

Efficient and Secure Access Control for IoT-based Environmental Monitoring

Asia Othman Aljahdali

Cybersecurity Department, College of Computer Sciences and Engineering, University of Jeddah, Saudi Arabia

aoaljahdali@uj.edu.sa (corresponding author)

Afnan Habibullah

Cybersecurity Department, College of Computer Sciences and Engineering, University of Jeddah, Saudi Arabia

habibullah.afnan@gmail.com

Huda Aljohani

Cybersecurity Department, College of Computer Sciences and Engineering, University of Jeddah, Saudi Arabia

huda.aljohani@outlook.com

Received: 14 August 2023 | Revised: 27 August 2023 | Accepted: 30 August 2023

Licensed under a CC-BY 4.0 license | Copyright (c) by the authors | DOI: <https://doi.org/10.48084/etasr.6193>

ABSTRACT

Environmental monitoring devices based on IoT collect a large amount of data about the environment and our surroundings. These data are collected and processed before being uploaded to third-party servers and accessed and viewed by ordinary or specialized users. However, they may hold sensitive information that should not be exposed to unauthorized users. Therefore, accessing this sensitive information must be strictly controlled and limited in order to prevent unauthorized access. This research intends to create an access control mechanism based on distributed ledger technologies. The idea is to use a hybrid of IOTA technology and Ciphertext-Policy Attribute-Based Signcryption (CP-ABSC) technology. The permissions to access these data are written in a token, and this token will be sent to the Tangle after being signcrypted with CP-ABSC. Consequently, the data will be safeguarded, their confidentiality and integrity will be maintained, and unauthorized individuals will be unable to access the information. The proposed system was evaluated in terms of performance and the results showed that the system is straightforward, rapid, and convenient to use. Furthermore, a security assessment was conducted by running several scenarios to evaluate its feasibility and protection.

Keywords-*ciphertext-policy; attribute-based signcryption; IOTA; access control; Internet of things (IoT); user authentication; privacy*

I. INTRODUCTION

Intelligent electronic devices are nowadays not limited to smartphones, but ubiquitous. These devices gather and analyze data in order to provide us with detailed information about our surroundings. These devices communicate via the Internet of Things (IoT), which allows information to be transferred between smart devices, analyzed, and displayed as usable information. The number of IoT applications is staggering and covers a wide range of topics, including IoT-based healthcare systems, IoT-based smart industries, IoT-based smart cities, and IoT-based environmental monitoring [1, 2], which will be the focus of the current paper. Environmental monitoring is a critical IoT application that involves monitoring the surrounding environment and reporting the results for effective short-term solutions. It plays a significant role in promoting a

safe quality of life. Nevertheless, to produce accurate data, environmental monitoring necessitates the use of specialized instruments and resources. This sort of information is critical because it assists in the early detection of any potential issues and aids workers and scientists in improving and well-managing the environment [3].

IoT devices typically acquire sensitive and confidential data that must be safeguarded. However, these devices frequently employ sensors that are susceptible to security flaws. One significant security threat is the unauthorized access to IoT data and resources, which might be exploited by a malicious user or utilized for any type of abuse [4]. Furthermore, the collected data by IoT devices are subsequently sent to a cloud or server hosted by a third party. But, since the third party is considered an untrusted entity, the gathered data may be insecure and

disclosed, allowing unauthorized parties to exploit them unlawfully. Therefore, the data must be safeguarded in numerous ways that can be taken into consideration, including restricting access or encryption. Accordingly, an advanced technology that employs Distributed Ledger Technology (DLT) for IoT access control called IOTA was established to implement robust access control to the resources and data acquired by IoT devices. IOTA is an excellent alternative to blockchain since it has overcome the shortcomings of blockchain in terms of throughput and fees, whereby IOTA is a technology with high throughput and no fees, making it an ideal alternative [5]. IOTA's DLT is referred to as the Tangle. A Tangle is an IOTA network of connected nodes. Data recorded in the Tangle in the form of objects are called a "transaction", and once written in the Tangle, they cannot be deleted or modified. In this research, IOTA technology will be combined with Ciphertext-Policy Attribute-Based Signcryption (CP-ABSC) to build a secure and efficient access control that will guarantee confidentiality, authenticity, and integrity by signing and encrypting the token that will contain the access rights as well as the resources and data stored in the cloud, whereby only authorized users will be able to decode this token and get access to the resources.

II. RELATED WORK

Countless studies have been conducted in the fields of DLT and attribute-based access control. Numerous methodologies have been employed to provide solutions for secure access control while preserving data protection, including blockchain [6] and machine learning [7]. The recent research that has been conducted in areas related to IoT will be discussed in this section.

The strategy developed in [8] to cope with the massive volume of data created by IoT devices is a lightweight ABSC (LH-ABSC) technique that combines Ciphertext-Policy Attribute-Based Encryption (CP-ABE) and Key-Policy Attribute-Based Signature (KP-ABS). The authors use a fog-cloud architecture to offload most of the computational overhead, such as signature, verification, and decryption. LH-ABSC has a constant signature size and meets public verification, which is critical for IoT devices. As a result, LH-ABSC provides confidentiality, unforgeability, and verifiability, in addition to selectively chosen-ciphertext security, selectively chosen-message security, and signer anonymity.

