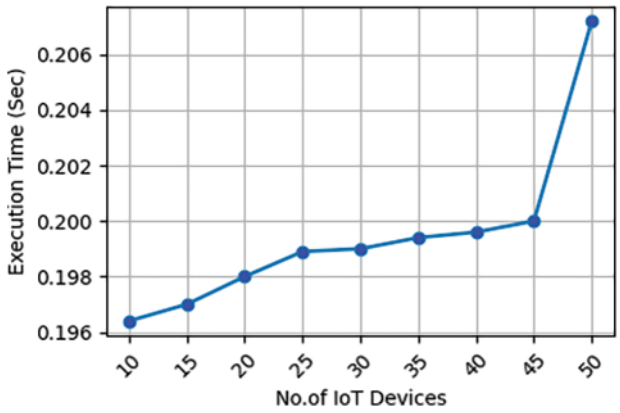

Figure 9: Execution time

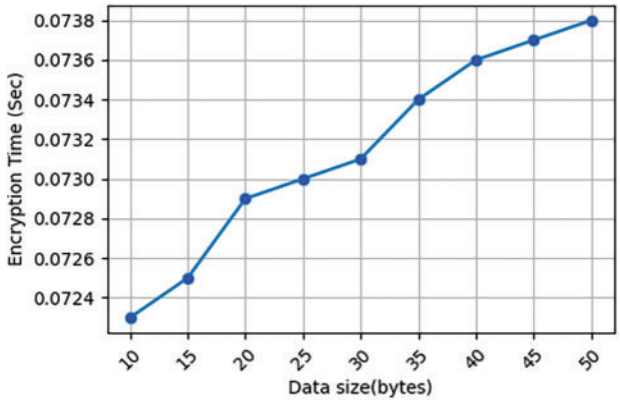

Figure 10: Encryption time

The proposed framework employs attribute-based cryptography in conjunction with blockchain to provide data privacy by encrypting and decrypting data in the blockchain. The presented technique accurately decrypts the data as original data with lower time consumption, which is depicted in Fig. 11. The decryption time has increased with the increasing amount of data size. The 10 bytes of data have been decrypted within 184.7 ms similarly, the 50 bytes of data have been decrypted within 188.3 ms.

Fig. 12 states the accuracy of the overall decentralized scalable framework with blockchain. The accuracy of the proposed work is around 96.9%. Although the accuracy has decreased as the number of IoT devices has grown, the differences are still very modest 10^{-2} percent.

Fig. 13 states the precision of the overall decentralized scalable framework with blockchain. The proposed work's precision is approximately 98.4%, with the precision that is closest to accuracy decreasing as more IoT devices enter the blockchain. However, the variation was too small for the increasing number of devices at 10^{-3} percent.

