The Eurasia Proceedings of Science, Technology, Engineering & Mathematics (EPSTEM)
ISSN: 2602-3199

The Eurasia Proceedings of Science, Technology, Engineering & Mathematics (EPSTEM), 2024

Volume 28, Pages 23-33

ICBASET 2024: International Conference on Basic Sciences, Engineering and Technology

Attribute-Based Access Control in Internet of Things Security

Melike Kukut
Gebze Technical University

Ibrahim Sogukpinar
Gebze Technical University

Abstract: With the rapid spread of the use of Internet of Things devices, it has become an important situation for these devices to be provided with critical infrastructure, integrated into daily life and the creation of robust security mechanisms. The attribute-based access control (ABAC) method has emerged as a promising approach to manage access of IoT resources based on users' attributes. However, current ABAC models lack adequate privacy protections and do not address specific vulnerabilities, especially in scenarios where sensitive data is involved. The research includes a comprehensive review of the ABAC models that stand out in the context of IoT security, including the limitations and vulnerabilities that they carry. In this work, a new framework has been proposed that integrates zero-knowledge proofs (ZKP) with homomorphic encryption into the ABAC model, providing stronger security guarantees and privacy protection. While ZKPs allow users to prove that they have certain attributes or access rights without disclosing sensitive information, homomorphic encryption allows calculations to be performed on encrypted data without decryption. The proposed framework has been evaluated by theoretical analysis and simulation studies. The findings of this research are expected to contribute significantly to the field of IoT security by providing a more robust and privacy-protecting access control mechanism for IoT environments. The proposed framework has the potential to mitigate various security threats, including unauthorized access, data and privacy violations.

Keywords: IoT, ABAC, Homomorphic encryption, Zero knowledge proof

Introduction

As the number of devices included in wireless networks increases every day, the vulnerabilities bringing with them are also increasing. Labeling of each of these devices, monitoring their timeliness and evaluating requests for access to resources are also of great importance for enterprises, especially in the context of information security. Information privacy is one of the most sensitive issues for IoT (Mahmoud et al., 2015). The need for easy accessibility of data also brings with it the challenge of protecting information in personalized services. Some factors should be taken into account when designing the privacy protection mechanism. For example, the authentication phase, the access control process and the development of trust management are topics that should be focused on with importance (Sicari et al., 2015). Although a number of projects have been developed to protect security and privacy, there is still no complete security protection mechanism for personal information privacy that provides data privacy for the IoT (Liu et al., 2020).

An incorrectly configured IoT device and/or switching devices can disrupt networks. For example, a device may be configured incorrectly to send unwanted broadcasts to the network, which can lead to a severely disruptive situation for the network. Even in situations that do not harbor malicious intent, networks can be damaged due to one or more misconfigured IoT devices or switches (Bandyopadhyay et al., 2011). The way to prevent such glitches is to make access control strict on IoT devices. Therefore, the attribute-based access control model

(ABAC); it is the most preferred method with the ability to enforce access control based on the attributes of devices, users and the environment (Baskaran et al., 2019).

In recent years, enterprises, various institutions and organizations engaged in scientific activities have updated their access control mechanisms with the attribute-based access control model (ABAC). This model, which has received a lot of attention, provides permission to users by blending resource access policies with attribute sets and manages the process. As the needs of institutions change, the ABAC model can easily adapt itself to new requirements. In this work, a new framework has been proposed that integrates zero-knowledge proofs (ZKP) with homomorphic encryption into the ABAC model, providing stronger security guarantees and privacy protection. Also, an application was implemented based on a sample scenario, theoretical and security analysis findings were included. The rest of the paper is organized as follows. Second section introduces basic information and related works. Proposed model is presented in the third section. Fourth section explains realization and discussion of the proposed solution. Last section is conclusion.

Basic Information and Related Studies

Attribute Based Access Control (ABAC)

Instead of basing access control decisions on a user's identity like traditional methods, ABAC bases access control on the attributes of assets. These attributes are user attributes, object attributes, environmental attributes, connection attributes, and administrative attributes. Attributes can be thought of as properties of anything that can be defined and assigned a value. Attributes that are predefined and assigned by an authority are properties that describe certain aspects of the subject, object, environmental conditions, and/or desired actions. In its most basic form, ABAC is based on the evaluation of the subject's attributes, the object's attributes, and a formal relationship or access control rule that defines the allowed operations for subject-object attribute combinations (Bhatt et al., 2020).