Researchers tend to implement blockchain as one of the DLTs to take advantage of its benefits, which include decentralization, auditability, immutability, and consensus. Authors in [7] developed an Intrusion Detection System (IDS) in IoT using machine learning and Blockchain. Authors in [9] suggested an IoT device access control mechanism based on attributes. The approach is done by integrating Blockchain technology with CP-ABE for recording the attribute, preventing data tampering, and avoiding a single point of failure by optimizing the access control process using smart contracts to achieve lightweight authentication while fulfilling the high-efficiency needs of the IoT. The authors employed two types of Blockchain: the public Blockchain which is used for authentication, tagging servers, and storing user-defined

policies, whereas a consortium Blockchain is employed for storage, i.e. the hashes of transactions are kept thereafter, after users and devices have been validated. Although the Blockchain promises security and decentralization, it has scalability and cost issues.

The Blockchain-Based Attribute-Based Signcryption (BABSC) technique for cloud data sharing security was proposed and compared to comparable ABSC schemes in terms of storage and computation costs in [10]. Additionally, the authors integrate the Blockchain idea with attribute-based encryption to offer a safe data-sharing environment in the cloud. The proposed technique addresses the cloud computing security criteria of secrecy and unforgeability. Moreover, performance evaluations and simulation results demonstrate that the proposed technique is more efficient and feasible than others. Electronic health record sharing in the cloud using the Blockchain-Assisted Verifiable Outsourced Attribute-Based Signcryption (BVOABSC) scheme was proposed in [11]. BVOABSC is a secure sharing method that combines CP-ABSC and Blockchain technology. This approach can protect Electronic Health Records' (EHRs') confidentiality, accuracy, and integrity without depending on third parties. The system allows the Cloud Server (CS) to authenticate users' identities while respecting their privacy. Due to ABSC's properties, the proposed approach enables anonymous source authentication of EHRs, ensuring only authorized users submit EHRs, and protecting signers' privacy. It also ensures that the ciphertext size is constant and independent of the characteristics saving bandwidth and storage space in sharing scenarios. Furthermore, the proposed approach uses CS to perform most decryption operations, which reduces the user's computational load. The user may check the partial ciphertext created by CS, hence, the system meets the condition of verifiability. The proposed approach can withstand malevolent physicians and CS hacking of outsourced EHRs. Even if unscrupulous physicians conspire with cloud servers, the Blockchain is unchangeable. Given that most patients have several physicians creating their EHRs, the system adds a timestamp to each doctor, thus, assuring security. The drawbacks of this approach is that the operational process takes time and all physicians must be trained to use the system.

In order to solve the limitations of Blockchains, such as their limited throughput and high transaction fees, IOTA proposes using a new data format for the ledger and a different consensus algorithm. Authors in [12] presented the Decentralized Capability-based Access Control framework based on IOTA (DCACI). In DCACI, the subject sends an access request to an object owner, who assesses the access permissions to grant the subject, based on local authorization policies and issues an access token to the subject. Simultaneously, the owner adds the token to the Tangle, using MAM as the original copy. In the future, whenever the subject needs to get access to an object, an access request will be sent to the owner along with the token. Therefore, to authenticate the legitimacy of the supplied token, the owner compares it to the original on the Tangle. The DCACI system offers privacy and integrity for capability tokens that may be granted, updated, delegated, and revoked by device owners and users using IOTA's MAM technology. Although the proposed approach provides scalable and fine-grained access control for

IoT networks, it has a few shortcomings, including that it necessitates the establishment of a secure communication connection amongst subjects and object owners since requests and tokens are transmitted without being encrypted, making them more vulnerable to being disclosed to malicious or unauthorized individuals. Also, it only allows one-to-one access control, which implies that each subject must have its own token, making token management more difficult for large-scale IoT systems. Moreover, it does not specify how the authorization procedure should be implemented on the owner's side.

To address the above issues, a novel access control framework was proposed in [5]. The authors proposed an integrated scheme that combines IOTA with a hybrid of Capability-Based Access Control (CapBAC) and CP-ABE technology for IoT access control. The CP-ABE encrypts the token that controls access to a resource, and that token is stored in the IOTA Tangle. The authors demonstrated the scheme's viability by utilizing IOTA technology and IoT devices. The approach enables more secure, fine-grained, and scalable access control. It also allows object owners to grant access rights to many topics in a fraction of the time required by the DCACI scheme. The proposed scheme's performance was compared to DCACI's execution time. They also explored the scheme's scalability by incorporating additional regulations. The results reveal that execution time for each operation is related to the number of characteristics involved, and the number of policies has minimal influence on total execution time.

The above-mentioned works are compared in Table I with regard to a set of criteria to guarantee the efficiency and feasibility of the proposed solution. The first criterion is the use of DLT, which is a decentralized database managed by

multiple participants across multiple nodes that is used for recording asset transactions in which the transactions and their details are recorded in multiple places at the same time. The second criterion is the access control strategy, which is a security technique that regulates who sees or uses resources. The security requirement criteria field lists the proposed frameworks' security goals in order to meet their requirements. Then they were compared to the transaction fee criterion, which indicates whether the scheme must pay fees for its transaction process. Since the proposed solution is intended for IoT systems, the developed frameworks are compared to determine whether they are meant for IoT. Finally, each scheme's limitations are demonstrated. Several access control types have been deployed. Hybrid techniques were used in [8] to implement lightweight ABSC. However, their approach lacks confidentiality and integrity. Authors in [9-11], used different attribute-based access control types, such as CP-ABE, ABSC, and CP-ABSC. Their approaches ensure data tampering prevention, secure data sharing, and secure access control. Despite these features, each strategy has its own set of limitations, as shown in Table I. IOTA technology was used with CapBAC in [12] and with a hybrid of CapBAC and CP-ABE in [5]. Both frameworks guarantee fine-grained access control and support scalability, immutability, and fee-free transactions.