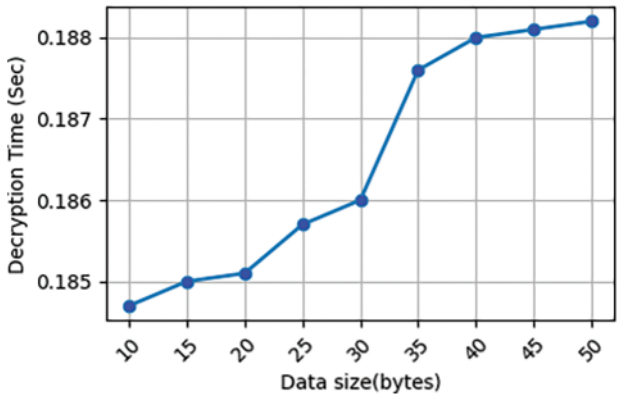

Figure 11: Decryption time

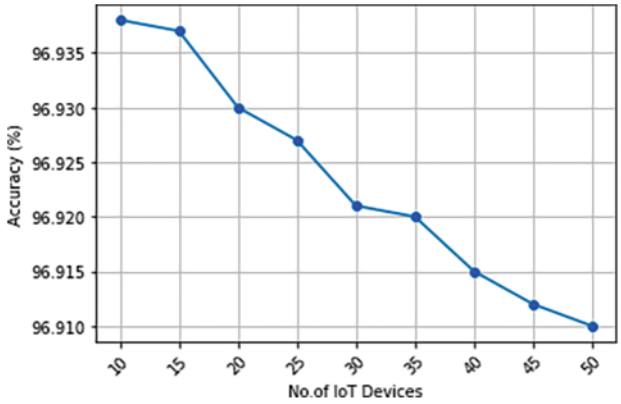

Figure 12: Accuracy

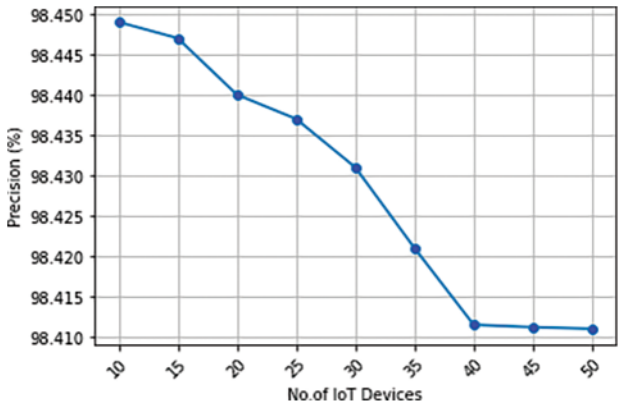

Figure 13: Precision

Fig. 14 states the sensitivity of the overall decentralized scalable framework with blockchain. The sensitivity of the suggested work is approximately 98.4%; nevertheless, as there are more IoT devices, the sensitivity has decreased. These fluctuations, however, are only 10^{-2} percent only.

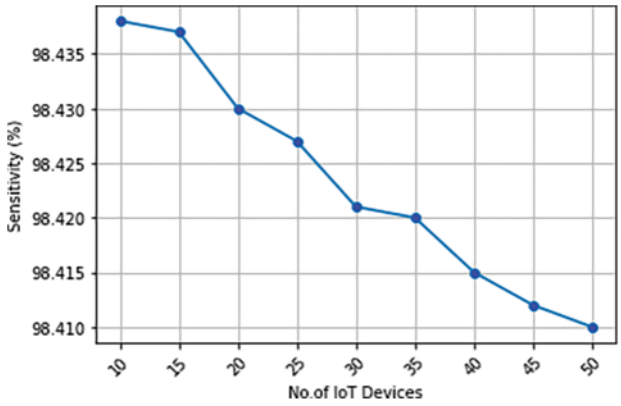

Figure 14: Sensitivity

Fig. 15 states the recall of the overall decentralized scalable framework with blockchain. The proposed work achieves a recall of approximately 98.4%, however, the recall was reduced as the number of IoT devices increased. However, the variations are too small in terms of 10^{-2} percent alone.

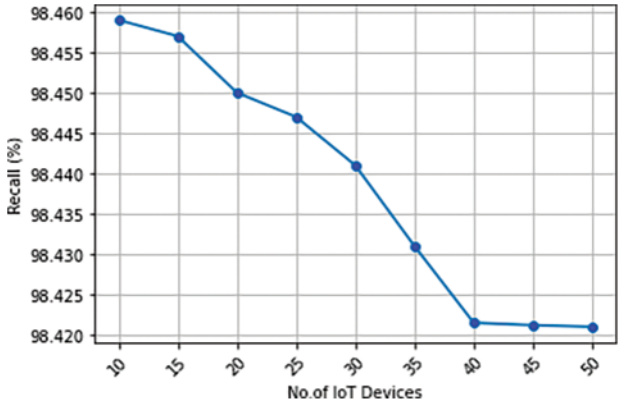

Figure 15: Recall

Fig. 16 states the F-measure of the overall decentralized scalable framework with blockchain. The F-measure of the proposed work achieves around 98.4%, whereas, the F-measure was decreased however, the variations are too smaller in terms of 10^{-2} percent only.

4.3 Comparison Analysis

To verify the performance of the suggested technique, this section compares the performance of the proposed framework with the IoT-based security work with already existing work.

