

# A Lightweight Access Control Scheme with Attribute Policy for Blockchain-Enabled Internet of Things

Syed Sajid Ullah<sup>a</sup>, Vladimir Oleshchuk<sup>b</sup> and Harsha S. Gardiyawasam Pussewalage<sup>c</sup>

*Department of Information and Communication Technology, University of Agder, Grimstad N-4898, Norway*

**Keywords:** Blockchain, Internet of Things (IoT), Access Control, blockchain-enabled Internet of Things, Digital Signature, Hyper Elliptic Curve Cryptography.


**Abstract:** The Internet of Things (IoT) revolution has increased the number of connected devices, leading to new security challenges. One of these challenges is the management of access control for these devices. Traditional access control methods may not be able to address these challenges effectively. This paper proposes attribute-based access control (ABAC) for the blockchain-enabled Internet of Things (BE-IoT). ABAC allows access to be granted or denied based on the attributes of the user or device requesting access rather than relying on a central authority to manage access control information. This allows for more flexible and dynamic access control policies that can adapt to changing situations and minimize the risk of unauthorized access. Blockchain technology provides a secure and transparent way to manage access control information for IoT devices. Blockchain is a decentralized and distributed ledger allowing secure and tamper-proof information storage. By storing access control information on the blockchain, it can be shared across a network of devices transparently and securely. The authors conduct a security analysis to evaluate and compare the proposed scheme to existing schemes. The analysis results indicate that the proposed scheme has the advantage of using minimal computation time and communication overhead compared to previous solutions. The authors suggest that the ABAC scheme using blockchain combined with a lightweight Hyperelliptic Curve Cryptosystem (HCC) is well suited for secure deployment in IoT.


## 1 INTRODUCTION


The Internet of Things (IoT) refers to the integration of diverse physical entities equipped with sensors, embedded software, and network interfaces, such as household appliances, automobiles, and industrial machinery (Kumar et al., 2019), (Sinha et al., 2022). These devices collect and exchange data, thereby expanding their capabilities. The remote interaction and control of these devices have the potential to radically alter lifestyle and occupational norms, with substantial implications for business dynamics. However, IoT also brings new security challenges to the table; as the number of connected devices increases, so does the number of potential vulnerabilities (Omolara et al., 2022), (Swessi and Idoudi, 2022). Protecting IoT devices from unauthorized access is crucial for preventing data leakage and protecting valuable and sensitive information stored on these IoT devices.

Access control is a vital aspect of cybersecurity that ensures that only individuals with the proper authorization can access computer systems, devices, and the sensitive information stored within them. By implementing effective access control measures, organizations can safeguard their critical assets and prevent potential security breaches (Sandhu and Samarati, 1994). When it comes to providing a secure and efficient mechanism for the protection of information in the large-scale and complex environment of the IoT, traditional access control models, such as discretionary access control (DAC), mandatory access control (MAC), and role-based access control (RBAC), have limitations (Hu et al., 2015). These models were designed for use in closed systems and did not have the capability to deal with the dynamic interactions that can arise between a large number of connected devices in an IoT environment.

The attribute-based access control (ABAC) (Wang et al., 2004), allows access to be granted or denied depending on the attributes of the user or device requesting access. A user's identity, location,

<sup>a</sup>  <https://orcid.org/0000-0002-5406-0389>

<sup>b</sup>  <https://orcid.org/0000-0002-7905-1016>

<sup>c</sup>  <https://orcid.org/0000-0002-3623-3362>

role, or even the device can be considered among these attributes. Traditional access control methods have been replaced by ABAC, which offers a finer-grained level of control over who can access various resources. In addition, ABAC makes it possible to have access control policies that are more adaptable and dynamic, which means they can accommodate shifting conditions and reduce the likelihood of unauthorized access.

Access control information can be stored in a ledger that is decentralized and distributed if blockchain technology is used, providing an increased level of security as well as transparency. In addition, because blockchain is a decentralized and distributed ledger, it enables all of the parties in the network to have a copy of the same data. This makes it extremely difficult to alter the data, further increasing its security. The combination of blockchain technology, IoT, and ABAC offers a more efficient and secure access control approach to handle a large number of IoT devices. In a Blockchain-Enabled ABAC (BE-ABAC) for IoT, each device has a unique identifier stored on the blockchain. Access requests are sent to the blockchain network for evaluation. Furthermore, the blockchain network would verify the attributes of the user or device against the device's access control policy, which is also recorded on the blockchain. Implementing blockchain in this setting offers several advantages over more conventional approaches to controlling access. Because it is decentralized and distributed, the blockchain does not have a single point that can be attacked or compromised. In addition, the utilization of smart contracts enables the automated execution of access control policies, which can help to contribute to an increase in efficiency while simultaneously decreasing the likelihood of a mistake being made by a human.

To guarantee the security of the attributes utilized in the access control determination, ABAC systems often use various cryptographic methods, such as RSA, Bilinear pairing (BP), Diffie-Hellman (DH), Elliptic Curve Cryptosystem (ECC), and HCC (Hussain et al., 2021). It has been demonstrated that HCC provides superior performance in terms of key length and efficiency compared to ECC, BP, DH, and RSA (Hussain et al., 2020). HCC also has a shorter key length. In addition, HCC uses an 80-bit key, which offers a high level of protection and has a size appropriate for the resource-constrained devices typical for IoT environments. In general, the utilization of HCC in ABAC systems for IoT, in combination with Blockchain technology, provides a balance of security and efficiency, making it an appropriate choice to secure communication in IoT systems.

Also, blockchain allows for creating a decentralized and tamper-proof record of access control decisions. This can be used to ensure the integrity of the attributes used in the access control decision and the authenticity of the devices accessing the resources.

Inspired by the above considerations, we present a lightweight ABAC scheme for BE-IoT. The proposed scheme is considered lightweight because it is built on the fundamental idea of HCC. The main contributions of the paper are listed below.

- We designed an ABAC system for blockchain-enabled Internet of Things (BE-IoT) that is both secure and lightweight.
- We proved that the proposed scheme is secure based on the hardness of the Hyperelliptic Curve Discrete Logarithm Problem in the random oracle model.
- We compare the efficiency of the proposed scheme with previous schemes, and the results indicate that the proposed scheme has superior efficiency in terms of computational and communication costs.

## 1.1 Paper Organization

The paper is organized into nine sections: Introduction and Motivation (Section 1), Literature Review (Section 2), Threat Model (Section 3), Network Model for Access Control (Section 4), Proposed Access Control Mechanism (Section 5), Deployment and Workflow (Section 6), Formal Security Analysis (Section 7), Performance Analysis (Section 8), and Conclusion (Section 9).

