Spring 2024

Towards Robust IoT Security: A Blockchain Design with Attribute-based Encryption

Bryan Ikei
Dakota State University

Hanna Thiry
Dakota State University

Shengjie Xu
San Diego State University

Towards Robust IoT Security: A Blockchain Design with Attribute-based Encryption

Bryan Ikei[1], Hanna Thiry[1], and Shengjie Xu[2]

[1] The Beacom College of Computer and Cyber Sciences, Dakota State University, Madison SD 57042, USA
[2] Department of Management Information Systems, San Diego State University, San Diego CA 92182, USA

Abstract. Internet of Things (IoT) data and devices face significant security concerns. It is well-known that IoT security standards and frameworks have yet to be established due to variations with IoT developers and manufacturers agreeing on fundamental design methods to address IoT security and its limited computational resources. This research aims to determine how security standards and frameworks can be better implemented to enhance IoT security. Specifically, this research investigates whether implementing an encryption scheme such as attribute-based encryption (ABE) along with blockchain, a distributed ledger technology (DLT), strengthens the security of IoT data and devices. In this context, an encryption scheme is applied at the IoT gateway on sensor data while implementing blockchain for non-repudiation of data as it traverses the network infrastructure. Finally, we present a performance analysis to assess our proposed solution and validate the performance of ciphertext-policy attribute-based encryption (CP-ABE) based on the number of attributes used in the access policy.

Keywords: Internet of things, attribute-based encryption, blockchain, distributed ledger technology, ciphertext-policy, public-key encryption

1 Introduction

Advancements in Internet-connected computing devices have increased the popularity and demand for Internet of Things (IoT) applications. This growing need for connected computing devices and the increasing demand for IoT solutions have led to the realization of security and privacy concerns across the Internet and in Internet Protocol (IP) networks [1–3]. Many connected IoT devices adhere to no security standards as a fundamental design tenet for IoT security. Furthermore, IoT devices are vulnerable to fundamental security and privacy issues because of their limited computational resources and memory/storage constraints, which prevent the use of efficient and robust encryption techniques to counter security threats [4].

This paper analyzes and evaluates the current and prospective capabilities of using an effective encryption scheme, namely attribute-based encryption (ABE),

along with blockchain, to safeguard the security and trust of IoT data and devices. This research study highlights two critical applications where cryptosystem technologies are helping to secure and provide reliable data transmitted to and from IoT devices.

One such application is blockchain. A blockchain framework is one technique that has become a popular potential solution for solving security and privacy concerns in IoT [5]. Blockchain is a technology that enables the ability to compute and distribute ledgers to record transactions over a network securely. Once the transactions are updated on the blockchain, the data is verified and cannot be altered. The advantage of blockchain is that it is a decentralized Peer-to-Peer (P2P) secure architecture that supports integrity and non-repudiation of IoT data. However, confidentiality and privacy of the data and devices are not fully protected by the blockchain framework alone [6, 7].

Another application, but an essential aspect of data security, is ABE. An encryption technique should be used along with the blockchain framework to address security and trust concerns for IoT data and devices. Owing to computational and storage restrictions, IoT requires an efficient, privacy-preserving encryption scheme that can scale in a distributed network. ABE is an effective encryption technique that delivers access control through a single encryption, thus leveraging the constraints of IoT devices [8].

Current research and evaluation suggest that utilizing an efficient, privacy-preserving encryption scheme and applying distributed ledger technology (DLT) will not only be a possible solution for IoT security but will also support adequate access control of IoT data and devices [9, 10].

In this research study, we evaluate the effectiveness of an ABE scheme in a blockchain framework to provide security and trust of IoT devices. Hence, the primary goal of our study is to determine whether IoT network traffic is encrypted from end-to-end (sensor to end-user), ensuring confidentiality of sensitive data, and investigate the importance of encryption as a method to protect the sensitive content of IoT data while in transit.

The rest of this paper is organized as follows: Section 2 covers previous work on the development and employment of ABE, blockchain, and the combination of both, ABE and blockchain, applied towards IoT security. Section 3 provides the cryptographic background for the basis of our work. Next, an IoT threat model is described in Section 4. An overview of the CP-ABE encryption scheme, the phases required to encrypt/decrypt data, and the addition of the blockchain framework are provided in Section 5. Our proposed solution and evaluation are presented in Sections 6 and 7 followed by concluding remarks in Section 8.

2 Related Work

In this section, we focus on previous papers that inspired this work and on papers related to blockchain technology, effective encryption techniques, and IoT security and privacy. The critical issues and challenges of IoT security and privacy were highlighted in [11]. Of note was the threat of data transit attacks in multi-

ple layers of an IoT system, including the perception layer (physical IoT sensors) and the communication layer (Wi-Fi, LTE, etc.). The literature also highlights the limited hardware and software resources available to the devices within an IoT system, thus requiring effective, privacy-preserving security measures.

2.1 Attribute-based Encryption (ABE)

Functional encryption (FE) lays the groundwork for ABE, a special case of FE. Known as a type of public-key encryption (PKE), Boneh et al. in [12] state that in an FE system, the decryption key is associated with a function of the encrypted data. Decrypting an encrypted message using the secret key associated with a function results in the evaluation of the function, *f(x)*, guaranteeing one cannot learn any more about *x*. This concept leads to the realization and expansion of a special type of FE called ABE [11, pp. 4-5]. As Micciancio notes,

> Attribute-based encryption (ABE) corresponds to functions indexed by a predicate P such that *f[P] (x,m) = (x,m)* if *P(x)* is true, and *f[P] (x,m)* $= x$ if *P(x)* is false. Here, x is interpreted as a set of attributes, and P is a policy that specifies under what conditions on the attributes a message can be decrypted [13].