Fig. 17 and Table 2 show a comparison of the effectiveness of DoS attack mitigation strategies based on machine learning, including Support Vector Machine (SVM), Decision Tree (DT), Naive Bayes (NB), Artificial Neural Network (ANN), and Unsupervised Machine Learning [33] (USML). The proposed method's accuracy is 96.9%, which is 2% better than the USML and 33% better than the ANN.

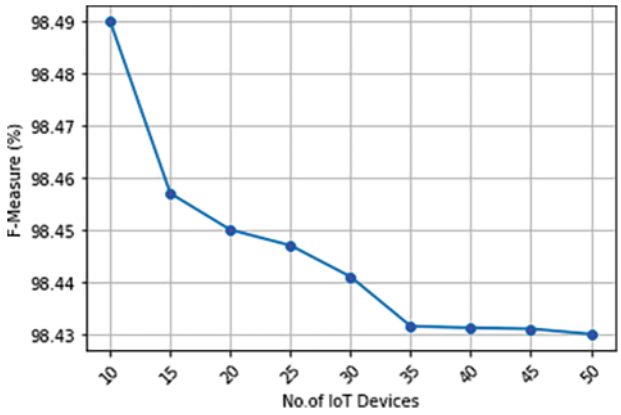

Figure 16: F-measure

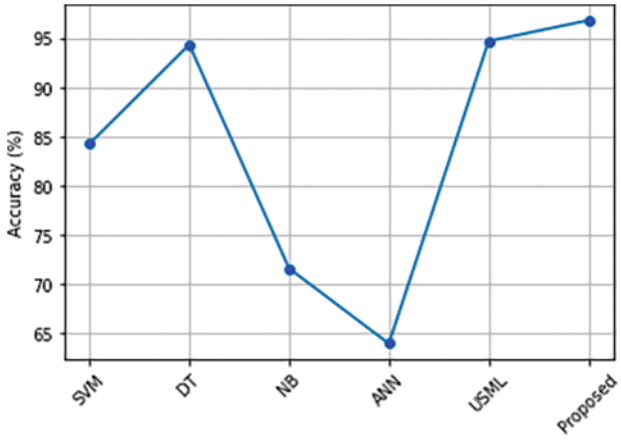

Figure 17: Comparison of accuracy

Table 2: Comparison of accuracy

Techniques	Accuracy
SVM	84.32%
DT	94.43%
NB	71.63%
ANN	63.97%
USML	94.78%
Proposed	96.9%

Fig. 18 and Table 3 compare various machine learning-based DoS attack mitigation strategies, including Support Vector Machine (SVM), Decision Tree (DT), Naive Bayes (NB), Artificial Neural Network (ANN), and Unsupervised Machine Learning, in terms of the precision of DoS attack mitigation (USML). The accuracy of the suggested method is 98.43%, which is 10.4% more accurate than the SVM and 4% more accurate than the USML.

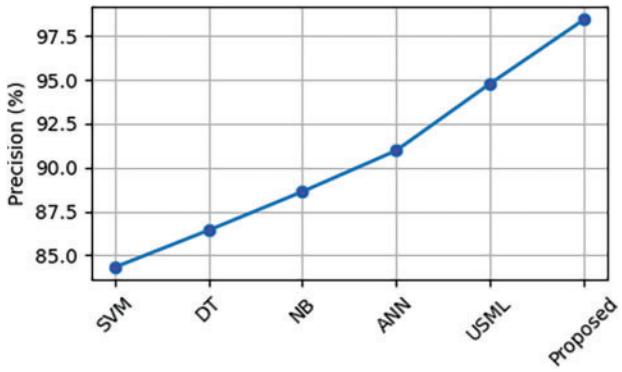

Figure 18: Comparison of precision

Table 3: Comparison of precision

Techniques	Precision
SVM	84.32%
DT	86.43%
NB	88.63%
ANN	90.97%
USML	94.78%
Proposed	98.43%

Fig. 19 and Table 4 present a comparison of the sensitivity of machine learning-based DoS attack mitigation techniques, including Support Vector Machine (SVM), Decision Tree (DT), Naive Bayes (NB), Artificial Neural Network (ANN), and Unsupervised Machine Learning (UML), with existing DoS attack mitigation techniques [33] (USML). The sensitivity of the suggested method is 98.8%, which is 9% more sensitive than the USML and 2% more sensitive than the ANN.