After reviewing all of the previously mentioned studies, it was noticed that there is an unfulfilled gap that deals with protecting the confidentiality of the data and its reliability from fraudulent activities, which can be achieved by signing and encrypting before uploading to the cloud, as well as delivering effective and scalable access control while preserving the signer's anonymity. This would be accomplished by combining IOTA and CP-ABSC technologies, which is the contribution of this paper.

TABLE I. CRITICAL ANALYSIS

Ref.	DLT	Access Control Strategy	Security requirements	Transaction Fees	Intended for IoT Systems	Limitations
[8]	Not applicable	ABSC with hybrid access policy (KPABS – CPABE)	Confidentiality. Ciphertext unforgeability. Fine-grained access control. CCA secure and CMA secure.	Not applicable	Yes	Does not ensure data confidentiality and integrity.
[9]	Public and private Blockchain	CP-ABE	Privacy and user authorization. Data tampering prevention and secure data sharing.	Yes	Yes	Suffers from scalability and cost issues.
[10]	Blockchain	ABSC	Secure data sharing over the cloud. Addresses confidentiality and integrity.	Yes	No	Requires improvement in the context of the computational cost of data encryption and authentication.
[11]	Blockchain	CP-ABSC	Data confidentiality, accuracy, and integrity. User authentication.	Yes	No	The operational process is time-consuming. Physicians need to be trained in using the system.
[12]	IOTA	CapBAC	Privacy and integrity for capability tokens. Fine-grained access control.	No	Yes	Required secure communication connection. Utilizes one-to-one access control.
[5]	IOTA	Hybrid of CapBAC and CP-ABE	Distributed, fee-less. Scalable and fine-grained access control.	No	Yes	Does not ensure data integrity and secure data sharing.
Proposed	IOTA	CP-ABSC	Data confidentiality and integrity. Scalable and fine-grained access control. User authentication. Ciphertext unforgeability	No	Yes	

III. PRELIMINARIES

A. IOTA

IOTA was introduced in 2015, deviating substantially from most of the existing cryptocurrencies, exhibiting features like quantum resistance, a ternary system, and replacing the Blockchain approach with a Directed Acyclic Graph (DAG) [13]. IOTA is a name derived from IoT and the word *iota*, which means "extremely small amount." The name was chosen to reflect the aim of IOTA, which is to connect things through microtransactions [14]. It is an innovative type of DLT designed for IoT access control. DLT does not use a central party in data storage. It secures the data into distributed databases without needing a central party to maintain them. An advanced cryptography technique is used to store records and transactions [15]. The Tangle stores transactions as vertices and links them with edges that represent the approval of previous transactions, using cryptographic signatures to secure the data. This technique aids in acquiring high throughput in recording the new incoming data [5]. The characteristics of IOTA are:

Transactions are fee-less since they are miner-free and do not require any involvement from miners [12]. The IOTA Tangle delivers scalability and authenticity as well as high-speed transactions. It is faster and more powerful to process new transactions [18]. IOTA is a decentralized technology [5]. IOTA integrates a data communication protocol called Masked Authentication Messaging (MAM). This protocol uses the Tangle network and provides an ideal solution for access control. The MAM protocol protects the transactions from tampering. It encrypts the messages before adding the transactions to the Tangle [16]. Each MAM transaction has an address that any peer can use to refer to the transaction. MAM transactions issued by the same peer are chronologically connected to establish a channel (i.e. a chain of transactions). A signature of the issuer is also linked to every MAM transaction, allowing subscribers to verify the issuer's validity (authenticated messaging). By subscribing to each other's channels, peers can safely share data across the Tangle using MAM [4].

B. Ciphertext-Policy Attribute-Based Signcryption (CP-ABSC)

Access control refers to the process of restricting access to only authorized parties in order to get access to a certain resource [12]. Access policies specify who may access what resources. Attribute-Based Access Control (ABAC) is a type of dynamic, fine-grained, and flexible access control in which attribute authorities give identities or responsibilities to a group of attributes, thereby avoiding the need to construct separate access control lists for each entity in the system. It successfully simplifies access control since there are fewer characteristics compared to the number of users in the system. ABE was first introduced in [7]. It is a vision and extension of public-key encryption that enables users to encrypt and decrypt data depending on user attributes. ABE is a crucial tool for tackling the issue of secure data sharing and access control. ABE is a significant improvement over traditional public key cryptography because it achieves flexible one-to-many encryption rather than one-to-one encryption, in which

ciphertexts encrypt a specific user. Users' private keys and ciphertexts, on the other hand, will be associated with a set of characteristics or policies that govern them. If a match exists between the user's private key and the ciphertext, the user would indeed decrypt the ciphertext. ABE is categorized into two categories [18]: Key-Policy ABE (KP-ABE) [4] and CP-ABE [18, 19]. The KP-ABE links the access policies to users' private keys while using attribute sets to annotate ciphertexts. On the other hand, in CP-ABE, each ciphertext is associated with an access policy, and each user's private key is associated with an attribute set, therefore, it is considered an ideal choice for data owners who want to control who can decipher their data [8].