## 2 RELATED WORK

(Alansari et al., 2017), presented an innovative identity and access management solution in cloud federations. The proposed solution utilizes ABAC policies and blockchain technology with trusted hardware from Intel to protect users' identities while ensuring the policy review process is honest and transparent. Due to the intensive Bilinear Pairing algorithm, the proposed method consumes a great deal of computational and communication resources, and the proposed system requires formal security proof. (Wang et al., 2018), examine a data storage and sharing scheme in decentralized storage systems and presents a framework that integrates the interplanetary file system, the Ethereum blockchain, and ABE technology. This framework allows data owners to encrypt shared data and control who can access it through access

policies while implementing a keyword search function on the ciphertext of the data using smart contracts on the Ethereum blockchain. The proposed method has a few limitations: it employs a computationally and communicatively intensive Bilinear Pairing algorithm. Formal security proof is required to ensure its security and reveal private key attacks. Besides, the proposed solution improves data storage and sharing in decentralized storage systems; it may require additional security guarantees for resource use to be practical. (Alniamy and Taylor, 2020) propose an architecture model to offer greater fine-grained access control over data stored in the cloud. The model integrates the Hyperledger blockchain technology and the ABE scheme. This allows data owners to encrypt shared data and control access through access control policies connected with attributes. However, the authors fail to provide a formal proof.

(Yang et al., 2021), propose a non-interactive access control strategy for the IoT based on blockchain technology and private set instruction (PSI). The proposed strategy allows data holders to store their information on a cloud server and users to access this data by adding attributes as a transaction to the blockchain. A smart contract then executes the PSI protocol to determine whether the characteristics set satisfies the threshold structure, and if it does, the user is granted access to the data. However, the proposed method employs a computationally intensive Bilinear Pairing algorithm, which is not suitable for a resource-limited environment. (Liu et al., 2021), offer a revocable ABAC system for blockchain applications. The design approach allows for attribute-level access control and user revocation. The proposed method employs a resource-intensive Bilinear Pairing algorithm, which necessitates extensive computational and communication resources. (Rouhani et al., 2021), ABAC on blockchain will allow reliable auditing of access attempts. The system's audibility and openness will benefit both parties. With Hyperledger Fabric, the authors claim high efficiency with low computational overhead. However, due to the intensive Bilinear Pairing algorithm, the proposed method consumes a great deal of computational and communication resources. In 2021, (Zaidi et al., 2021) propose a blockchain-based ABAC approach for the IoT. IoT devices can control the user's environment and collect personal data. Smart contracts automate data access, while Proof of Authority improves system performance and reduces gas usage. Data are encrypted and can only be decrypted within a valid access time when using blockchains. Due to the intensive Bilinear Pairing algorithm, the proposed method consumes a great deal of computational and communication resources. (Lu

et al., 2021), propose using ABE with blockchain technologies to regulate IoT data access. Data encryption and ABE algorithms create fine-grained access control while ensuring IoT security. Aside from data hash values, the blockchain currently stores ciphertext location, access control policy, and other critical information in hash values. However, due to the intensive Bilinear Pairing algorithm, the proposed method consumes a great deal of computational and communication resources. There also needs to be explicit security proof for the proposed approach. (Arasi et al., 2022) propose a new data-sharing system combining blockchain technology and ABAC management. The author creates a trustworthy blockchain-based scheme for safe data sharing with integrity audits that maintain data integrity. Due to the intensive Bilinear Pairing algorithm, the proposed method consumes a great deal of computational and communication resources, and the proposed system requires formal security proof. A blockchain-enabled ABAC that maintains confidentiality was proposed by (Zhang et al., 2022) for use in intelligent healthcare systems. The proposed method prevents failure at a single point and lowers the expenses of online operations thanks to online-offline encryption.

(Zhu et al., 2018b), focus on creating a secure resource-sharing platform that leverages the advantages of a decentralized blockchain environment, flexible and diverse permission management, and a verifiable and transparent access mechanism. They propose a transaction-based access control (TBAC) platform that combines the blockchain system and the industry-standard ABAC model. The authors propose a TBAC-related cryptosystem (CryptoTBAC) for secure attribute exchanging and dynamic policy decision-making. (Zhu et al., 2018a), presented a digital asset management platform, DAM-Chain, which utilizes TBAC and combines the benefits of the distribution ABAC paradigm and blockchain technology. The ABAC in the platform offers flexible and decentralized authorization mechanisms for digital asset management on the blockchain. Blockchain transactions serve as a traceable and verifiable method for access requests. (Dukkipati et al., 2018), proposed an ABAC system for the IoT that enables users to access and manage their data. The authors used a blockchain model to create access control measures, but there were privacy concerns and a lack of explicit security evidence. (Ding et al., 2019), introduced a new ABAC approach for IoT systems that leverages blockchain technology to prevent single points of failure and data tampering. Streamlining access control methods and technologies has also enhanced low-power processing efficiency for IoT hardware.

(Jiang, 2021), introduce smart contract-based access control, which eliminates the need for a central trusted server and instead uses the blockchain to complete access authorization. The proposed technique addresses the standard access control strategy’s centralization issue. The scheme contains a security flaw and uses heavy computation and communication resources. (Ghorbel et al., 2021), reveal blockchain-based ABAC and fine-grained access control, which maintains user privacy and accountability. The authors constructed a permission blockchain prototype and ran numerous tests to establish the solution’s scalability, which they presented at the conference. Unfortunately, Due to the intensive Bilinear Pairing algorithm, the proposed method consumes a great deal of computational and communication resources, and the proposed system requires formal security proof.

After conducting a comprehensive study, it has been found that the recommended methods, particularly those using bilinear pairing, have significant computational and communication resource utilization drawbacks. The underlying cryptographic algorithms used in these methods are computationally intensive and result in substantial overheads, making them impractical for many applications. Moreover, despite their popularity, these methods have not been rigorously tested and analyzed for security, and proper formal security proof is lacking. This raises concerns regarding the security of these methods, as they rely heavily on theoretical assumptions and lack empirical evidence to support their claims. As a result, it is essential to conduct more extensive security analysis and testing before these methods can be widely adopted and relied upon. Despite these challenges, developing a secure and efficient scheme is essential for ensuring the privacy and security of digital communications and transactions. As such, continued research and development in this field are critical for advancing the state of the art and addressing the current limitations of existing methods.

### 3 NETWORK MODEL FOR ACCESS CONTROL IN BLOCKCHAIN-ENABLED IOT

We used a lightweight ID-based signature and attributes access policy to provide and fill the access control requirements for IoT using blockchain. Figure 1 presents a network model for secure and well-managed access control in blockchain-enabled IoT. This modal consists of IoT Devices, Users, Blockchain, and Attributes Authority participants.