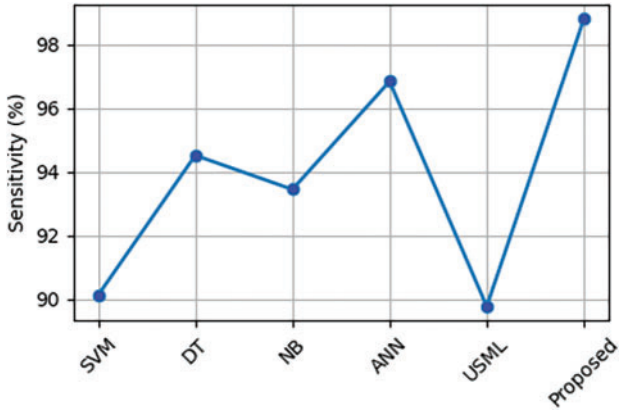

Figure 19: Comparison of sensitivity

Table 4: Comparison of sensitivity

Techniques	Sensitivity
SVM	90.13%
DT	94.52%
NB	93.45%
ANN	96.84%
USML	89.78%
Proposed	98.8%

Fig. 20 and Table 5 compare the recall of DoS attack mitigation with known machine learning-based DoS attack mitigation strategies [33] such as Support Vector Machine (SVM), Decision Tree (DT), Naive Bayes (NB), Artificial Neural Network (ANN), and Unsupervised Machine Learning (USML). The recall achieved by the suggested method is 98.437%, which is 14% more than the SVM and 4% more than the USML.

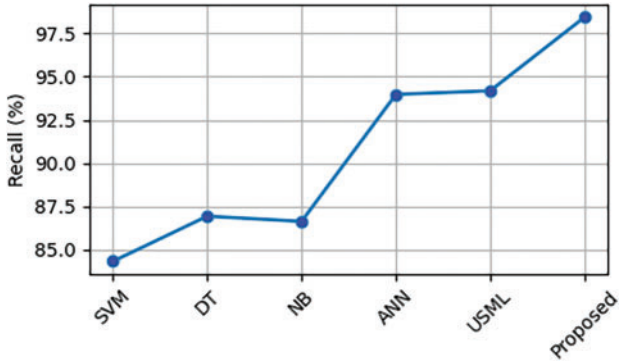

Figure 20: Comparison of recall

Table 5: Comparison of recall

Techniques	Recall
SVM	84.32%
DT	86.93%
NB	86.63%
ANN	93.97%
USML	94.18%
Proposed	98.437%

Fig. 21 and Table 6 show a comparison of the existing machine learning-based DoS attack mitigation techniques, such as Support Vector Machine (SVM), Decision Tree (DT), Naive Bayes (NB), Artificial Neural Network (ANN), and Unsupervised Machine Learning, with the F-measure

of DoS attack mitigation (USML). The F-measure of the suggested method is 98.4%, 14% better than the SVM, and 4% better than the USML.

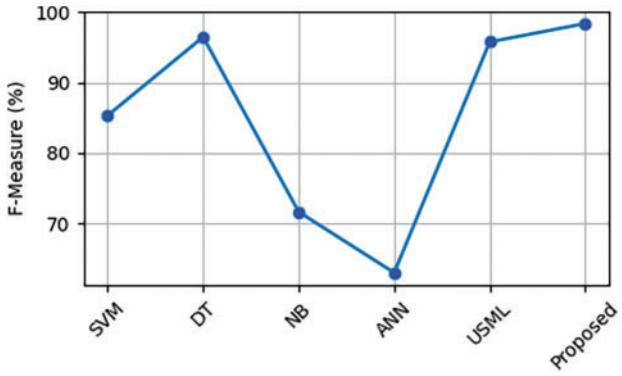

Figure 21: Comparison of F-measure

Table 6: Comparison of F-measure

Techniques	F-measure
SVM	85.32%
DT	96.49%
NB	71.62%
ANN	62.97%
USML	95.78%
Proposed	98.4%