Attribute-Based Signatures (ABS) was proposed in [20] as a new type of digital signature. ABS is a cryptographic primitive that enables a signing entity to generate a signature with fine-grained control over identifying information. A valid ABS signature certifies that a particular user, for whom attributes stratify the predicate, attested the message without exposing further information [21]. Therefore, it anonymously provides message authenticity, which implies that colluding parties are not able to pool their attributes together. The concept of Attribute-Based Signcryption (ABSC) [22] merges the features of encryption and signature in a single phase, generating an effective approach to achieving security requirements including authentication, data confidentiality, data integrity, and non-repudiation. Additionally, it has a lower computational cost as compared to the traditional signature strategy than encryption strategies. ABSC consists of four algorithms [10], as follows:

- **Setup:** It is configured by a Trusted Authority (TA) who generates a master secret key (msk) and public parameters (pk) using a security parameter (k). The user will receive the (pk). However, the (msk) will be kept private.
- **Keygen:** this algorithm generates the private key (Sk), and the verification key (Vk) based on the user's attributes set (S) and the input (msk) (S).
- **Signcrypt:** is run by the administrator and takes two inputs: plaintext (M) and private key (Sk) to output the ciphertext (CT).
- **Designcrypt:** is run by the users. It takes the (Sk), the (CT), and (S) as inputs to produce (M).

In this paper, an efficient and flexible approach termed as Ciphertext Policy Attribute-Based Signcryption (CP-ABSC) will be used to accomplish fine-grained access control, confidentiality, authenticity, unforgeability, and sender privacy concurrently.

IV. THE PROPOSED SCHEME

Protecting data from unauthorized access is critical in preventing unlawful access to information and resources and safeguarding them from any attack in order to obtain the trust of the concerned parties and guarantee that their data are secure from any breaches. As a suggested solution to this issue, a scheme is proposed that develops a mechanism that offers

efficient and secure access control. It employs IOTA technology in conjunction with CP-ABSC technology to provide a protected access control scheme with finer granularity, flexibility, and scalability. More precisely, the proposed approach uses CP-ABSC to sign and encrypt access rights before recording them in the IOTA Tangle. Furthermore, the data will be encrypted before being uploaded to the cloud server, ensuring that they are secure from any security breaches. Additionally, it is ensured that the user is authorized to access the data by properly determining the CP-ABSC policies. Therefore, the proposed scheme can achieve fine-grained access control and implement the principle of least privilege. As demonstrated in Figure 1, which simplifies how the proposed system works, it has two types of users, the data owner, and the data user. The data owner is anyone who owns environmental monitoring data, whether it is a government agency or an individual who wants to monitor the environment around him, whether indoors or outdoors, while a data user is anyone who wants to view and access this data.

- The data owner can define the policies and access permissions that must be followed when accessing the data in the form of a small object named token, which can then be signcryptured using CP-ABSC and be sent to the Tangle.
- The data user can submit a request for access to the data along with the appropriate token (after fetching it from the Tangle) to demonstrate that he is authorized to access that data.

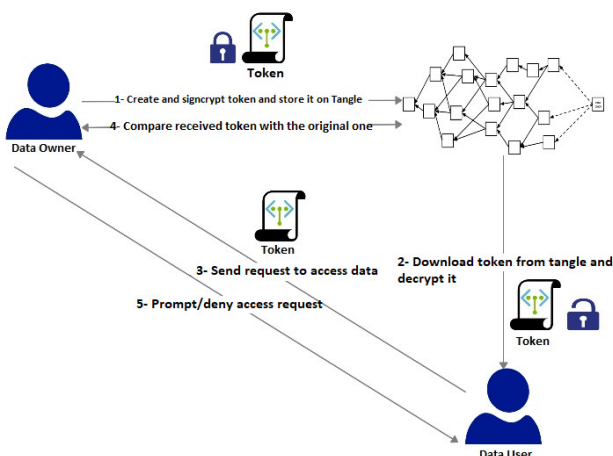


Fig. 1. The proposed scheme.

A. Token Structure

In the proposed system, Tangle is used to store tokens after being signcryptured using CP-ABSC, which contains an attribute set that encompasses the policies and access permissions that the user must meet in order to access the data. A token is a JavaScript Object Notation (JSON) object issued by data owners that contains an identifier (ID), the issuer's name, the policy, and the access rights. The token will be fetched from the Tangle by those who meet these attributes and have the decryption keys, and anyone else will not be able to download or use it. Figure 2 shows an example of a token that will be

available to those with the role of staff who want to access air quality data.

```

token #1:{
  ID: 1938484234
  Issuer: Afnan Hussein
  Policy: role: staff
  Access rights:
    [
      Type of data: Air Quality
      action : read/write
    ]
}

```

Fig. 2. Token example.

B. System Functions

The proposed system intends to assist the data owner in preserving the integrity and reliability of his information and restricting the access to them, ensuring that only authorized data users have access to it. The functions of the proposed system are briefly described below:

- User Identification (Login): users must enter a valid login credential to enroll in the system, otherwise, an error message will be displayed.
- Generation and Protection of Access Tokens: The data owner creates tokens and associates them with the data that contain the permissions required for access. Then, CP-ABSC will be used to signcrypt the token before storing it in the Tangle.
- Retrieval and Decryption of Access Token: The data user can obtain the token from the Tangle and decrypt it before sending a request to access the data. If the data user is authorized to download the token from the Tangle, then he can easily decrypt and view the token for the selected date.
- Send Access Request: The data user sends an access request along with the downloaded token to the data owner to ensure its authorization to access the data.
- Access Requests Validation: The data owner compares the received token to the original one stored in the Tangle and prompts the user if they match. Otherwise, he denies access.