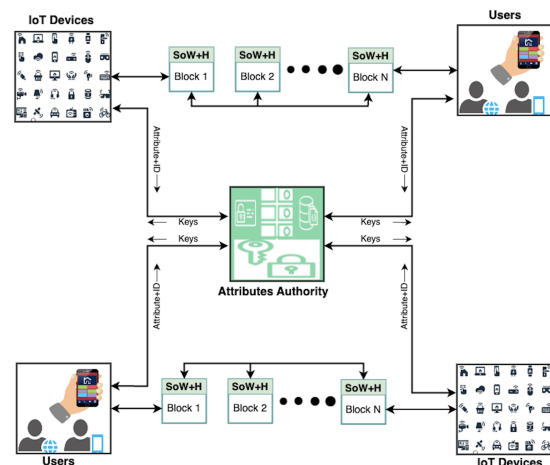


Figure 1: Proposed network modal for access control in blockchain-enabled IoT.

**IoT Device:** The IoT is a network of physical devices equipped with sensors, software, and network connectivity that allow them to gather and exchange data. In the context of a blockchain-enabled IoT (BE-IoT) infrastructure, an IoT device refers to any physical device that is used in IoT applications such as smart healthcare, smart homes, banking, and smart contract trading. These devices can include devices like smart thermostats, cameras, door locks, and many other types of connected devices. These devices provide access and data to users using blockchain technology.

**Users:** Users refer to end-users or devices that want to access and retrieve data from IoT devices. The users can be individuals or organizations looking to access data from IoT devices for various reasons like monitoring, control, and decision-making. These users need to be authenticated and authorized to access the IoT data.

**Blockchain:** In a BE-IoT infrastructure, the data is stored in a combination of blocks containing IoT device requests. Blockchain is a decentralized technology that uses a digital ledger to record and secure transactions between multiple parties. It employs cryptography to ensure the authenticity, integrity, and immutability of the data stored on the ledger. The data are organized in blocks, each containing a set of transactions and a cryptographic hash of the previous block. This structure creates a blockchain that forms the blockchain, making it tamper-resistant.

**Attributes Authority (AA):** An essential aspect of a BE-IoT infrastructure is the Attributes Authority (AA), which is a trustworthy authority that establishes secure access. The AA assigns access attributes and provides participants with a key pair. These attributes can be things like user identification, location, time,

and other information that can be used to make access decisions. The key pair is used to sign and verify data, ensuring only authorized parties can access it. The AA is a critical element in a BE-IoT system, playing a crucial role in maintaining data security and protection. It verifies the attributes and identity of users to ensure that only authorized entities are granted access to IoT device data, preventing any unauthorized access and safeguarding the integrity of the data.

The algorithm sections explain in detail the activities of all participants in the proposed access control scheme.

## 4 THREAT MODEL

In a BE-IoT infrastructure, the main issue that could compromise the system is illegal access to IoT data. Threats in a BE-IoT include actions that compromise data access, integrity, availability, and verification of data owner. Individuals with malicious intent and technical capabilities can exploit these vulnerabilities. Researchers have developed various access control cryptographic schemes to address security and privacy concerns in the open BE-IoT environment. These schemes aim to ensure secure data exchange between peers and prevent adversaries from accessing, retrieving, or tampering with the information. The typical threat model for designing these security solutions is the (Dolev and Yao, 1983), which assumes an insecure public channel and powerful adversaries who can access and receive data through the BE-IoT network. However, this model does not account for the possibility of an attacker guessing random numbers or obtaining access without a valid key. In this work, our proposed access control scheme for BE-IoT is based on the DY threat model and assumes that only the AA is trusted and secure. The scheme leverages digital signatures to verify devices and data sources and grant secure access to end users. The digital signatures-based access control allows for secure verification of devices and data sources, granting secure access to end-users. The proposed scheme aims to provide enhanced security compared to previous solutions while still operating within the constraints of the DY threat model.

To enhance security in the BE-IoT environment with minimal cost, an access control scheme has been proposed. The objective of this scheme is to provide secure access to the users while operating in the BE-IoT where adversaries can access, retrieve, and exchange block data. The scheme is designed to be Existentially Unforgeable and Secure against Attacks on Access Control (UAACA). In this scheme, a game

is played between the adversary ( $AV$ ) and the challenger ( $CA$ ). The  $AV$  inputs the public parameter  $P$ , which has a polynomial running time and tries to win a game with a probability of non-negligibility. The  $CA$ , on the other hand, must respond to the queries made by the  $AV$  in order to play the game. The aim of the game is to ensure that the access control scheme remains secure and prevents unauthorized access to the data and devices in the BE-IoT environment.

- For any participants identity  $ID_u$ , the  $AV$  issues an extraction query  $Q_{ex}$ , and the  $CA$  executes a key generation query using  $ID_u$  as input, obtaining a private key  $PVK_u$ , which is then sent back to the  $AV$  as a response.
- When the  $AV$  receives a Signature Generation Query  $Q_{signature}$ , they provide  $PVK_u$  as input. The  $CA$  then runs the Signature Generation Algorithm using  $PVK_u$  and provides the resulting signature  $Sd$  to the  $AV$ .
- The  $AV$  inputs  $ID'_u$  and user/object attributes or data  $\Pi'$ . It generates  $Z'$  as the signature. The extraction query  $Q_{ex}$  and the signature generation query  $Q_{signature}$  have not been executed previously for  $ID'_u$  and  $\Pi'$ .

## 5 PROPOSED ACCESS CONTROL ALGORITHM FOR BLOCKCHAIN-ENABLED IOT

The following is the detail of the proposed algorithm and its working steps.

*Access Policy and Condition:* Let  $S$  be a set of attributes,  $U$  be a set of users with identities ( $ID_u$ ), and  $\Pi$  be an object or data in our BE-IoT. Every user and object must sign attributes or data ( $Sd$ ). The access will grant according to the following conditions and rules  $R$ .

- Access grants if  $Sd$  verified ( $S \models R$ ).
- Access denied if  $Sd$  verification field ( $S \not\models R$ ).

*Setup for Registration:* The Attribute Authority (AA) executes this phase. The AA takes the parameter of security ( $ps$ ), selects finite field ( $FF$ ) and divisor ( $Dv$ ) of HCC of order  $n$ .

- Choose the master secret key ( $Ms$ ), such that  $Ms \in \{1, 2, 3, \dots, n-1\}$ .
- calculate the master public key ( $Mb$ ),  $Mb = Ms \cdot Dv$ .
- choose hash functions  $H_1, H_2$  of SHA-256 nature.

The AA then publishes  $P = (n, H_1, H_2, Dv, Mb)$  as public parameters set in the blockchain-enabled IoT network and keeps  $(Ms)$  secret with itself.

*Key Generation:* In this step, the IoT devices, and users send the identities (attributes)  $(ID_u)$  to AA. The AA calculates keys for all participants by computing follow steps.