ABE, like FE, is a type of PKE where multiple users' private keys and ciphertexts are related to a set of attributes, thus making decryption possible only by ensuring that the set of attributes of the user's keys and ciphertext match. Two known implementations of ABE are key-policy attribute-based encryption (KP-ABE) and ciphertext-policy attribute-based encryption (CP-ABE). According to Boneh et al., in a KP-ABE system, "the key provides an access formula that operates over a set of $\boldsymbol{n}$ attributes that must evaluate to true for decryption to yield the message $\boldsymbol{m}$" [12, p. 5]. Essentially, the user's secret keys are created based on the policy for access control of the user, i.e., attributes, based on the set of attributes the data is encrypted. However, Boneh et al. state that the roles are reversed for a CP-ABE system where the ciphertext provides the access formula to encrypt data. At the same time, the user's secret keys are created based on the set of attributes, i.e., the policy for access control [12].

An application of ABE can be observed through the work of [14], where J. Li et al. focus on securing access and storage of cloud-based IoT systems to ensure user data security and privacy. This idea is accomplished using an attribute-based encryption technique that allows access control of encrypted IoT data in the cloud. Their study describes the implementation of ciphertext-policy hiding the CP-ABE scheme to ensure privacy and accountability for their proposed security model in a CloudIoT. The authors further test the traceability of the ABE scheme for accountability to detect malicious activities such as user and authorization center key abuse. The two levels of traceability are level one or Whitebox and level two or Blackbox traceability. The study emphasizes a Whitebox traceability model and proposes future work using a Blackbox model where the decryption key and algorithm are unknown or hidden, then the traceability

algorithm attempts to detect malicious activities such as user and authorization center key abuse.

In another study, M. Ali et al. proposed a lightweight revocable hierarchical ABE (LW-RHABE) for IoT [15]. The study's primary focus is the protection of user privacy by applying an encryption scheme with minimal overhead on existing constrained IoT resources along with efficient, flexible key delegation and user revocation. The authors designed a lightweight cryptosystem for encryption and decryption by placing computational operations in the cloud server. The advantage of this is that during the encryption phase, the cloud server has no knowledge of any information about the underlying data file. Like the encryption phase, sensitive users' data and secret keys are not leaked during decryption since the cloud server performs the computational operations during the decryption phase. They also achieved flexible access control since the proposed encryption scheme supports access trees as the access control policy to determine the access rights of the data users [15, p. 2].

2.2 Blockchain Technology

The limitations of using blockchain in cybersecurity and IoT are discussed in [16–18]. One issue that needs to be addressed is that blockchain results in a broader attack surface. Since blockchain is a decentralized framework whose nodes store a complete copy of all data, an attacker has more options to access data. Other common points in this literature are the need to consider access control and key management problems in cryptographic algorithms used. Our work considers these limitations and proposes a model that addresses these issues.

In [19], the authors proposed IoTChain, a scheme that utilizes the security advantages of blockchain, AES encryption, and smart contracts to solve security and privacy issues in IoT systems. The scheme uses IPFS as the blockchain technology to store the ciphertext of the AES-encrypted sensor data. Authorized users, determined by a smart contract, can obtain the decryption key and access the content in the IPFS system. However, this technique has restrictions when providing data confidentiality due to the use of a symmetric key algorithm. Symmetric key algorithms require the decryption key to be shared along with the data. Our work aims to use ABE to achieve access control and address the constraints of symmetric key encryption algorithms.

In [20], Li and Sato consider using blockchains to protect the privacy of consumer data stored in the cloud. They propose a model where blockchain provides data integrity and auditability due to its transparency and immutability. Due to blockchain's limited capabilities to share data securely and concerns over conventional access control methods to the shared data, the authors combine CP-ABE and blockchain to address those issues. This proposal allows for a fully decentralized storage and sharing solution while ensuring the security and trust of users' data.

The previous studies noted above primarily focus on IoT data at rest as opposed to data in motion. Applying the ABE scheme either with or without blockchain while IoT data is stored in the cloud protects the sensitive data,

thereby addressing the concerns for IoT data security. However, it does not consider IoT data in transit/motion.

2.3 ABE Techniques used in conjunction with blockchain

In [21], Q. Wen et al. propose a model based on a supply chain system where privacy and security are achieved through blockchain, an ABE scheme, and an industrial IoT environment. In this model, due to the many entities involved with a supply chain system, concerns over tampering with cargo data during the process of circulation have been one of the major challenges for supply chain management. Nonetheless, fine-grained access control to the cargo data is accomplished using CP-ABE since ciphertext-policy attributes are associated with the entities involved in the supply chain. Furthermore, blockchain allows seamless transactions between the supply chain entities without needing third-party validation, thus ensuring trusted and tamper-proof transactions.

The work in [22], K. O. Obour Agyekum et al. presented research similar to [21]. However, instead of using CP-ABE, the authors use KP-ABE as the data are encrypted by a set of attributes, and the users' private keys are associated with the access structure of KP-ABE. Thus, if the attribute of the encrypted data satisfies the access structure of the user's private key, decryption of the ciphertext can occur" [22, p. 5]. Future work in this model will focus on computational efficiency.

In another study on the security and privacy of IoT data using ABE and blockchain, Y. Rahulamathavan et al. propose using the "ABE technique to address the privacy and confidentiality of the data shared in blockchain-based IoT ecosystems" [23, p. 1]. Here, the authors model the encryption of sensitive users' data using ABE, where the attributes are based on each user's access control. When used with blockchain, the miners must have the correct attributes to perform blockchain transactions. In this model, the attributes are used to decrypt (ABE) and verify the transaction (BC) of the IoT data.

For this study, we selected an ABE method, a FE scheme derived from PKE, and the use of DLT or, in this case, a blockchain framework. The advantages of using ABE for IoT data follow [8, 9, 12]:

- ✓ it is effective and efficient, so computing and storing should not place a heavy burden on resource-constrained IoT devices,
- ✓ it is based on the PKE method where encryption and decryption are based on access policies while access control is based on the user's attributes,
- ✓ it is flexible and scalable, and
- ✓ rather than encrypting/decrypting a device to a single user, it allows for single-device encryption followed by decryption from multiple users with the correct access policies and user attributes.