V. SYSTEM IMPLEMENTATION

A web-based application named Management of Environmental Monitoring Data was developed that has a flexible, simple, and convenient user interface, while making the process of preserving and maintaining access to the data smoother. To develop the proposed system, an HP laptop was used with the following characteristics: Windows 11 Home Edition, 16GB RAM, Intel Core i7 10th generation processor. The Laravel framework was used to build and design the web application using the model-view-controller architectural pattern, along with MetaMask, which is a software cryptocurrency wallet, used to send the data to the Tangle through the interaction between the web application and the smart contract, as well as Remix for writing, compiling, and debugging the solidity code of the smart contract (that is used

to store the data that will be sent to the Tangle). Additionally, the IOTA-EVM network was used for setting up an IOTA network in order to send data transactions. When the data are sent from the web application to the Tangle, their transactions can be shown using <https://explorer.wasp.sc.iota.org/>. The proposed scheme aims to protect the resources' integrity and reliability while also restricting access to them. Therefore, the user must enter valid login information using the email address and password they used to register for IoT-based environmental monitoring devices in order to log in to the system, as shown in Figure 3. If the user enters his credentials correctly, the system will redirect him to his dashboard, otherwise, it will display an error message. There are two types of users: data owners and data users, and the information displayed on the dashboard will differ depending on the type of user. The data owner's dashboard gives him access to all the downloaded environmental data from the cloud and provides capabilities for accessing requests and creating tokens. On the other hand, the data user is able to view the data that he has previously been granted access to, as well as send new requests to data owners for access to other types of environmental data.

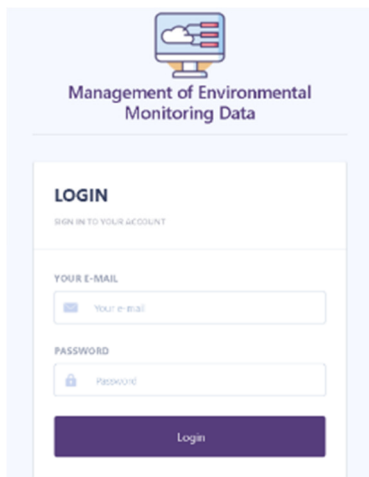


Fig. 3. Login page.

A. Generation and Protection of the Access Token

During the token generation step, the data owner will create tokens and link them to the data, which contain the policy and permission required for access. As illustrated in Figure 4, the token will determine the data type, such as air quality, humidity, and temperature. Additionally, it specifies the user role, indicating whether the user is a staff member or an ordinary user, and the permission type, indicating whether the user has read-only, write-only, or read-and-write access rights. The data owner then signcrypts the token with CP-ABSC and stores it in the Tangle via a MetaMask connection.

B. Retrieval and Decryption of the Access Token

As displayed in Figure 5, before sending a request for access to the data, the data user must first obtain a token from the Tangle and decrypt it with his own key. Since the proposed system employs CP-ABSC, only authorized users who match the policies that the data owner specified during the token generation step can download the tokens.

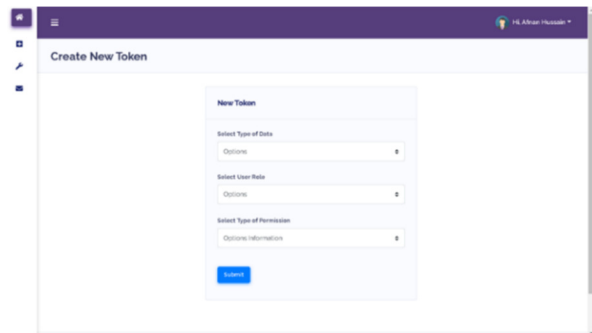


Fig. 4. Token creation page.

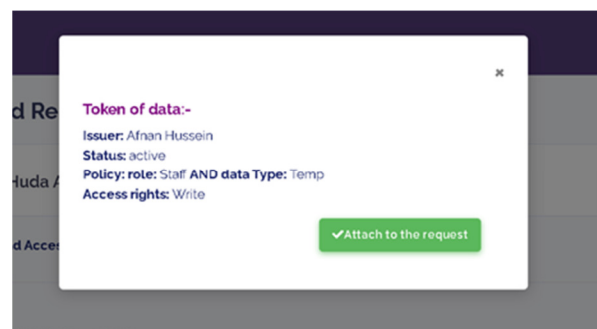


Fig. 5. Fetched token details.

C. Send Access Request

The data user can gain access to the data by submitting a request to the data owner requesting authorization and clearly stating the type of data he desires to view and the action he seeks to take with that data, as shown in Figure 6. More importantly, the appropriate token should be attached to this request, which has been downloaded during the Retrieval of the Access Token step.

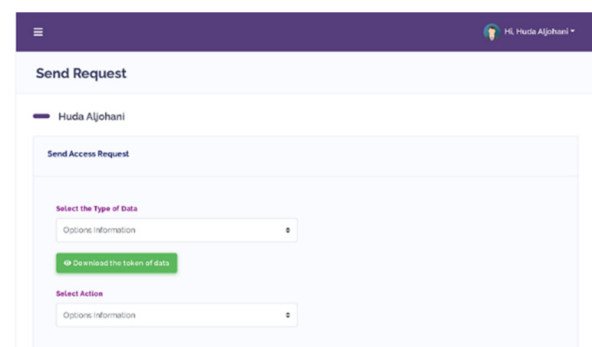


Fig. 6. Sending request page.