- Calculate private keys for participants  $(PVK_u)$ .
- At the start, the AA pick a number randomly  $Rn \in \{1, 2, 3, \dots, n-1\}$ .
- Compute  $h_1 = H_1(ID_u, Mb)$ .
- Set the  $PVK_u = Rn + h_1 \cdot Ms \pmod n$  where  $PVK_u$  of every participants will be different.
- In the same, the AA calculate public keys  $(PBK_u)$  for participants as  $PBK_u = Rn \cdot Dv$  where  $PBK_u$  of every participants will be different from each other. Then AA set a factor  $FA = h_1 \cdot Mb$ .

After calculations, the AA sends  $(PVK_u, PBK_u)$  to the participants via a secure channel.

*Access:* In this step, the IoT devices, users, or block owner requests to access any data or block addition in IoT networks.

- Grants access if the attribute matches  $S \models R$ .
- Denied access if the attribute does not match  $S \not\models R$ .

The following steps of signature generation and verification will be used to find the validity of IoT devices, and users, in our BE-IoT.

*Signature Generation:* The signature will be applied to validate the user for access, or data sources authentication. This algorithm will be run by IoT devices, a user when requested to access IoT data, IoT data owner for delivering data. It takes an attribute, object, or IoT data as input represented by  $\Pi$ , a nonce  $(Fn)$ ,  $ID_u$ ,  $PVK_u$ ,  $PBK_u$ , and executes the following steps.

- The participant picks a random number  $Rs \in \{1, 2, 3, \dots, n-1\}$  and calculates  $Pn = Rs \cdot Dv$ .
- The participant computes a message digest  $h_2 = H_2(\Pi, Pn, ID_u, Fn)$  where  $ID_u$  and  $h_2$  of every IoT device, users, and IoT Data Owner will be different from each other. Here We use an additional fresh nonce  $(Fn)$  to achieve the goal of revocation.
- The participant generate  $Z = Rs + h_2 \cdot PVK_u \pmod n$

The participant delivers the signed attribute or data  $Sd = ID_u, Z, PVK_u$  to the recipient.

Note: The user will execute this algorithm to request access, and the sender, after access is granted, signs the data.

*Signature Verification:* To find the validation of the user for access, verification of block addition, IoT devices, and data source verification, the applied signature  $(Z)$  will be verified as.

- Compute the digest of a message  $h_2 = H_2(\Pi, Pn, ID_u, Fn)$ .
- Compute  $Z \cdot Dv = Pn + h_2(PBK_u + FA)$

If  $Sd$  is verified it holds  $S \models R$  then access will be granted. Otherwise, denied access according to  $S \not\models R$ .

Note: The sender will execute this algorithm to verify the requested users for access grant, IoT Data Owner for allowing block addition, and receivers to verify the data source.

## 5.1 Consistency of the Proposed Scheme

The following calculations proved the correctness of the designed attribute for access.

$$Z = Rs + h_2 \cdot PVK_u$$

To prove this, we multiply  $Dv$  by both sides;

$$Z \cdot Dv = (Rs + h_2 \cdot PVK_u)Dv$$

Multiply  $Dv$  by both elements of the brackets;

$$Z \cdot Dv = Rs \cdot Dv + (h_2 \cdot PVK_u)Dv$$

As we know  $Rs \cdot Dv = Pn$ , so put the value of  $Rs$ ;

$$Z \cdot Dv = Pn + h_2(PVK_u)Dv$$

Similarly  $PVK_u = PBK_u + h_1 \cdot Mb$ , put the value;

$$Z \cdot Dv = Pn + h_2(PBK_u + h_1 \cdot Mb)$$

Also  $h_1 \cdot Mb = FA$ , so put the value of  $h_1 \cdot Mb$ ;

$$Z \cdot Dv = Pn + h_2(PBK_u + FA)$$

So, the above equations securely calculate the value of  $Z$ .

## 6 DEPLOYMENT AND WORKFLOW OF THE PROPOSED SCHEME

As depicted in Figure 2, our access control scheme is intended to be used in a BE-IoT environment. This scheme aims to allow multiple users to securely access IoT devices while ensuring that only valid users are granted access as per the set Blockchain policies. To achieve this goal with minimal resource consumption, the scheme is designed to operate in the following consecutive steps:

*Access Policy and Condition :* Let  $S$  be a set of attributes,  $U$  set of users with identities  $(ID_u)$ , and  $\Pi$  be objects or data in our BE-IoT. Every user and object must sign attributes or data ( $Sd$ ). Access grants if  $Sd$  verified ( $S \models R$ ). Access denied if  $Sd$  verification field ( $S \not\models R$ ).

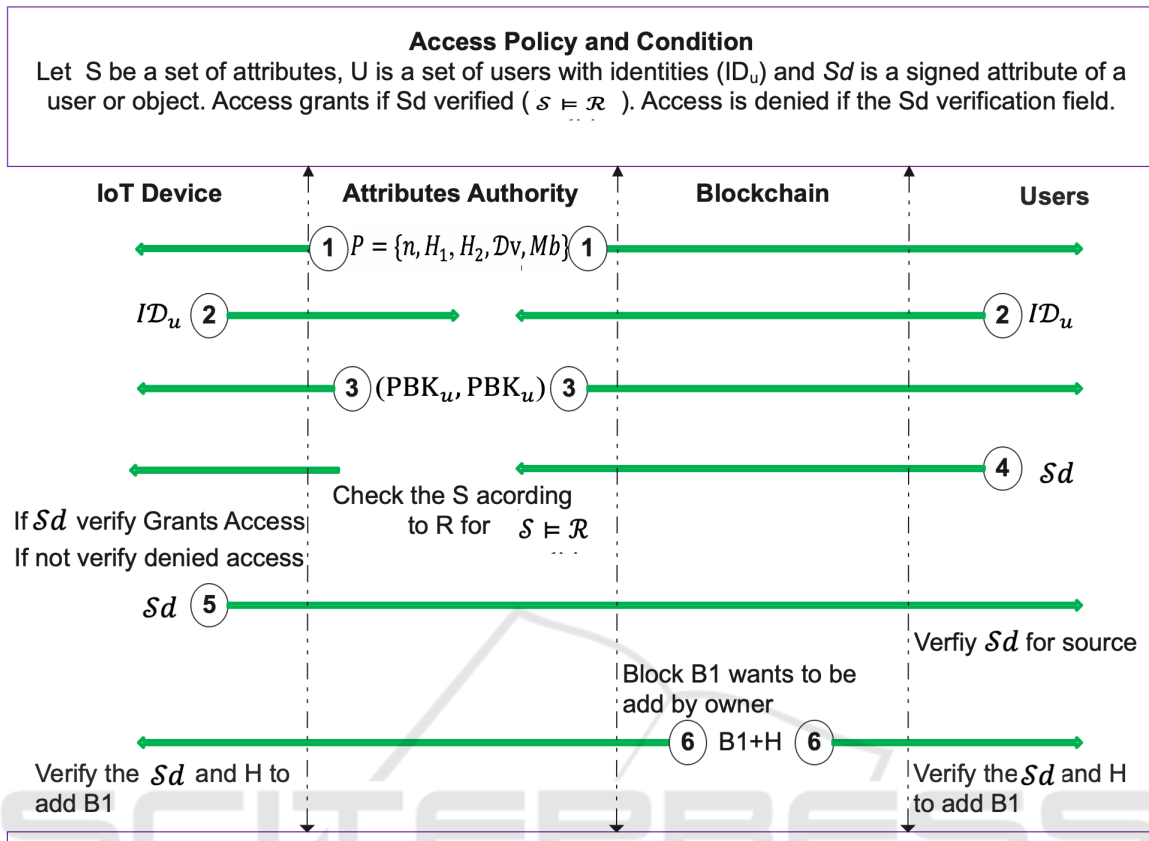


Figure 2: Deployment and workflow of the proposed scheme.