5 Conclusion

The Internet of Things (IoT), which has applications in smart homes, wearable technology, healthcare, and other areas, is gradually becoming part of our daily lives. Because of the wide variety of uses, shared data contains a sizable amount of personal data. In the IoT, the privacy of this information becomes of utmost importance. This study introduces a novel decentralized and secure framework with blockchain integration. A decentralized, scalable framework has been proposed based on blockchain for privacy preservation in IoT. To avoid the single-point OF failure, an accredited access control scheme has been introduced by incorporating blockchain with local peers to record each transaction and verify the signature to access. As a result, blockchain-based attribute-based cryptography has been implemented to safeguard data storage privacy by generating threshold parameters, managing keys, and revoking users on the blockchain. Finally, an innovative contract-based DoS attack mitigation method has been incorporated to effectively validate devices with intelligent contracts as trusted or untrusted, preventing the server from becoming overwhelmed. The results show that the suggested framework performs best in terms of accuracy, precision, sensitivity, recall, and F-measure at 96.9%, 98.43%, 98.8%, 98.43%, and 98.4%, respectively.

Acknowledgement: The first author is thankful to all co-authors who contributed to carrying out the proposed work.

Funding Statement: The authors received no specific funding for this study.

Author Contributions: Sohaib A. Latif: Conceptualization, Methodology, Writing, Supervision, Conceptualization, Innovation. M. Saad B. Bin Ilyas: Software, Methodology. Azhar Imran: Visualization, Revisions. Hamad Ali Abosaq: Validation, Software. Abdulaziz Alzubaidi: Results, Software. Vincent Karovič Jr. Technical writing, Revisions, Grammar check.

Availability of Data and Materials: Not applicable.

Conflicts of Interest: The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] S. A. Latif *et al.*, "Blockchain and SDN integrated security architecture for IoT network of cyber-physical systems," *Comput. Commun.*, vol. 181, pp. 274–283, 2022.

[2] A. S. Putra and H. L. H. S. Warnars, "Intelligent traffic monitoring system (ITMS) for smart city based on IoT monitoring," in *2018* Indonesian. *Association for Pattern Recognit. Int. Conf. (INAPR)*, IEEE, 2018, pp. 161–165.

[3] Y. Jie *et al.*, "Smart home system based on IoT technologies," in *2013 Int. Conf. Comput. Inform. Sci.*, IEEE, 2013, pp. 1789–1791.

[4] T. Poongodi, R. Krishnamurthi, R. Indrakumari, P. Suresh, and B. Balusamy, "Wearable devices and IoT," in *A Handbook of Internet of Things in Biomedical and Cyber Physical System*, 2019, pp. 245–273.

[5] L. D. Xu, W. He, and S. Li, "Internet of things in industries: A survey," *IEEE Trans. Ind. Inform.*, vol. 10, no. 4, pp. 2233–2243, 2014. doi: 10.1109/TII.2014.2300753.

[6] H. Arasteh *et al.*, "IoT-based smart cities: A survey," in *2016 IEEE 16th Int. Conf. Environ. Electr. Eng. (EEEIC)*, IEEE, 2016, pp. 1–6.

[7] M. Wazid, A. K. Das, K. Vivekananda Bhat, and A. V. Vasilakos, "Lam-CIoT: Lightweight authentication mechanism in cloud-based IoT environment," *J. Netw. Comput. Appl.*, vol. 150, pp. 102496, 2020. doi: 10.1016/j.jnca.2019.102496.

[8] A. Chaudhuri, "Internet of things data protection and privacy in the era of the general data protection regulation," *J. Data Protec. & Priv.*, vol. 1, no. 1, pp. 64–75, 2017.

[9] I. Farris, T. Taleb, Y. Khettab, and J. Song, "A survey on emerging SDN and NFV security mechanisms for IoT systems," *IEEE Commun. Surv. & Tutor.*, vol. 21, no. 1, pp. 812–837, 2019. doi: 10.1109/COMST.2018.2862350.