D. Access Request Validation

The data owner can view the upcoming users' access requests, examine the request's details (the request details should include the user information such as name and role), and verify the attached token against the original one. Consequently, upon these details, the request will be approved or denied by the data owner as presented in Figure 7.

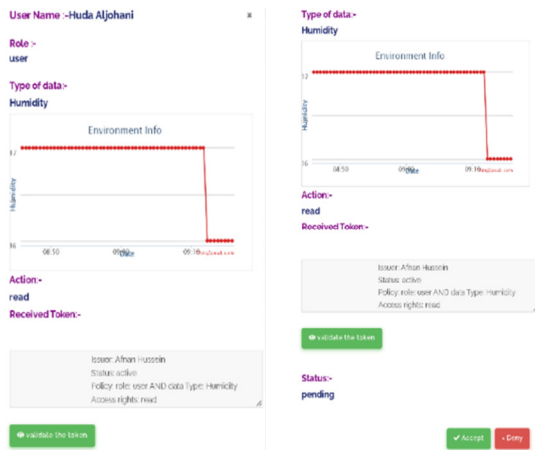


Fig. 7. Access request details.

As demonstrated in Figure 8, by pressing the validate token button, the token attached to the request is compared to the original one stored in the Tangle. If they match, a suitable message will be displayed, allowing the data owner to approve the request. However, if the token has been altered or counterfeited, it will be known due to the Tangle’s immutability, resulting in a message stating that they are incompatible, as shown in Figure 9. As a result, the request will be denied by the data owner.

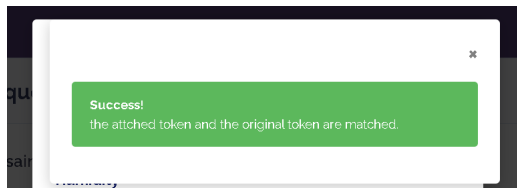


Fig. 8. Token matched.

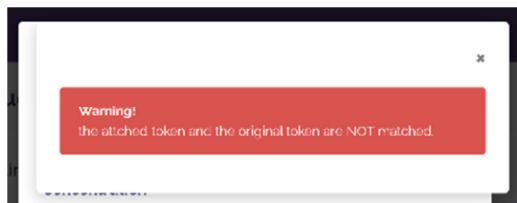


Fig. 9. Token not matched.

VI. PERFORMANCE RESULTS

In this section, the proposed system was evaluated for throughput performance in terms of execution time. Different target users were selected to use and assess the system. For easier evaluation, the tasks were divided for each user and the amount of time it takes for the user to accomplish each task was recorded, as illustrated in Table II (the time indicated is the maximum time that can be used to complete these tasks, with the age of the user affecting these values). For performing the testing tasks, there are two users: a data owner who is in charge of environmental data, setting privileges, creating tokens, maintaining, and managing account requests, and the data user, who accesses the system through login and uses tokens in order to gain access to the data.

TABLE II. SYSTEM PERFORMANCE BASED ON USER TASKS

User	Tasks	Time (s)	Details
Data owner - Data user	Login	15-30	<ul style="list-style-type: none"> • Login • View data
Data owner	Create and store token in the Tangle	20-50	<ul style="list-style-type: none"> • Create token • Fill out the form • Submit the form • Verify token details before sending to Tangle • Signcrypt and save to Tangle
	View request list	25-40	<ul style="list-style-type: none"> • Choose request list • Click on any received request • View details • Verify the received token with the original one • Accept (or deny) the request
Data user	Send request	15-30	<ul style="list-style-type: none"> • Send a request • Fill out the form • Download the token and view its details • Attach it with the request • Submit form

Figure 10 represents how much time each user spends during the system testing process. Figure 10 represents the time spent while executing the functions of the data owner. Time is represented in seconds (s) through the login step, creating and storing the token, and viewing the request list. The time through the login step was between 15 and 25 s, during creating and storing the token it was between 20 and 30 s and during the execution of the view request list step, it was between 25 and 35 s. Figure 11 shows the data user’s execution time through the login process and sending requests for accessing data. The executed time was approximately 20 s during the login step whereas it was between 15–20 s during the sending request.

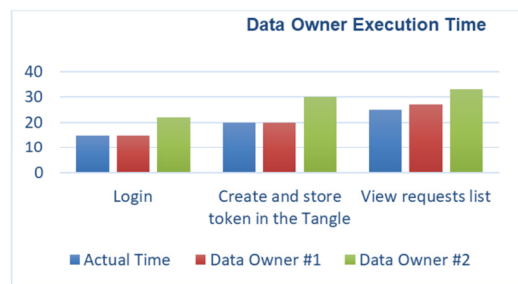


Fig. 10. Data owner execution time.

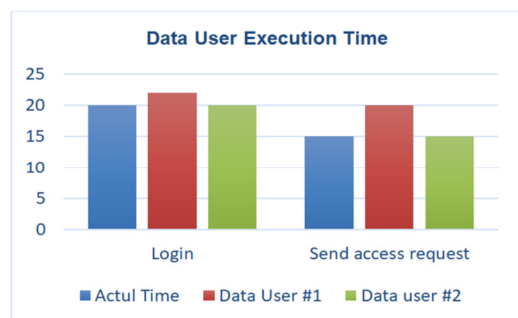


Fig. 11. Data user execution time.