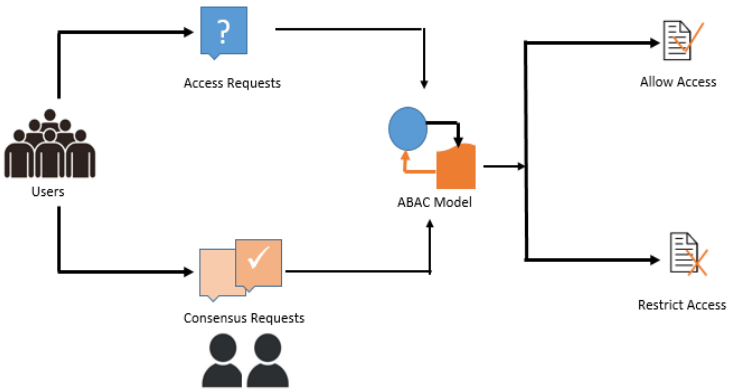

Figure 1. Attribute based access model

Access control is not the same thing as authentication. Authentication is the act of verifying that the person performing a transaction is actually the person he/she says he/she is. Access control or authorization, on the other hand, refers to the ability of a subject to access a specific object (network, data, application, service, etc.) is the decision to allow or deny access (implicit or explicit). Traditional Access Control (AC) methods attempt to verify the user's identity of the request to perform an operation (for example, reading) on an object (for example, a file) directly or through predefined attribute types, such as roles or groups assigned to that user, thus performing the control operation. However, this process remains cumbersome and insufficient. ABAC provides a more dynamic AC management capability and limits the long-term maintenance requirements of object protections (Hao et al., 2013).

ABAC offers a flexible, fine-grained mechanism and is also detailed. ABAC allows object owners or administrators to implement the AC policy without prior knowledge of the specific subject and for an unlimited number of subjects that may require access. Under ABAC, access decisions can enable switching between requests by simply changing attribute values without needing to change the subject/object relationships that define the underlying rule sets. ABAC is the critical management element of corporate information sharing in large organizations or enterprises with unified organizational structures. However, it is becoming quite

complicated to carry out the access control mechanism in a healthy way in these structures. At the system level, the focus is on the access control mechanism and its working logic (Liu et al., 2020) .

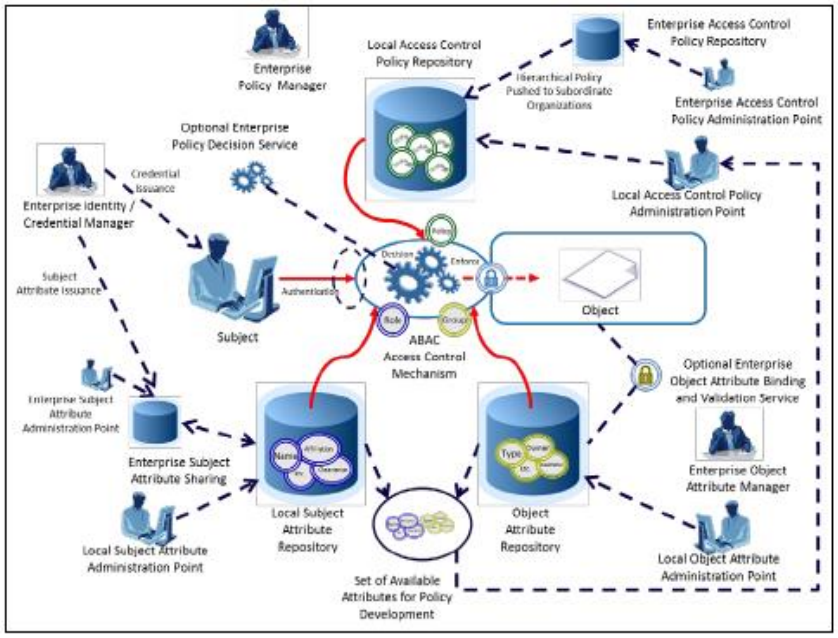

Figure 2. Enterprise ABAC scenario

ABAC does not work without a sufficient set of objects and subject attributes. There are four elements that are taken into account as basic security needs in the ABAC access control model for the sharing, transmission, storage, updating of attributes. These are preparation, veracity, security, readiness. The security structure of the attribute evaluation scheme (AES) is constructed based on these four basic areas. In the ABAC access control model, the concept of veracity, one of the basic security needs, has two dimensions: attribute trustworthiness, attribute accuracy. How well an attribute resource invoked for use from a remote access point (AP), or access control function (AF) is validated and identified is evaluated by the attribute reliability metric (Hao et al., 2013).