The addition of applying a blockchain framework improves the integrity of IoT data through its anti-tamper and strong security aspects, which prevents unknowingly third-party access. Combining these two technologies should provide confidentiality and privacy for IoT data either at rest or in transit.

3 Preliminaries

M. Ali et al. [15] states, "For an algorithm A, assume that $O \leftarrow A\ (I)$ denotes running A on input I and outputting O. Also, for an attribute set S, let $x \leftarrow S$ denote the random selection of x form S. In the following, we give some cryptographic background related to our work."

3.1 Cryptographic Background

M. Ali et al. describe the cryptographic background for bilinear maps as follows:

> **Bilinear map**: Consider a prime number q and two cyclic groups G_1 and G_2 of order q. We say that a function $\hat{e} : G_1 \times G_1 \rightarrow G_2$ is a bilinear map if the following conditions hold:
> - **Bilinearity:** $\hat{e}(g^a, g^b) = \hat{e}(g^b, g^a) = \hat{e}(g, g)^{ab}$, for each $a, b \in \mathbb{Z}_q$ and $g \in G_1$.
> - **Non-degeneracy:** There is a $g \in G_1$ such that $\hat{e}(g, g) \neq 1$.
> - **Computability:** There is an efficient algorithm computing $\hat{e}(g, h)$, for any $g, h \in G_1$.
>
> Consider a probabilisitc polynomial time (PPT) algorithm $\mathscr{G}$ that $(\lambda, q, G_1, G_2, \hat{e}) \leftarrow \mathscr{G}(1^\lambda)$, where λ is the security parameter of the system and $(q, G_1, G_2, \hat{e})$ is the same as above.
>
> In this work, we consider the Decisional Bilinear Diffie Hellman (DBDH) assumption on $\mathscr{G}$:
>
> **The DBDH assumption:** Consider $g \leftarrow G_1, \alpha, \beta, \gamma \leftarrow \mathbb{Z}_q, and$ $(\lambda, q, G_1, G_2, \hat{e}) \leftarrow \mathscr{G}(1^n)$. This assumption states that for all PPT adversaries $\mathscr{A}$, there is a negligible function *negl* such that:
>
> $$\begin{aligned} &|Pr(\mathscr{A}(n, q, g, g^\alpha, g^\beta, g^\gamma, g^{\alpha\beta\gamma}, G_1, G_2, \hat{e}) = 1) \\ &- Pr(\mathscr{A}(n, q, g, g^\alpha, g^\beta, g^\gamma, g^z, G_1, G_2, \hat{e}) = 1)| \leq negl(\lambda) \end{aligned} \tag{1}$$
>
> where the probabilities are taken over the selection of $g \in G_1$ and $\alpha, \beta, \gamma, z \in \mathbb{Z}_q$, and the randomness used in $\mathscr{G}$ and $\mathscr{A}$ [12, p. 5].

3.2 Access Trees

Next, the authors in [15] formally define the access structure for attribute-based encryption schemes.

> In an access tree, leaf nodes represent an attribute set, and inner nodes represent a threshold value set. Also, the threshold value associated with each leaf node is equal to 1. Assume that $\mathscr{T}$ is an access tree, v_a denotes the leaf node corresponding to an attribute a, k_v denotes the threshold value associated with a node v, $R_\mathscr{T}$ denotes root node $\mathscr{T}$, $L_\mathscr{T}$ denotes the leaf node set of the access tree, and $\mathscr{T}_v$ denotes the subtree of $\mathscr{T}$ rooted at a node v.

Let $\mathbb{U}$ be the universal attribute set, and $\mathscr{T}$ be an access tree. For a node v in $\mathscr{T}$, consider a function $F_{\mathscr{T}_v} : 2^{\mathbb{U}} \to \{0,1\}$ perform as follows:

- When v is the leaf node corresponding to an attribute a, $F_{\mathscr{T}_v}(Att) = 1$ if and only if $a \in Att$.
- When v is an inner node with threshold value k_v, $F_{\mathscr{T}_v}(Att) = 1$ if and only if v has at least k_v children $c_1, ..., c_{k_v}$ such that $F_{\mathscr{T}_{c_i}}(Att) = 1$, for $i = 1, ..., k_v$.

We say that an attribute set Att satisfies $\mathscr{T}$ if $F_{\mathscr{T}_{R_\mathscr{T}}}(Att) = 1$.

For a prime number q and an access tree $\mathscr{T}$, consider an algorithm $\{q_v(0)\}_{v \in L_\mathscr{T}} \leftarrow \mathbf{Share}_q(\mathscr{T}, r)$ that shares a secret $r \in \mathbb{Z}_q$ with respect to q and $\mathscr{T}$ as follows:

- Assign a $(k_{r_\mathscr{T}} - 1)$-degree polynomial $q_{R_\mathscr{T}}$ to root node $R_\mathscr{T}$ such that $q_{R_\mathscr{T}}(0) = r$, and other coefficients are selected uniformly at random from $\mathbb{Z}_q$.
- For each non-leaf node v with a polynomial q_v, if children of v have not got their polynomials yet, assign a $(k_{c_i} - 1)$-degree plynomial q_{c_i} to the i-th child such that $q_{c_i}(0) = q_v(i)$, and other coefficients of q_{c_i} are selected uniformly at random from $\mathbb{Z}_q$.

When this algorithm stops, a value $q_{v_i}(0)$ is assigned to the leaf node v_i [15, p. 5].

3.3 A Chain of Blocks

Blockchain technology, a form of distributed ledger technology (DLT), structures data in a chain of blocks, each block containing the hash value from the previous block. The sequence of blocks forms a chain beginning with a *genesis block* and ending with the current block. This structured distributed database allows for [24]:

1. **Greater data transparency** - all data transactions are viewable by others in the network.
2. **Enhanced security** - the blockchain is immutable, i.e., data remains unchanged.
3. **Traceability and auditability of data** - the transactions are recorded in a ledger made available to peers in the network.
4. **Decentralized control** - no single control or authority of the data and transactions, all peers in the network collectively control the blockchain.