VII. SECURITY EVALUATION

In order to ensure that the proposed scheme achieves security, confidentiality, and fine-grained access control, several test cases were created to evaluate the system’s security against these scenarios. The token is used in the proposed system to define the policies and permissions that the data user must satisfy in order to ensure that he is authorized to access the data. Therefore, anyone who does not meet these attribute sets will be unable to download the token from the Tangle and, as a result, will be unable to use it to send a request for data access. However, attackers may attempt to commit fraud in order to obtain the token. Various test cases were run on the proposed system to ensure that it meets the security requirements of the token, and the outcomes are displayed in Tables III-VI.

TABLE III. TEST CASE #1

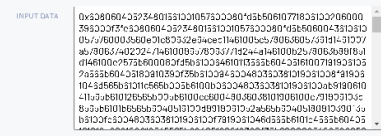
Test Case #1	Create and store tokens in the Tangle.
Description	The data owner creates the token and signcrypts it before sending it to the Tangle. Additionally, to store data through Metamask to the Tangle, they must be converted from text to hexadecimal.
Outcome	The token in the proposed system will be signencrypted using CP-ABSC before being converted to hexadecimal, making it completely secure and non-falsifiable.
Result	

TABLE IV. TEST CASE #2

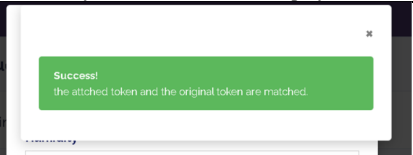
Test Case #2	The data user sends a valid token.
Description	The case of a valid user who is able to decrypt the token and send it with a request to access data.
Outcome	The attached token will be compared to the original one stored in the Tangle. If they match, a message stating that they are identical will be displayed.
Result	

TABLE V. TEST CASE #3

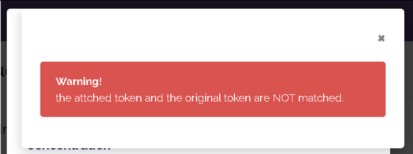
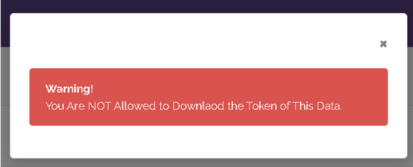
Test Case#3	A data user/attacker sends an invalid token.
Description	Whenever an invalid token is sent, it has been modified by a data user with malicious intent or by an attacker who stole another valid user’s information.
Outcome	If the token has been forged or altered after being downloaded and decrypted from the Tangle, the changes made to the token will be discovered since the Tangle is not subject to change. Therefore, after comparison to the original one, a message will be displayed to clarify that the tokens do not match.
Result	

TABLE VI. TEST CASE #4

Test Case #4	An attacker or ineligible user seeks to obtain a token.
Description	An attacker or an unauthorized user attempts to obtain the token from the Tangle in order to gain access to the data.
Outcome	The use of CP-ABSC technology on the token prevents unauthorized individuals from accessing the token because it can be fetched by those legitimate users who meet the attribute set written in the token and have the decryption keys. Thus, illegitimate attempts to access the token will be detected, and a warning message will appear.
Result	

It was demonstrated in the previous test cases that the proposed system is secure, it protects users’ information and preserves data confidentiality by maintaining the token’s security while also preserving the anonymity of the signer’s identity. The key to its success is IOTA technology and CP-ABSC technology.

VIII. CONCLUSION

The number of devices deployed in IoT systems is growing exponentially. Some of these devices conduct environmental monitoring. As the industrial and infrastructure frameworks have grown rapidly, environmental monitoring has become more important. Because IoT systems frequently handle sensitive data, proper access control is essential to prevent unauthorized access. Numerous studies have been carried out to create ways to protect these data while simultaneously guaranteeing user authorization. These studies have combined various kinds of ABSC with Blockchain and IOTA to implement various sorts of access control. Nevertheless, their approaches suffer from several shortcomings, such as scalability and cost difficulties, failing to guarantee confidentiality, integrity, and secure sharing of the data. IOTA and CP-ABSC were integrated into the proposed system to cover this issue. The proposed system uses the CP-ABSC to sign and encrypt the access privileges before storing them in the IOTA Tangle. Additionally, the data will be encrypted before being sent to the cloud server, ensuring protection against breaches. Moreover, the correct CP-ABSC policies are determined to ensure that the user has appropriate permissions to access the resources. The integrity and confidentiality of the data and resources collected by IoT devices are preserved by employing the above approach, which creates a more secure, granular, and scalable access control system.

REFERENCES

[1] S. Zafar, G. Miraj, R. Baloch, D. Murtaza, and K. Arshad, "An IoT Based Real-Time Environmental Monitoring System Using Arduino and Cloud Service," *Engineering, Technology & Applied Science Research*, vol. 8, no. 4, pp. 3238–3242, Aug. 2018, <https://doi.org/10.48084/etasr.2144>.

[2] Y. B. Zikria, R. Ali, M. K. Afzal, and S. W. Kim, "Next-Generation Internet of Things (IoT): Opportunities, Challenges, and Solutions," *Sensors*, vol. 21, no. 4, Jan. 2021, Art. no. 1174, <https://doi.org/10.3390/s21041174>.