It is tried to create a security policy in the form of using encryption technologies, taking measures to immediately recognize unwanted changes in attribute values and making the policies mandatory, protecting data stores with a defense system, logging and continuous monitoring of the functioning of the entire ABAC model. Security protocols are used to ensure the security of attributes that are processed for use from attribute repositories, that is, that are in transmission. In order to protect against repeated attacks, the information provided by the remote access point or access control functions is transmitted digitally signed. This guarantees the integrity and confidentiality of the attribute. For higher assurance levels, the use of digitally signed attributes (Cryptobinding) provides a hash of the attribute. Thus, the access control function (AF) can ensure that an attribute has not been modified or tampered with before processing. Attributes between access control functions must be protected from changing during transition processes (Hu et al., 2017). The main security vulnerabilities that the ABAC is vulnerable to abuse and the measures that should be taken against them are listed in Table 1.

Homomorphic Encryption

Homomorphic encryption is an encryption technique that allows calculations to be performed on encrypted data without decrypting it. In other words, it protects the confidentiality of information throughout the computational process by supporting meaningful operations on the data, while ensuring that the data remains encrypted. This ability is especially valuable in scenarios where privacy and security are of critical importance (Çebi, 2019).

Description: An encryption technique E is called homomorphic if it satisfies the following equation for any possible input m:

$$D(f(E(m))) = f(m), \qquad (1)$$

D is the decryption function, and f is any function (e.g. multiplication, addition) (Gentry, 2009).

Table 1. The security risks that ABAC carries

	Security Risk	**Precautions to Be Taken**
Attribute Spoofing	Attackers may try to imitate or modify attribute values to gain unauthorized access.	Strong authentication and verification mechanisms should be implemented to ensure the integrity of attribute values.
Inadequate attribute protection	If attributes are not properly protected, attackers can gain access to sensitive information, which can lead to unauthorized access.	Encryption and access control policies should be used to protect attribute stores and transmission channels.
Incomplete or Incorrect Policies	Access control policies that are incorrectly defined or left incomplete may cause unwanted access or deny legitimate access.	Access control policies should be reviewed regularly and updated if necessary to ensure that they accurately reflect the organization's requirements.
Lack Of Policy Management	Poor management of access control policies can lead to inconsistencies or errors in the implementation of access rules.	A robust policy management system with appropriate version control and audit capabilities should be implemented.
Insufficient Logging and Monitoring	Inadequate logging and monitoring makes it difficult to detect and respond to security incidents or suspicious activities.	Extensive daily recording and monitoring should be implemented to monitor access events, and alerts should be created for unusual patterns or possible attacks.
Single Point Of Failure	If the central decision point or qualification authority becomes a single point of failure, the entire access control system may be compromised.	Redundancy and failover mechanisms should be put into operation to ensure the availability of the system and resistance to failures.
Attribute Inference	Attackers can try to obtain sensitive attribute values by observing patterns in access requests and responses to them	Techniques such as data masking or anonymization should be used to prevent attribute extraction.
Insecure Attribute Transmission	If attribute values are transmitted unsecure, they may be intercepted or changed during transmission.	Secure communication protocols for encrypting attribute data during transmission (e.g. HTTPS should be preferred.
Unauthorized Attribute Changes	Unauthorized changes to attribute values may cause unauthorized access.	Appropriate access controls and control mechanisms should be implemented to prevent and detect unauthorized changes to attribute values.
Inconsistent Attribute Format	Inconsistencies in attribute formats can lead to misinterpretation and incorrect access control decisions.	To ensure consistency, it is necessary to standardize attribute formats and apply validation rules.
Complexity and Over-Privilege	Granting complex attribute-based policies or excessive privileges may cause unwanted access.	It is very important to configure access control policies in a simple, well-defined way and to keep them in line with corporate security requirements.