**Setup for Registration and Connectivity:** To connect to the network. First, the Attribute Authority (AA) take the parameter of security ( $ps$ ), selects finite field  $FF$  and divisor  $Dv$  of order  $n$ , chooses master secret key ( $Ms$ ), where  $Ms \in \{1, 2, 3, \dots, n - 1\}$ , calculate the master public key ( $Mb$ ),  $Mb = Ms \cdot Dv$ , and chose hash functions  $H_1, H_2$ . The AA then publishes  $P = (n, H_1, H_2, Dv, Mb)$  as public parameters set in the IoT network publicly and keeps ( $Ms$ ) secret with itself. To connect to the network, the IoT devices and users send the identities (attributes) ( $ID_u$ ) to AA. The AA calculates private keys for participants ( $PVK_u$ ). At the start, the AA pick a number randomly  $Rn \in \{1, 2, 3, \dots, n - 1\}$ , compute  $h_1 = H_1(ID_u, Mb)$ . Then set  $PVK_u = Rn + h_1 \cdot Ms \text{ mod } n$  where  $PVK_u$  of every participant will differ. In the same, the AA calculates public keys ( $PBK_u$ ) for participants as  $PBK_u = Rn \cdot Dv$  where  $PBK_u$  of every participant will be different from each other. Then AA set a factor  $FA = h_1 \cdot Mb$ . After calculations, the AA sends ( $PVK_u, PBK_u$ ) to the participants via a secure channel.

**Request for Access:** Let the user request to access data ( $\Pi$ ). The user will apply a digital signature ( $Z$ ); for that, the user takes the requested data name ( $\Pi$ ), a

fresh nonce ( $Fn$ ),  $ID_u, PVK_u, PBK_u$ . To generate  $Z$ , the user picks a random number  $Rs \in \{1, 2, 3, \dots, n - 1\}$ , calculate  $Pn = Rs \cdot Dv$ , compute data name digest  $h_2 = H_2(\Pi, Pn, ID_u, Fn)$ . The user generates  $Z = Rs + h_2 \cdot PVK_u \text{ mod } n$  and sends an access request. The requested data must include attributes like the thing's name, identity, etc.

**User Verification to Grant or Denied Access:** To validate the user's access, the attributes must be present in  $S$  according to  $R$ , and the applied signature  $Z$  will be verified by computing the digest data name  $h_2 = H_2(\Pi, Pn, ID_u, Fn)$  and computing  $Z \cdot Dv = Pn + h_2(PBK_u + FA)$ . If  $Z$  is verified according to  $R$ , then the conditions  $S \models R$  are satisfied, and access will be granted. Otherwise, access will be denied according to the state  $S \not\models R$ . When access is granted, the IoT devices will apply a digital signature on the requested data  $Sd = ID_u, Z, PVK_u$  using the same signature generation process as explained in the request for access step. The user can verify the signature to validate the data sources of the IoT device.

**Block Verification for Addition:** let the owner want to add a new block. IoT Data Owner will contain signature  $Z$ , and the block will be hash  $h$  and informa-

tion of the last block. Here, the same digital signature process will be applied to generate the signature, and every user and IoT Data Owner will verify the signature using our verification process. If the IoT Data Owner's signature is confirmed, it will be added to the chain. Otherwise, it will remove.

## 7 FORMAL ANALYSIS OF SECURITY

In this section of the paper, we will demonstrate the security of our access control scheme under the assumption of the hardness of the *HCDLP* problem using the Random Oracle Model (ROM). If an attacker/adversary *AV* has non-negligible advantage  $NNA$  and can make at most  $MosT$  queries for hash  $Q_{hash}$ , extraction  $Q_{ex}$ , and signature generation  $Q_{signature}$ , then the security of the scheme is guaranteed against malicious access, unverified data sources, and unverified block additions. The *CA* with an execution time of  $\left(\frac{23(Q_{hash}H_2^5)}{NNA}\right)$  and a probability of  $NNA' \geq \frac{1}{9}$  can solve the *HCDLP* problem if  $\left(NNA \geq \frac{10(Q_{hash}H_2+1)(Q_{hash}H_2+Q_{signature})}{2^{ps}}\right)$  and  $MosT' \leq \left(\frac{23(Q_{hash}H_2^5)}{NNA}\right)$  (Ullah et al., 2020).

*PROOF:* Let  $a$  be such that the *CA* is challenged with an *HCDLP*. Also, the task of the *CA* is to calculate  $Z$  from  $W = Z \cdot Dv$ , where  $Z \in \{1, 2, 3, \dots, n-1\}$ . The *CA* sets  $P = (n, H_1, H_2, Dv, Mb)$  as a set of parameters for the public. The response to the *AV* queries is given below.

1. Queries on  $H_1$ : The *CA* in start maintains an empty list  $H_1^{LS}$  containing the tuples  $(ID_u, PBK_u)$ . If the tuples  $(ID_u, PBK_u)$  exist in  $H_1^{LS}$ , the *CA* returns  $h_1$ ; otherwise, the *CA* chooses a random  $h_1 \in \{1, 2, 3, \dots, n-1\}$  and stores  $(ID_u, PBK_u, h_1)$  in  $H_1^{LS}$  and returns  $h_1$ .
2. Queries on  $H_2$ : The *CA* initially maintains an empty  $H_2^{LS}$  containing the tuples  $(\Pi, Pn, ID_u)$ . If the tuples  $(\Pi, Pn, ID_u)$  exist in  $H_2^{LS}$ , the *CA* returns  $h_2$ ; otherwise, the *CA* selects a number at random  $h_2 \in \{1, 2, 3, \dots, n-1\}$ , stores  $(\Pi, Pn, ID_u)$  in  $H_2^{LS}$ , and returns  $h_2$ .
3. Query on Extraction  $Q_{ex}$ : When *CA* submits a request with  $ID_u$ , then *CA* randomly selects  $x, y \in \{1, 2, 3, \dots, n-1\}$ , sets  $PBK_u = x \cdot Mb + y \cdot Dv$ ,  $PVK_u = x$ , and  $h_1 = (ID_u, PBK_u) = -i \pmod n$ . The tuple  $(PVK_u, PBK_u)$  satisfies the equation  $PVK_u \cdot Dv = Pub_u + FA$  in the key generation algorithm, where  $FA = h_1 \cdot Mb$  and  $h_1 = H_1(ID_u, PBK_u)$ . The *CA* generates  $(PVK_u, PBK_u)$

as the public-private key pair of  $ID_u$  and copies the tuple  $(PVK_u, PBK_u, H_1(ID_u, PBK_u), ID_u)$  in the  $H_1^{LS}$ .