4 IoT Threat Model

Fig. 1 depicts the IoT threat model. Using a five-layer model representing the IoT architectural framework, we can align the threat modeling method, STRIDE, to the five layers [25]. The layers from IoT sensor to end-user are as follows:

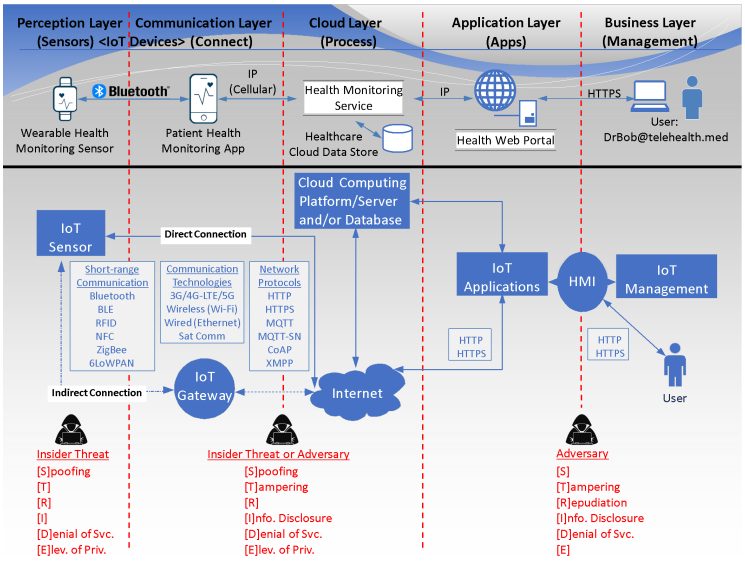

Fig. 1. IoT Threat Model.Source: Adapted from [25, 26].

– Perception Layer (Sensors) - the physical layer where sensors and actuators interact with the physical environment. Kalla et al. [25, p. 5] state "key responsibilities include data acquisition, processing the state information associated with smart objects, and transmitting the raw data or processed information to the upper layers."

– Communication (Connect) & Cloud (Process) Layers - these two layers combine to make up the network layer where data transmission and information processing occur. The primary responsibilities are transmitting sensor data through integrating heterogeneous and disparate networks and storing, processing, and analyzing data received from the communication layer [25, pp. 5-6].

– Application Layer (Apps) - this layer is responsible for the essential messaging services between the IoT devices and end-users. Application layer protocols bridge the gap between the end-users and IoT applications [25, p. 6].

– Business Layer (Management) - according to A. Kalla et al., "this layer manages the overall IoT system" [25, p. 6]. In other words, its primary functions are to manage and control IoT applications, business models, and, to a certain extent, user privacy [26].

5 The Scheme

In this section, we provide the scheme of our system and show how CP-ABE and blockchain technology are used to provide confidentiality and privacy for IoT data and devices.

5.1 Ciphertext-Policy Attribute-based Encryption

According to J. Bethencourt et al. [27], a "ciphertext-policy attribute-based encryption scheme consists of four fundamental algorithms:"

1. *Setup*
   Input: *none*.
   Output: system parameters, a public key PK, and a master secret key MK for use with $Key\_Gen()$, $Encrypt()$, and $Decrypt()$.
2. $Key\_Gen(MK, S_{\{att\}}) \rightarrow SK$
   Input: master secret key MK and a set of attributes $S_{\{att\}}$ that describe the key.
   Output: private key SK.
3. $Encrypt(PK, M, \mathbb{A}) \rightarrow CT$
   Input: public key PK, a message M, and an access policy $\mathbb{A}$.
   Process: encrypt M using the public key PK and the access policy $\mathbb{A}$ expressed in terms of attributes $S_{\{att\}}$.
   Output: ciphertext CT.
4. $Decrypt(PK, CT, SK) \rightarrow M$
   Input: public key PK, ciphertext CT containing the access policy $\mathbb{A}$, and a private key SK containing a set of attributes $S_{\{att\}}$.
   Process: decrypt CT if the set of attributes $S_{\{att\}}$ matches the content of the access policy $\mathbb{A}$.
   Output: a message M.

In CP-ABE, the ciphertexts provide the access structure to encrypt data, and the user's private keys are created based on the set of attributes [12].

5.2 Blockchain Design with Attribute-based Encryption

Following data encryption, the IoT gateway processes the encrypted data and places it in the blockchain's ledger. The authors in [29] implement their model using a permissioned blockchain such as Hyperledger's blockchain implementation. In Fig. 2, we depict the high-level overview of the blockchain transactions containing ABE-IoT data for our implementation.

Finally, expanding upon the blockchain framework, Fig. 3 shows the overall scheme of our system.

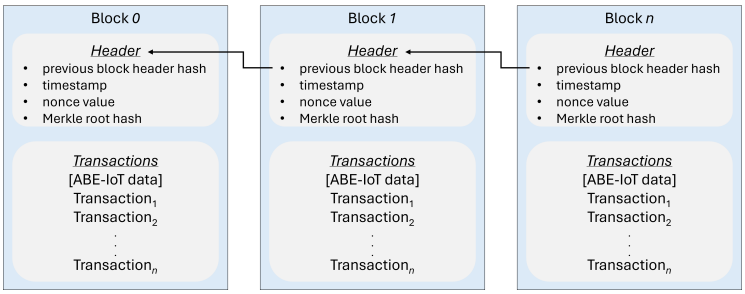

Fig. 2. Blockchain Transactions containing ABE-IoT Data.