[10] C. Liu, Y. Xiao, V. Javangula, Q. Hu, S. Wang and X. Cheng, "Normachain: A blockchain-based normalized autonomous transaction settlement system for IoT-based e-commerce," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4680–4693, 2019.

[11] M. Frustaci, P. Pace, G. Aloi, and G. Fortino, "Evaluating critical security issues of the IoT world: Present and future challenges," *IEEE Internet Things. J.*, vol. 5, no. 4, pp. 2483–2495, 2018. doi: 10.1109/JIOT.2017.2767291.

[12] K. Choudhary, G. S. Gaba, I. Butun, and P. Kumar, "Make-it—a lightweight mutual authentication and key exchange protocol for industrial internet of things," *Sens.*, vol. 20, no. 18, pp. 5166, 2020. doi: 10.3390/s20185166.

[13] S. Kumar, Y. Hu, M. P. Andersen, R. A. Popa, and D. E. Culler, "JEDI: Many-to-many end-to-end encryption and key delegation for IoT," arXiv:1905.13369, 2020.

[14] N. Zhang *et al.*, "Physical-layer authentication for internet of things via WFRFT-based gaussian tag embedding," *IEEE Internet Things J.*, vol. 7, no. 9, pp. 9001–9010, 2020. doi: 10.1109/JIOT.2020.3001597.

[15] J. Han *et al.*, "Do you feel what I hear? Enabling autonomous IoT device pairing using different sensor types," in *2018 IEEE Symp. on Secur. and Privacy (SP)*, IEEE, May 2018, pp. 836–852.