- [3] A. N. Chaudhari and G. A. Kulkarni, "IOT based environmental pollution monitoring system," *International Research Journal of Engineering and Technology*, vol. 4, no. 6, pp. 1823–1829, Jun. 2017.
- [4] R. Nakanishi, Y. Zhang, M. Sasabe, and S. Kasahara, "IOTA-Based Access Control Framework for the Internet of Things," in *2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*, Paris, France, Sep. 2020, pp. 87–95, <https://doi.org/10.1109/BRAINS49436.2020.9223293>.
- [5] Y. Zhang, R. Nakanishi, M. Sasabe, and S. Kasahara, "Combining IOTA and Attribute-Based Encryption for Access Control in the Internet of Things," *Sensors*, vol. 21, no. 15, Jan. 2021, Art. no. 5053, <https://doi.org/10.3390/s21155053>.
- [6] G. Lin, Y. Xia, C. Ying, and Z. Sun, "F2P-ABS: A Fast and Secure Attribute-Based Signature for Mobile Platforms," *Security and Communication Networks*, vol. 2019, Dec. 2019, Art. no. e5380710, <https://doi.org/10.1155/2019/5380710>.
- [7] N. A. Alsharif, S. Mishra, and M. Alshehri, "IDS in IoT using Machine Learning and Blockchain," *Engineering, Technology & Applied Science Research*, vol. 13, no. 4, pp. 11197–11203, Aug. 2023, <https://doi.org/10.48084/etasr.5992>.
- [8] J. Yu, S. Liu, S. Wang, Y. Xiao, and B. Yan, "LH-ABSC: A Lightweight Hybrid Attribute-Based Signcryption Scheme for Cloud-Fog-Assisted IoT," *IEEE Internet of Things Journal*, vol. 7, no. 9, pp. 7949–7966, Sep. 2020, <https://doi.org/10.1109/JIOT.2020.2992288>.
- [9] S. Y. A. Zaidi *et al.*, "An Attribute-Based Access Control for IoT Using Blockchain and Smart Contracts," *Sustainability*, vol. 13, no. 19, Jan. 2021, Art. no. 10556, <https://doi.org/10.3390/su131910556>.
- [10] N. Eltayieb, R. Elhabob, A. Hassan, and F. Li, "A blockchain-based attribute-based signcryption scheme to secure data sharing in the cloud," *Journal of Systems Architecture*, vol. 102, Jan. 2020, Art. no. 101653, <https://doi.org/10.1016/j.sysarc.2019.101653>.
- [11] X. Yang, T. Li, W. Xi, A. Chen, and C. Wang, "A Blockchain-Assisted Verifiable Outsourced Attribute-Based Signcryption Scheme for EHRs Sharing in the Cloud," *IEEE Access*, vol. 8, pp. 170713–170731, 2020, <https://doi.org/10.1109/ACCESS.2020.3025060>.
- [12] S. K. Pinjala and K. M. Sivalingam, "DCACI: A Decentralized Lightweight Capability Based Access Control Framework using IOTA for Internet of Things," in *2019 IEEE 5th World Forum on Internet of Things (WF-IoT)*, Limerick, Ireland, Apr. 2019, pp. 13–18, <https://doi.org/10.1109/WF-IoT.2019.8767356>.
- [13] O. Lamtzidis and J. Gialelis, "An IOTA Based Distributed Sensor Node System," in *2018 IEEE Globecom Workshops (GC Wkshps)*, Abu Dhabi, United Arab Emirates, Sep. 2018, <https://doi.org/10.1109/GLOCOMW.2018.8644153>.
- [14] "What does IOTA stand for?," *Quora*. <https://www.quora.com/What-does-IOTA-stand-for>.
- [15] M. M. Akhtar, M. Z. Khan, M. A. Ahad, A. Noorwali, D. R. Rizvi, and C. Chakraborty, "Distributed ledger technology based robust access control and real-time synchronization for consumer electronics," *PeerJ Computer Science*, vol. 7, Jun. 2021, Art. no. e566, <https://doi.org/10.7717/peerj-cs.566>.
- [16] P. C. Bartolomeu, E. Vieira, and J. Ferreira, "IOTA Feasibility and Perspectives for Enabling Vehicular Applications," in *2018 IEEE Globecom Workshops (GC Wkshps)*, Abu Dhabi, United Arab Emirates, Sep. 2018, <https://doi.org/10.1109/GLOCOMW.2018.8644201>.
- [17] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proceedings of the 13th ACM conference on Computer and communications security*, New York, NY, USA, Jul. 2006, pp. 89–98, <https://doi.org/10.1145/1180405.1180418>.
- [18] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," in *2007 IEEE Symposium on Security and Privacy (SP '07)*, Berkeley, CA, USA, Feb. 2007, pp. 321–334, <https://doi.org/10.1109/SP.2007.11>.
- [19] A. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, "Fully Secure Functional Encryption: Attribute-Based Encryption and (Hierarchical) Inner Product Encryption," in *Advances in Cryptology – EUROCRYPT 2010*, 2010, pp. 62–91, https://doi.org/10.1007/978-3-642-13190-5_4.
- [20] H. K. Maji, M. Prabhakaran, and M. Rosulek, "Attribute-Based Signatures," in *Topics in Cryptology – CT-RSA 2011*, 2011, pp. 376–392, https://doi.org/10.1007/978-3-642-19074-2_24.
- [21] G. Lin, Y. Xia, C. Ying, and Z. Sun, "F2P-ABS: A Fast and Secure Attribute-Based Signature for Mobile Platforms," *Security and Communication Networks*, vol. 2019, Dec. 2019, Art. no. e5380710, <https://doi.org/10.1155/2019/5380710>.
- [22] Y. Zheng, "Digital signcryption or how to achieve $\text{cost}(\text{signature} \& \text{encryption}) \ll \text{cost}(\text{signature}) + \text{cost}(\text{encryption})$," in *Advances in Cryptology – CRYPTO '97*, 1997, pp. 165–179, <https://doi.org/10.1007/BFb0052234>.