4. Queries on Signature Generation  $Q_{signature}$ : Upon request with  $ID_u$  from the *AV*, *CA* performs the following steps.
  - The  $Q_{signature}$  check determines whether it has been queried for  $ID_u$ . If it has been queried for  $Q_{hash}$  or  $Q_{signature}$ , it retrieves  $(ID_u, PVK_u, PBK_u, H_1(ID_u, FA), ID_u)$  from the list  $H_1^{LS}$ . Then, the Signature Generation process is performed by the *CA*, which produces  $Z$  and inserts it into  $H_2(\Pi, Pn, ID_u)$  within  $H_2^{LS}$ .
  - If it is not asked to perform the  $Q$  Queries on Signature Generation ( $Q_{signature}$ ), then the *CA* processes the specified oracle and retrieves the matching secret key to generate a signature for access.
  - If it is queried, then the *CA* selects two random numbers  $x$  and  $y$  from the set  $1, 2, 3, \dots, n-1$ . It retrieves  $h_1 = H_1(ID_u, PBK_u)$  from  $H_1^{LS}$  and calculates  $Pn = x \cdot Dv - y \cdot PBK_u - y \cdot h_1 \cdot Mb$ . Then, it sets  $x = Z$  and  $h_1 = y$ , and inserts  $(\Pi, Pn, ID_u, y)$  into  $H_2^{LS}$ . If  $(\Pi, Pn, ID_u, y)$  already exists in  $H_2^{LS}$ , the *CA* response is false, and it exits. The failure probability is not more than  $1/n'$  as  $y$  is selected randomly.

When *AV* can produce the same signature for access as described in the Signature Generation procedure by using the function  $\left(\frac{NNA \geq 10(Q_{hash}H_2+1)(Q_{hash}H_2+Q_{signature})}{2^{ps}}\right)$ . It is important to note that if *CA* has not undergone the Signature Generation oracle for access, two valid signatures can be created:  $(\Pi, PBK_u, Pn, h_2, Z)$  and  $(\Pi, PBK'_u, Pn', h'_2, Z')$ .

Thus, verification processes are necessary to grant access or verify data

Firstly,

$$Pn = g(Dv), PBK_u = x \cdot Mb + y \cdot Dv, Mb = Ms \cdot Dv$$

$$Z(Dv) = g \cdot Dv + h_2 \cdot x \cdot sMs \cdot Dv + h_2 \cdot h_1 \cdot Ms \cdot Dv$$

Secondly,

$$Z'(Dv) = g \cdot Dv + h'_2 \cdot x \cdot Ms \cdot Dv + g \cdot Dv = h'_2 \cdot y \cdot Dv + h'_2 \cdot h_1 \cdot Ms \cdot Dv$$

$$Z' \cdot Z \cdot Dv = Z' \cdot g \cdot Dv + Z' \cdot h_2 \cdot x \cdot Ms \cdot Dv + Z' \cdot h_2 \cdot y \cdot Dv + Z' \cdot h_2 \cdot h_1 \cdot Ms \cdot Dv$$

$$Z \cdot Z' \cdot Dv = Z \cdot g \cdot Dv + Z \cdot h'_2 \cdot x \cdot Ms \cdot Dv + Z \cdot h'_2 \cdot y \cdot Dv + Z \cdot h'_2 \cdot h_1 \cdot Ms \cdot Dv$$

So, if we perform the subtraction, then we have  $(Z \cdot -Z' \cdot g + Z \cdot h'_2 \cdot y - Z' \cdot h_2 \cdot y) \cdot (Dv = Z \cdot h'_2 \cdot x - Z' \cdot h_1 \cdot x + Z \cdot \dots \cdot h'_2 \cdot h_1) \cdot Ms \cdot Dv$ .

Then we have  $k = (Z \cdot g - Z' \cdot g + Z \cdot h'_2 \cdot x - Z' \cdot h_1 \cdot x) \pmod n$  and  $(\zeta) \pmod n = (Z \cdot h'_2 \cdot x - Z \cdot h_2 \cdot$



$x + Z \cdot h_2' \cdot h_1)^{-1} \pmod n$ , which is the solution of the *HCDLP* for *CA* with the time  $MosT' \leq \left( \frac{23(Q_{hash}H_2^5)}{NNA} \right)$  and probability  $NNA' \geq \frac{1}{9}$  (Ullah et al., 2020).

## 8 EFFICIENCY ANALYSIS

The goal is to determine how well the scheme performs in terms of its resource requirements. For efficiency analysis, we selected four schemes ((Wang et al., 2018), (Liu et al., 2021), (Zhang et al., 2022), and (Zhu et al., 2018a)) based on their formal proofs and clear cryptographic operations. This analysis is essential because it helps to assess the feasibility of using a particular scheme in a given application and can also be used to compare different schemes and choose the most appropriate one. Some factors that are commonly considered in efficiency analysis include the time and number of bits required for secure access, as well as the size of the keys and ciphertext.

### 8.1 Computation Time

In the ABAC system, the attributes of both users and a resource are embedded in a digital signature, which is then checked to ensure that the attributes are correct and have not been altered in any way. Verifying a digital signature is a computationally expensive process. The more attributes used in a policy, the more signatures must be verified, which drives up the computation cost. The computation cost is also affected by the size of the digital signature and the complexity of the algorithm being used. The computation cost will be increased, for instance, if a larger key size is used for the algorithm that generates digital signatures or a more complex algorithm, such as RSA, is used. Using a more efficient digital signature algorithm, such as the ECC and HCC, which is more efficient than RSA, is one approach to reducing the computation cost in an ABAC system. Similarly, reducing the number of characteristics used in the policies by only utilizing the attributes required to determine who has access to the resources.