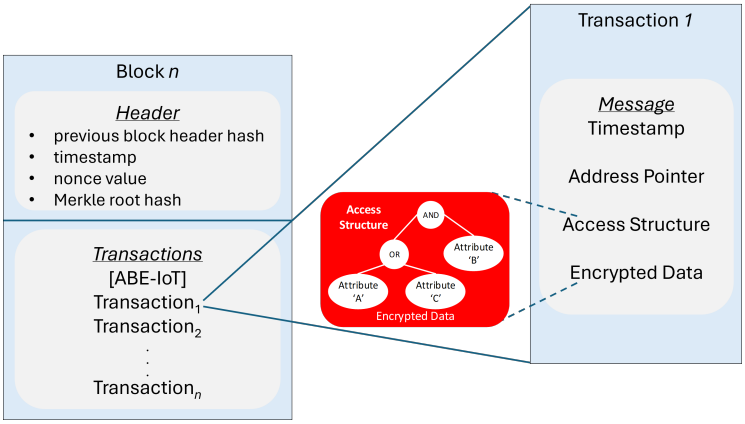

Fig. 3. Access Structure and Encrypted Data within a block transaction.

5.3 UML Sequence Diagrams

Fig. 4, phases 1 and 2, depicts the sequence for the *Setup* algorithm where system parameters, a public key PK, and a master secret key MK are prepared for use in $Key\_Gen()$, $Encrypt()$, and $Decrypt()$.

Fig. 5, phases 3 and 4, depicts the sequences required for the Key_Gen, *Encrypt*, and *Decrypt* algorithms. Additionally, the blockchain framework UML sequences are shown in the gray box. Once the ciphertext is created using CP-ABE, it is placed in the blockchain where the data is recorded as a transaction and contains access structure, encrypted data, and a digital signature.

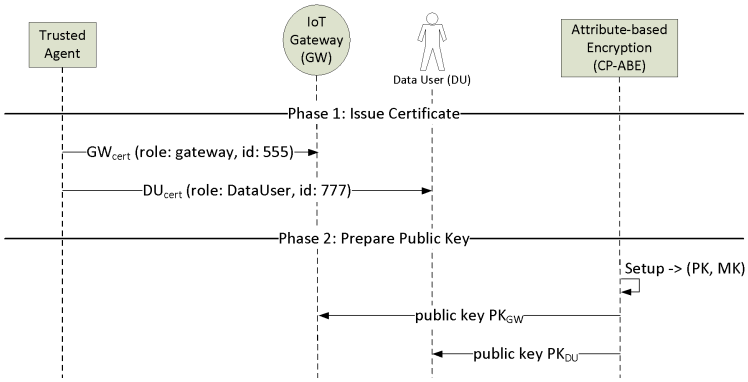

Fig. 4. UML Sequence Diagram for Phases 1 & 2. Source: Adapted from [28].

6 Proposed Solution

This research proposes a novel Blockchain-IoT system where we apply an effective ABE scheme to the IoT devices and then use blockchain-connected IoT gateways (blockchain-enabled IoT with ABE) to provide a certain level of security for data in transit.

The key to achieving confidentiality and privacy of sensitive data depends on whether IoT network traffic is encrypted from end-to-end (sensor to end-user, e.g., data owner or data user) while investigating the value of encryption to protect the sensitive contents of IoT devices. If encrypting IoT sensor data, the use of an effective ABE technique will provide encryption of sensitive users' data based on attributes for fine-grained access control to the data however, if using blockchain for trust and verification, distributed ledger technology (DLT) will create and maintain transactional log data per blocks in the chain. Since IoT data is encrypted using ABE, the preferred use of federated blockchain networks enables faster transactional throughput at a higher level of confidentiality, i.e., faster and more secure IoT data in transit.

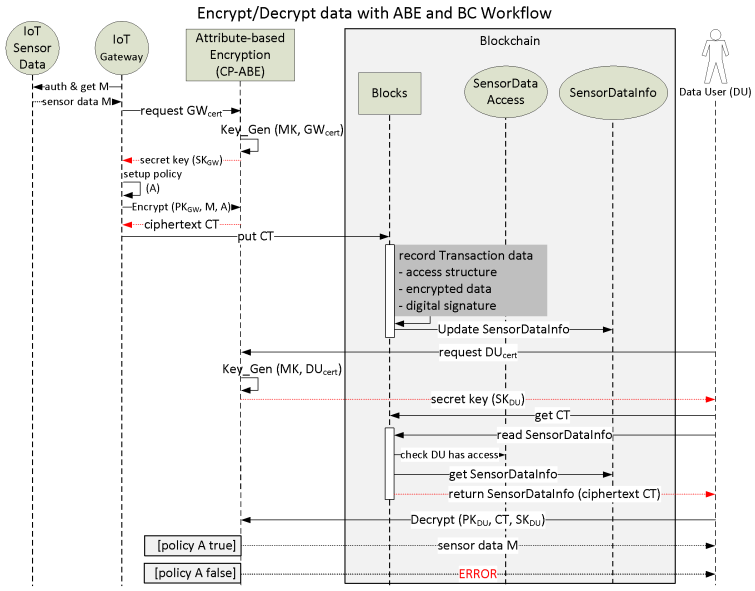

Fig. 5. UML Sequence Diagram for Phases 3 & 4. Source: Adapted from [28, 29].

The basis of this study relies on an encryption scheme that does not consume the already limited resources of IoT devices while ensuring that the encrypted data traverses the network securely. According to the authors in [23], the latter is accomplished using blockchain. The security advantages of incorporating a blockchain framework with ABE-IoT data and devices follow [5, 7, 10]:

1. (Verification) IoT sensor data is verified by the blockchain miners for legitimacy prior to accepting it in the chain.
2. (Tamper-proof) Once accepted and added to the distributed ledger, it is impossible to tamper with the data.
3. (Trust) Blockchain is a P2P decentralized secure architecture that supports integrity and non-repudiation of IoT data.