[16] J. Mao, S. Zhu, and J. Liu, "An inaudible voice attack to context-based device authentication in smart IoT systems," *J. Syst. Architect.*, vol. 104, pp. 101696, 2020.
[17] S. Koppula and J. Muthukuru, "Secure digital signature scheme based on elliptic curves for internet of things," *Int. J. Electr. Comput. Eng. (IJECE)*, vol. 6, no. 3, pp. 1002, 2016. doi: 10.11591/ijece.v6i3.9420.
[18] M. Lavanya and V. Natarajan, "LWDSA: Light-weight digital signature algorithm for wireless sensor networks," *Sādhanā*, vol. 42, no. 10, pp. 1629–1643, 2017. doi: 10.1007/s12046-017-0718-5.
[19] M. Wazid, A. K. Das, V. Odelu, N. Kumar, M. Conti and M. Jo, "Design of secure user authenticated key management protocol for generic IoT networks," *IEEE Internet Things J.*, vol. 5, no. 1, pp. 269–282, 2018. doi: 10.1109/JIOT.2017.2780232.
[20] J. Sugier, "Improving FPGA implementations of blake and BLAKE2 algorithms with memory resources," in *Advances in Dependability Engineering of Complex Systems:* Brunów, Poland: Springer International Publishing, 2017, pp. 394–406.
[21] D. Fang, Y. Qian, and R. Q. Hu, "A flexible and efficient authentication and secure data transmission scheme for IoT applications," *IEEE Internet Things J.*, vol. 7, no. 4, pp. 3474–3484, 2020. doi: 10.1109/JIOT.2020.2970974.
[22] U. Chatterjee *et al.*, "Building PUF based authentication and key exchange protocol for IoT without explicit crps in verifier database," *IEEE Trans. Depend. Secure. Comput.*, vol. 16, no. 3, pp. 424–437, 2019. doi: 10.1109/TDSC.2018.2832201.
[23] K. Rahim, H. Tahir, and N. Ikram, "Sensor based PUF IoT authentication model for a smart home with private blockchain," in *2018 Int. Conf. Appl. Eng. Math. (ICAEM)*, 2018.
[24] M. Samaniego, U. Jamsrandorj, and R. Deters, "Blockchain as a service for IoT," in *2016 IEEE Int. Conf. Internet Things (iThings)*, 2016.
[25] D. Minoli and B. Occhiogrosso, "Blockchain mechanisms for IoT security," *Internet. of Things.*, vol. 1–2, pp. 1–13, 2018. doi: 10.1016/j.iot.2018.05.002.
[26] S. Latif *et al.*, "An enhanced virtual cord protocol based multi-casting strategy for the effective and efficient management of mobile ad hoc networks," *Computers*, vol. 12, no. 1, pp. 21, 2023. doi: 10.1109/JIOT.2017.2780232.
[27] S. C. Lin, C. Y. Wen, and W. A. Sethares, "Two-tier device-based authentication protocol against puea attacks for IoT applications," *IEEE Trans. Signal Inform. Process. Over Netw.*, vol. 4, no. 1, pp. 33–47, 2018. doi: 10.1109/TSIPN.2017.2723761.
[28] S. Latif *et al.*, "IoT technology enabled stochastic computing paradigm for numerical simulation of heterogeneous mosquito model," *Multimedia Tools and Appl.*, vol. 82, no. 12, pp. 18851–18866, 2023.
[29] A. K. Das, M. Wazid, N. Kumar, A. V. Vasilakos, and J. J. Rodrigues, "Biometrics-based privacy-preserving user authentication scheme for cloud-based industrial internet of things deployment," *IEEE Internet Things J.*, vol. 5, no. 6, pp. 4900–4913, 2018. doi: 10.1109/JIOT.2018.2877690.
[30] X. Li, J. Niu, M. Z. Bhuiyan, F. Wu, M. Karuppiah and S. Kumari, "A robust ECC-based provable secure authentication protocol with privacy preserving for industrial internet of things," *IEEE Trans. Indust. Inform.*, vol. 14, no. 8, pp. 3599–3609, 2018. doi: 10.1109/TII.2017.2773666.
[31] S. Paliwal, "Hash-based conditional privacy preserving authentication and key exchange protocol suitable for industrial internet of things," *IEEE Access*, vol. 7, pp. 136073–136093, 2019. doi: 10.1109/ACCESS.2019.2941701.
[32] V. Rao and K. V. Prema, "Light-weight hashing method for user authentication in internet-of-things," *Ad Hoc Netw.*, vol. 89, pp. 97–106, 2019. doi: 10.1016/j.adhoc.2019.03.003.
[33] R. Kumar, P. Kumar, R. Tripathi, G. P. Gupta, N. Kumar and M. M. Hassan, "A privacy-preserving-based secure framework using blockchain-enabled deep-learning in cooperative intelligent transport system," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 9, pp. 16492–16503, 2022. doi: 10.1109/TITS.2021.3098636.
[34] P. Kumar, R. Kumar, G. P. Gupta, R. Tripathi, A. Jolfaei and A. K. M. N. Islam, "A blockchain-orchestrated deep learning approach for secure data transmission in IoT-enabled healthcare system," *J. Parallel. Distr. Comput.*, vol. 172, pp. 69–83, 2023. doi: 10.1016/j.jpdc.2022.10.002.

[35] R. Kumar, P. Kumar, M. Aloqaily, and A. Aljuhani, "Deep-learning-based blockchain for secure zero touch networks," *IEEE Commun. Mag.*, vol. 61, no. 2, pp. 96–102, 2023.
[36] P. Kumar, R. Kumar, S. Garg, K. Kaur, Y. Zhang and M. Guizani, "A secure data dissemination scheme for IoT-based e-health systems using AI and blockchain," in *GLOBECOM 2022–2022 IEEE Global Commun. Conf.*, 2022.
[37] P. Kumar, R. Kumar, A. A. F. Abhinav Kumar, S. Garg, and S. Singh, "Blockchain and deep learning for secure communication in digital twin empowered industrial IoT network," *IEEE Trans. Netw. Sci. Eng.*, pp. 1–13, 2022.
[38] P. Kumar, G. P. Gupta, and R. Tripathi, "A distributed ensemble design based intrusion detection system using fog computing to protect the internet of things networks," *J. Amb. Inteli. Hum. Comput.*, vol. 12, no. 10, pp. 9555–9572, 2020.
[39] Z. A. Lux *et al.*, "Distributed-ledger-based authentication with decentralized identifiers and verifiable credentials," in *2020 2nd Conf. Blockchain Res. & Appl. Innov. Netw. Serv. (BRAINS)*, IEEE, 2020, pp. 71–78.