The cost of pairing-based point multiplication ( $P_{mp}$ ), bilinear pairing ( $B_p$ ), exponentiation ( $E_{xp}$ ), and Hyperelliptic Curve Divisor Multiplication ( $H_{dm}$ ) are essential parameters in evaluating the performance and efficiency of pairing-based cryptography methods. The authors in (Khan et al., 2020) and (Ullah et al., 2021), report that the cost of one pairing-based point multiplication is 4.31 milliseconds, the cost of a single bilinear pairing is approximately 14.90 milliseconds, the cost of single exponentiation

is approximately 1.25 milliseconds, and the cost of a single *HCDM* is about 0.48 milliseconds. These values are used to measure the performance of the cryptographic algorithm and can be used to compare different methods.

In Table 1, the performance of the designed scheme is compared to previously related access control schemes, such as (Wang et al., 2018), (Liu et al., 2021), (Zhang et al., 2022), and (Zhu et al., 2018a) in terms of the computation time required in milliseconds. Table 1 suggests that our scheme is more efficient than the previously related schemes regarding the time required for cryptographic operations. The designed scheme is evaluated for its performance by comparing the cost of mathematical operations used with the previously related schemes. The performance is measured in terms of time required for the cryptographic operations, and based on the comparison results, the designed scheme is more efficient than the previous ones as shown in Figure 3.

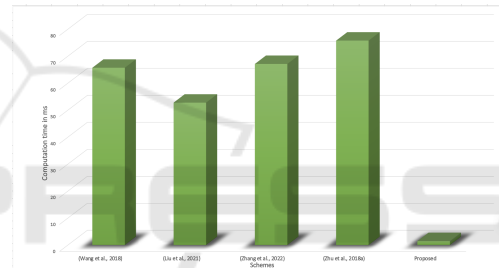


Figure 3: Computation time analysis.

**Concluding Remarks:** We evaluated the performance of various ABAC schemes for IoT using blockchain technology in terms of computation time. The table above summarizes the results of the evaluation, which show that the computation time for the existing schemes evaluated ranges from 65.69 milliseconds to 75.75 milliseconds. In contrast, the computation time for our proposed scheme is significantly lower at 1.44 milliseconds. This indicates that the proposed scheme is more efficient in computation time as it takes less time to perform cryptographic operations. This makes it a more suitable option for real-world IoT applications requiring low computation time and real-time processing, such as applications with many users or real-time data processing.

### 8.2 Communication Overhead

In the context of ABAC, the term "communication overhead" refers to the amount of data that needs to be exchanged between the client, the attribute authority, and the access control decision point to arrive at an access control decision. This must take place be-

Table 1: Computation time analysis.

Ref. No	Costly cryptographic operations	Computation time in milliseconds (ms)
(Wang et al., 2018)	$3E_{xp} + 4P_{mp} + 3B_p$	65.69 ms
(Liu et al., 2021)	$3E_{xp} + 1P_{mp} + 3B_p$	52.76 ms
(Zhang et al., 2022)	$6E_{xp} + 4B_p$	67.1 ms
(Zhu et al., 2018a)	$1E_{xp} + 5B_p$	75.75 ms
Proposed	$3H_{dm}$	1.44 ms

fore an access control decision can be made. The size of the messages exchanged can be measured to determine this, including the size of the attribute query, the size of the attribute response, and the size of the access control decision. Another method for determining the extent of the communication burden caused by ABAC is to count the number of messages passed back and forth between the various entities. Counting the number of attribute queries, the number of attribute responses, and the number of access control decisions made is one way to determine this (Hussain et al., 2020).

In this comparison, the designed approach is being evaluated against some of the previously suggested schemes regarding communication overhead. The proposed scheme is compared with (Wang et al., 2018), (Liu et al., 2021), (Zhang et al., 2022), and (Zhu et al., 2018a). The analysis assumes certain variables such as bilinear pairing ( $G$ ), hyperelliptic curve cryptosystem ( $q$ ), and message ( $m$ ), as shown in Table 1. The results, as shown in Figure 3 and Table 2, indicate that the designed scheme substantially improves communication overhead compared to the previous schemes. The length of the elements in different cryptographic schemes are assumed to be specific values: bilinear pairing ( $G$ ) is assumed to have a length of 1024 bits, message ( $m$ ) is considered to have a length of 512 bits, and Hyperelliptic curve ( $q$ ) is considered to have a length of 80 bits.

The communication overhead for (Wang et al., 2018) scheme is calculated to be  $4|G| + |m|$ , and for (Liu et al., 2021) scheme it is calculated to be  $3|G| + |m|$ , for (Zhang et al., 2022) scheme it is calculated to be  $4|G| + |m|$ , Zhu et al. (Zhu et al., 2018a) scheme is calculated to be  $3|G| + |m|$  and for the proposed is calculated to be  $3|q| + |m|$ . The results, as presented in Figure 4 and Table 2, indicate that the designed scheme significantly improved communication overhead compared to the previous schemes. We suggest that the proposed scheme is a better option than the previous ones based on the comparison regarding communication overhead and cost reduction. *Concluding Remarks:* We have evaluated the communication overhead of several ABAC schemes for IoT using blockchain technology. The results of our analysis are summarized in the table above, which shows

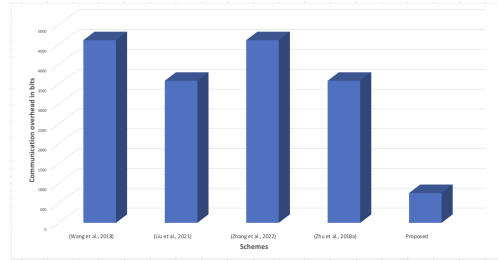


Figure 4: Communication overhead in bits.

the communication overhead in bits for four existing schemes and our proposed scheme. The existing schemes considered in this research are (Wang et al., 2018), (Liu et al., 2021), (Zhang et al., 2022), and (Zhu et al., 2018a). The communication overhead of these schemes ranges from 4608 bits to 3584 bits. It is worth noting that two of the existing schemes, (Wang et al., 2018) and (Zhang et al., 2022), have the same communication overhead of 4608 bits.

On the other hand, our proposed scheme has a communication overhead of 752 bits, which is significantly lower than the existing schemes. This indicates that our proposed scheme is more efficient in terms of communication overhead.

## 9 CONCLUSION AND FUTURE WORK

The Internet of Things (IoT) revolution has created new security challenges, particularly managing access control for connected devices. Traditional methods may not be effective in addressing these challenges. This paper proposes the use of IoT-enabled attribute-based access control (ABAC) using blockchain technology as a solution to this problem. ABAC allows access to be granted or denied based on the attributes of the user or device requesting access rather than relying on a central authority. This allows for more flexible and dynamic access control policies that can adapt to changing situations and minimize the risk of unauthorized access. Blockchain technology provides a secure and transparent way to manage access control information for IoT devices. The authors propose a new lightweight ABAC scheme for

Table 2: Communication overhead analysis.