The idea is to aggregate IoT sensor data at the gateway where ABE is applied prior to entering the blockchain network. Fig. 6 illustrates a ciphertext-policy attribute-based encryption (CP-ABE) model that is applied to IoT sensor data at the gateway. Each user has a secret key and applies it to the encrypted data, shown to the right of the objects (Users). If the user's attributes match, decryption occurs. Otherwise, there is no access to the data. In this example, User C has a secret key and the associated set of attributes to decrypt the data.

Applying the above ABE model to the blockchain framework allows for reliable, trustworthy, and verifiable transactions of IoT data. In Fig. 7, we expand the security architecture to depict how incorporating blockchain enables the ability to compute and distribute ledgers that securely record transactions over a

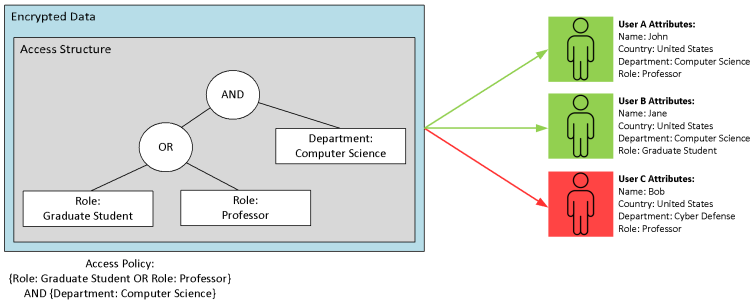

Fig. 6. Ciphertext-policy attribute-base encryption (CP-ABE) model.

network [20,30]. As previously stated, once the transactions are updated on the blockchain, the data in the blockchain is verified and cannot be altered.

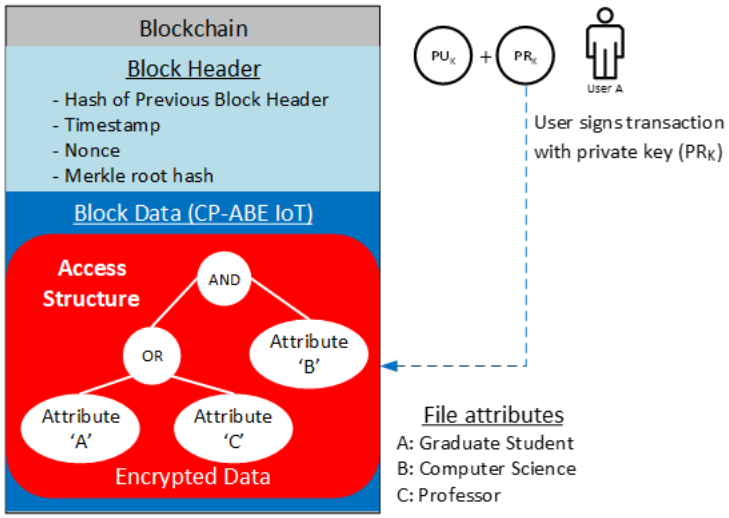

Fig. 7. Blockchain Transaction Data containing the encrypted data model.

7 Performance Evaluation

The performance evaluation metrics for this study are (1) execution time to generate keys based on the number of attributes in the private key and (2) data encryption/decryption execution time based on the number of leaf nodes in the access policy. In lieu of an IoT environment, we tested ABE using a VMware Workstation image running 64-bit Ubuntu 20.04.1, virtually allocating

4GB RAM with four 2-core processors. The physical device runs 64-bit Windows 10 Pro with a 2.40GHz Intel Core i9-9980HK CPU and 16GB RAM [31].

For this evaluation, we implemented the Bethencourt et al. [26] ABE cryptosystem using the `cp-abe` toolkit [32]. According to [27], "the implementation uses a 160-bit elliptic curve group based on the supersingular curve $y^2 = x^3 + x$ over a 512-bit finite field" [p. 9].

In Fig. 8, we computed the execution time to generate keys based on the number of attributes associated with the private key using `cpabe-keygen` from the `cp-abe` toolkit. For $S_{\{att\}} <= 5$, the run-time is not as linear with the number of attributes when compared to a number of attributes $S_{\{att\}} >= 10$.

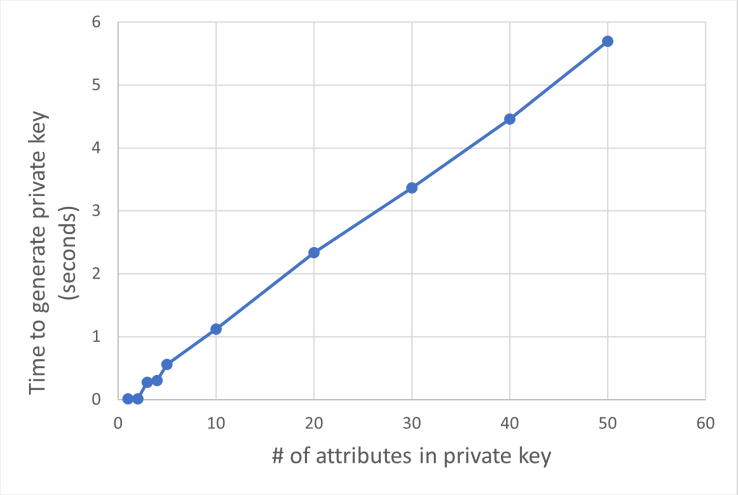

Fig. 8. Key Generation (# of attributes in private key).

Fig. 9 depicts the data encryption run-time based on the number of leaf nodes in the access policy using `cpabe-enc` from the `cp-abe` toolkit. As Bethencourt et al. [27] state, "the polynomial operations at internal nodes amount to a modest number of multiplications and do not significantly contribute to the running time. Both remain quite feasible for even the largest problem instances" [p. 9].

On the other hand, Fig. 10 shows the performance of `cpabe-dec` from the `cp-abe` toolkit. The data decryption run-time is not linear with respect to the number of leaf nodes in the access policy. This non-linearity of run-time with respect to the number of leaf nodes in the policy is most likely due to the lack of optimization techniques used for efficient decryption algorithms [27, pp. 7-8].