Ref. No	Costly operations for Communication overhead	Communication overhead in bits
(Wang et al., 2018)	$4 G  +  m $	4608 bits
(Liu et al., 2021)	$3 G  +  m $	3584 bits
(Zhang et al., 2022)	$4 G  +  m $	4608 bits
(Zhu et al., 2018a)	$3 G  +  m $	3584 bits
Proposed	$3 q  +  m $	752 bits

IoT using blockchain technology and conduct a security analysis to evaluate and compare the proposed scheme to existing schemes. The results indicate that the proposed scheme has the advantage of using minimal computation time and communication bandwidth compared to previous solutions. The authors suggest that the ABAC scheme using blockchain combined with a lightweight Hyperelliptic Curve Cryptosystem (HCC) is well suited for secure deployment in IoT.

In the future, we will address the privacy concerns that are raised by the practice of storing access histories on a blockchain. We will look into a more advanced privacy-preserving technique that offers the benefits of blockchain technology without compromising user privacy.

## REFERENCES

Alansari, S., Paci, F., and Sassone, V. (2017). A distributed access control system for cloud federations. pages 2131–2136. IEEE.

Alniamy, A. and Taylor, B. D. (2020). Attribute-based access control of data sharing based on hyperledger blockchain. pages 135–139.

Arasi, V. E., Gandhi, K. I., and Kulothungan, K. (2022). Auditable attribute-based data access control using blockchain in cloud storage. *Journal of Supercomputing*, 2022(1):1–27.

Ding, S., Cao, J., Li, C., Fan, K., and Li, H. (2019). Novel attribute-based access control scheme using blockchain for iot. *IEEE Access*, 7(1):38431–38441.

Dolev, D. and Yao, A. (1983). On the security of public key protocols. *IEEE Trans. Inf. theory*, 29(2):198–208.

Dukkipati, C., Zhang, Y., and Cheng, L. C. (2018). Decentralized, blockchain based access control framework for the heterogeneous internet of things. pages 61–69. ACM.

Ghorbel, A., Ghorbel, M., and Jmaiel, M. (2021). Accountable privacy preserving attribute-based access control for cloud services enforced using blockchain. *International Journal of Information Security*, 2021(1):1–22.

Hu, Vincent, C., Kuhn, D. R., Ferraiolo, D. F., and Voa, J. (2015). Attribute-based access control. *Computer*, 48(2):85–88.

Hussain, S., Ullah, I., Khattak, H., Adnan, M., Kumari, S., Ullah, S. S., Khan, M. A., and Khattak, S. J. (2020). A lightweight and formally secure certificate based

signcryption with proxy re-encryption (cbsre) for internet of things enabled smart grid. *IEEE Access*, 8(1):93230–93248.

Hussain, S., Ullah, I., Khattak, H., Khan, M. A., Chen, C., and Kumari, S. (2021). A lightweight and provable secure identity-based generalized proxy signcryption (ibgps) scheme for industrial internet of things (iiot). *Journal of Information Security and Applications*, 58:102625.

Jiang, X. (2021). Decentralized, blockchain based access control framework for the heterogeneous internet of things. pages 21–23. J. Phys Conf. Ser. 1955.

Khan, M., Rehman, S., Uddin, M., Nisar, S., and Noor, F. (2020). An online-offline certificateless signature scheme for internet of health things. *Journal of Healthcare Engineering*, 2020(1):1–10.

Kumar, S., Tiwari, P., and Zymbler, M. (2019). Internet of things is a revolutionary approach for future technology enhancement: a review. *Journal of Big data*, 6(1):1–21.

Liu, X., Zheng, Y., and Li, X. Z. (2021). A revocable attribute-based access control system using blockchain. *In Journal of Physics: Conference Series*, 1971(1):012058.

Lu, X., Fu, S., Jiang, C., and Lio, P. (2021). A fine-grained iot data access control scheme combining attribute-based encryption and blockchain. *Security and Communication Networks*, 2021:1–13.

Omolara, Esther, A., Alabdulatif, A., Abiodun, I., Alawida, M., and Arshad, H. (2022). The internet of things security: A survey encompassing unexplored areas and new insights. *Computers and Security*, 112(1):102494.

Rouhani, S., Belchior, R., and Cruz, R. S. (2021). Distributed attribute-based access control system using permissioned blockchain. *World Wide Web*, 24(1):617–644.

Sandhu, S. R. and Samarati, P. (1994). Access control: principle and practice. *IEEE communications magazine*, 32(9):40–48.

Sinha, Bahadur, B., and Dhanalakshmi, R. (2022). Recent advancements and challenges of internet of things in smart agriculture: A survey. *Future Generation Computer Systems*, 126(1):169–184.

Swessi, D. and Idoudi, H. (2022). A survey on internet-of-things security: threats and emerging countermeasures. *Wireless Personal Communications*, 124(2):1557–1592.

Ullah, I., Khan, M. A., F.Khan, M.A.Jan, R.Srinivasan, S.Mastorakis, S.Hussain, and Khattak, H. (2021). An efficient and secure multimediasage and multireceiver

- signature scheme for edge-enabled internet of vehicles. *IEEE Internet of Things Journal*, 29(9):2688–2697.
- Ullah, S. S., Ullah, I., Khattak, H., Khan, M., Adnan, M., Hussain, S., Amin, N., and Khattak, M. (2020). A lightweight identity-based signature scheme for mitigation of content poisoning attack in named data networking with internet of things. *IEEE Access*, 8(1):98910–98928.
- Wang, L., Wijesekera, D., and Jajodia, S. (2004). A logic-based framework for attribute based access control. pages 45–55. ACM.
- Wang, S., Zhang, Y., and Zhang, Y. (2018). Blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems. *IEEE Access*, 6(1):38437–38450.
- Yang, Q., Zhang, M., Zhou, Y., Xia, T. W. Z., and Yang, B. (2021). Non-interactive attribute-based access control scheme by blockchain for iot. *Electronics*, 15:1–11.
- Zaidi, S. Y. A., Shah, M. A., Khattak, H. A., Maple, C., Rauf, H. T., El-Sherbeeney, A. M., and El-Meligy, M. A. (2021). An attribute-based access control for iot using blockchain and smart contracts. *Sustainability*, 13(21):10556.
- Zhang, Y., Wei, X., Cao, J., Ning, J., Ying, Z., and Zheng, D. (2022). Blockchain-enabled decentralized attribute-based access control with policy hiding for smart healthcare. *Journal of King Saud University - Computer and Information Sciences*.
- Zhu, Y., Qin, Y., Gan, G., Shuai, Y., and Chu, W. C. C. (2018a). Digital asset management with distributed permission over blockchain and attribute-based access control. pages 535–544. IEEE.
- Zhu, Y., Qin, Y., Zhou, Z., Song, X., Liu, G., and Chu, W. C. C. (2018b). Digital asset management with distributed permission over blockchain and attribute-based access control. pages 193–200. IEEE.