In summary, our performance evaluation clearly shows that `cpabe-keygen` and `cpabe-enc` have run-times that increase linearly with the number of attributes in the private key or number of leaf nodes in the access policy. However, `cpabe-dec` depends on an efficient decryption algorithm using optimization

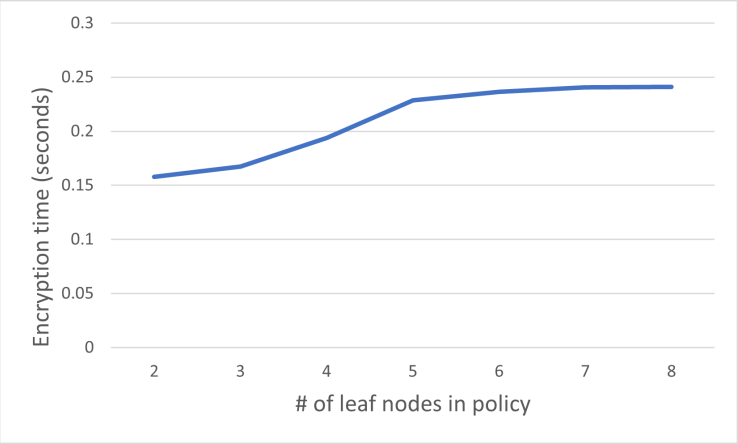

Fig. 9. Encryption Time (# of leaf nodes in policy).

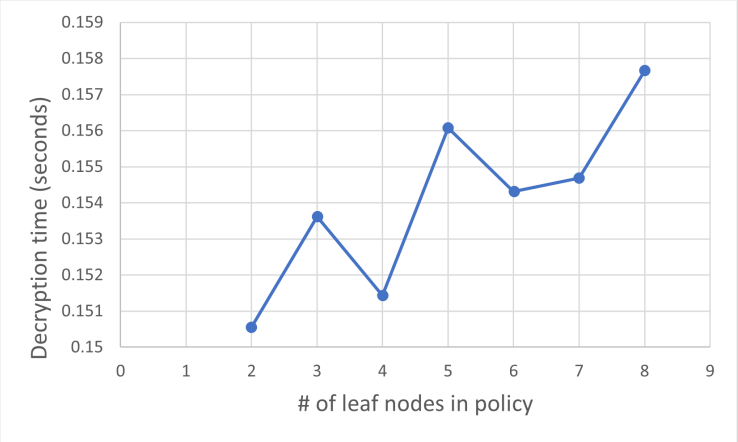

Fig. 10. Decryption Time (# of leaf nodes in policy).

techniques since the performance "depends on the specific access tree of the ciphertext and the attributes available in the private key" [27, p. 10].

8 Conclusion and Future Work

In this paper, we proposed a scheme that used the combination of Blockchain technology and Attribute-based Encryption to secure and protect the privacy of data transmitted in IoT networks. Our system provides verification, trustworthiness, and tamper-proof data through blockchain, while simultaneously achieving privacy and fine-grained access control through the use of ABE. In our model, the key to preserving confidentiality and privacy is applying encryption at the

IoT gateway so that the data is encrypted before entering the blockchain, thus achieving end-to-end network traffic encryption. A performance experiment evaluated the influence of the number of attributes used in the ABE access policy. Our evaluation shows that ABE is efficient for encrypting data in an IoT system. In the future, we will develop a testbed for further studies.

References

1. S. Xu, Y. Qian and R. Q. Hu, "Cybersecurity in Intelligent Networking Systems," *Wiley-IEEE Press*, 2023.
2. S. Xu, Y. Qian and R. Q. Hu, "Privacy-Preserving Data Preprocessing for Fog Computing in 5G Network Security," *2018 IEEE Global Communications Conference (GLOBECOM)*, Abu Dhabi, United Arab Emirates, 2018.
3. S. Xu and F. Ye, "A Predicate Encryption Based Anomaly Detection Scheme for E-Health Communications Network," *2018 IEEE International Conference on Communications (ICC)*, Kansas City, MO, USA, 2018.
4. N. Hasan, A. Chamoli, and M. Alam, "Privacy challenges and their solutions in IoT," in *Internet of Things (IoT)*, M. Alam, K. A. Shakil, and S. Khan, Ed., 1st ed. Cham, Switzerland: Springer, 2020, ch. 11, pp. 219-231.
5. L. Zhu, K. Gai, and M. Li, "Introduction," in *Blockchain Technology in Internet of Things*. 1st ed. Cham, Switzerland: Springer, 2019, ch. 1, pp. 3-6.
6. L. Zhu, K. Gai, and M. Li, "Blockchain and Internet of Things," in *Blockchain Technology in Internet of Things*. 1st ed. Cham, Switzerland: Springer, 2019, ch. 2, pp. 9-14.
7. M. A.J. Jamali, B. Bahrami, A. Heidari, P. Allahverdizadeh, and F. Norouzi, "IoT security," in *Towards the Internet of Things*, I. Chlamtac, Ed., 1st ed. Cham, Switzerland: Springer, 2020, ch. 3, pp. 76-77.
8. A. Skarmeta, J. L. Hernandez-Ramos, and J. A. Martinez, "User-centric privacy," in *Internet of Things Security and Data Protection*, S. Ziegler, Ed., 1st ed. Cham, Switzerland: Springer, 2019, ch. 13, pp. 199-200.
9. K. A. Fasila and S. Mathew, "Blockchain based protocols for IoT security using ABE cryptosystems," in *2020 International Conference on Communication and Signal Processing (ICCSP)*, Chennai, India, 2020, pp. 0079-0083, doi: 10.1109/ICCSP48568.2020.9182247.
10. Q. He, Y. Xu, Z. Liu, J. He, Y. Sun, R. Zhang. "A privacy-preserving Internet of Things device management scheme based on blockchain," *International Journal of Distributed Sensor Networks*. vol. 14, no. 11, pp. 1-12, Nov. 2018. doi:10.1177/1550147718808750.
11. M. Frustaci, P. Pace, and G. Aloi, "Securing the IoT world: Issues and perspectives," *2017 IEEE Conference on Standards for Communications and Networking (CSCN)*, Helsinki, 2017, pp. 246-251.
12. D. Boneh, A. Sahai, and B. Waters, "Functional encryption: Definitions and challenges," in *Theory of Cryptography*, Y. Ishai Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 253-273.
13. D. Micciancio, "Functional encryption." Lattice cryptography. Available: https://cseweb.ucsd.edu/~daniele/LatticeLinks/FE.html (accessed Oct. 10, 2020).
14. J. Li, Y. Zhang, J. Ning, X. Huang, G. S. Poh and D. Wang, "Attribute based encryption with privacy protection and accountability for CloudIoT," in *IEEE Transactions on Cloud Computing*, doi: 10.1109/TCC.2020.2975184.

15. M. Ali, M. Sadeghi and X. Liu, "Lightweight revocable hierarchical attribute-based encryption for Internet of Things," in *IEEE Access*, vol. 8, pp. 23951-23964, 2020, doi: 10.1109/ACCESS.2020.2969957.
16. J. Sengupta, S. Ruj, and S. Das Bit, "A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT," *Journal of Network and Computer Applications*, vol. 149, January 2020. [Online]. Available: https://doi.org/10.1016/j.jnca.2019.102481 (http://www.sciencedirect.com/science/article/pii/S1084804519303418)
17. D. Pavithran, K. Shaalan, J. Al-Karaki, and A. Gawanmeh, "Towards building a blockchain framework for IoT," *Cluster Computing*, vol. 23, pp. 2089–2103 (2020). [Online]. Available: https://doi.org/10.1007/s10586-020-03059-5
18. F. Dai, Y. Shi, N. Meng, L. Wei, and Z. Ye, "From Bitcoin to cybersecurity: A comparative study of blockchain application and security issues," *2017 4th International Conference on Systems and Informatics (ICSAI)*, Hangzhou, 2017, pp. 975-979.
19. S. Fan, L. Song, and C. Sang, "Research on Privacy Protection in IoT System Based on Blockchain," Oct 2019. Presented at International Conference on Smart Blockchain [Online]. Available: https://doi.org/10.1007/978-3-030-34083-4_1
20. G. Li and H. Sato, "A privacy-preserving and fully decentralized storage and sharing system on blockchain," in *2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC)*, Milwaukee, WI, USA, 2019, pp. 694-699, doi: 10.1109/COMPSAC.2019.10289.
21. Q. Wen, Y. Gao, Z. Chen and D. Wu, "A blockchain-based data sharing scheme in the supply chain by IIoT," *2019 IEEE International Conference on Industrial Cyber Physical Systems (ICPS)*, Taipei, Taiwan, 2019, pp. 695-700, doi: 10.1109/ICPHYS.2019.8780161.
22. K. O. Obour Agyekum, Q. Xia, E. B. Sifah, J. Gao, H. Xia, X. Du, and M. Guizani, "A secured proxy-based data sharing module in IoT environments using blockchain," in *Sensors*, Basel, Switzerland, 2019, vol. 19(5), no. 1235, Mar. 2019. doi:10.3390/s19051235
23. Y. Rahulamathavan, R. C.-W. Phan, M. Rajarajan, S. Misra and A. Kondoz, "Privacy-preserving blockchain based IoT ecosystem using attribute-based encryption," *2017 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, Bhubaneswar, 2017, pp. 1-6, doi: 10.1109/ANTS.2017.8384164.
24. O. Novo, "Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT," *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 1184–1195, Apr. 2018, doi: https://doi.org/10.1109/jiot.2018.2812239.
25. A. Kalla, P. Prombage, and M. Liyanage, "Introduction to IoT," in *IoT Security: Advances in Authentication*, M. Liyanage, A. Braeken, P. Kumar, and M. Ylianttila, Ed., 1st ed. Hoboken, NJ, USA: Wiley, 2020, ch. 1, pp. 5-20.
26. A. Jurcut, P. Ranaweera, and L. Xu, "Introduction to IoT Security," in *IoT Security: Advances in Authentication*, M. Liyanage, A. Braeken, P. Kumar, and M. Ylianttila, Ed., 1st ed. Hoboken, NJ, USA: Wiley, 2020, ch. 1, pp. 27-41.
27. J. Bethencourt, A. Sahai and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," *2007 IEEE Symposium on Security and Privacy (SP '07)*, Berkeley, CA, 2007, pp. 321-334, doi: 10.1109/SP.2007.11.
28. B. Cheung, "Attribute-based encryption for healthcare blockchain," bennycheung.github.io. Available: https://bennycheung.github.io/attribute-based-encryption-for-healthcare-blockchain (accessed Nov. 7, 2020).

29. D. Li, B. Cheung, and A. Yang. "Why blockchain for healthcare?," jonahgroup.com. Available: https://www.jonahgroup.com/blog/why_blockchain_for_healthcare (accessed Nov. 7, 2020).
30. J. Lee, S. Oh, and J. Jang, "A work in progress: Context based encryption scheme for internet of things," *Procedia Computer Science*, vol. 56, pp. 271–275, 12 2015.
31. X. Wang, J. Zhang, E. M. Schooler and M. Ion, "Performance evaluation of Attribute-Based Encryption: Toward data privacy in the IoT," *2014 IEEE International Conference on Communications (ICC)*, Sydney, NSW, 2014, pp. 725-730, doi: 10.1109/ICC.2014.6883405.
32. J. Bethencourt, A. Sahai and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," hms.isi.jhu.edu. Available: http://hms.isi.jhu.edu/acsc/cpabe/ (accessed Nov. 5, 2020).