There are different types of homomorphic encryption schemes, each with different levels of functionality and security features. Depending on the number of operations to be performed, it is divided into two: partial homomorphic encryption (PHE) and full homomorphic encryption (FHE). PHE supports addition or multiplication operations on encrypted data, but not both. In partial homomorphic encryption, the RSA algorithm is one of the first known homomorphic encryption methods. It shows partial homomorphic encryption property with respect to multiplication. The Paillier algorithm is partially homomorphic in terms of both addition and multiplication. The ElGamal algorithm also works in the partially homomorphic property for two mathematical operations. In summary, PHE is usually used only in applications where a certain type of calculation needs to be performed on encrypted data. Nevertheless, PHE provides a valuable level of

functionality for certain applications. PHE is a relatively simpler structure compared to fully homomorphic encryption (FHE), which supports both addition and multiplication operations, and it is also efficient. Moreover, it does not impose any additional overhead, which makes it preferable for certain practical applications where the level of homomorphic functionality is sufficient (Domingo-Ferrer, 2022).

For example, let E represent encryption, D represents decryption, and K represents the secret key used in encryption. In addition, let the + and * signs also express addition and multiplication operations on the Q set. If

$$"a + b = DK" ("EK" ("a")"+ EK"("b"))" \forall a,b \epsilon Q" \quad (2)$$

the encryption function E is assumed to have a homomorphic addition property, and if

$$"a * b = DK" ("EK" ("a")"* EK"("b"))" \forall a,b \epsilon Q" \quad (3)$$

it is assumed that the encryption function E has a homomorphic multiplication property (Gentry, 2009).

EK(a), used in these equations, shows the encryption of the number a with the secret key K, and DK shows the decryption of the encrypted sum or multiplication operation result obtained, again using the secret key K. Homomorphic secrecy can be realized using a symmetric or public key infrastructure. Thus, the confidentiality of the data content and the safe completion of the transactions can be ensured.

Full homomorphic encryption (FHE) is a structure that allows performing an innumerable number of different types of operations on encrypted data. It allows data to remain hidden even during calculation. FHE is suitable for scenarios where complex calculations are required on encrypted data without disclosing the decrypted results. It provides the highest level of homomorphic functionality. It supports the evaluation of any mathematical function on encrypted data. FHE is especially ideal in scenarios where privacy is very important, such as secure cloud computing. Because with FHE, data can be processed on a cloud server without the server needing to know the actual content of the data. It provides users with the opportunity to securely outsource calculations on untrusted servers. FHE is especially preferred in sensitive areas such as health, finance and government, where data privacy protection is very important (Hoscoskun, 2020).

Zero Knowledge Proofs

The concept of zero knowledge was first proposed by Shafi Goldwasser, Silvio Micali and Charles Rackoff in their article "The Knowledge Complexity of Interactive Proof-Systems" in 1985. A zero-knowledge proof structure is a technique developed to limit the amount of information transferred from a prover A to a verifier B in an encryption protocol. A zero-knowledge proof is a cryptological concept that indicates a situation in which one party (the prover) can prove to another party (the verifier) that they know a certain piece of information or a secret without disclosing the actual information itself. Zero-knowledge proofs are a fundamental concept in cryptographic protocols and are a powerful tool used to ensure security and privacy in various applications (Hasan, 2019).

The term "zero knowledge" means that after the interaction, the verifier acquires zero knowledge about the actual information or secret; they gain confidence that only the verifier has the information. There are three concepts that are essential in this method (Beydemir & Sogukpinar, 2017)

- *Completeness*: If the verifier has confidential data or information and follows the protocol correctly, the verifier will be convinced of this fact.
- *Soundness*: If the verifier does not have any confidential data or information, he/she should not be able to convince the verifier otherwise, even if he/she follows the protocol.
- *Zero Knowledge*: After the proof is completed, the verifier can not obtain anything about the actual information except that the substantiator has it.

Zero-knowledge proofs can be used in authentication protocols to prove the knowledge of a password without revealing the password itself. In blockchain and cryptocurrency systems, zero-knowledge proofs are used to demonstrate the ownership of coins or tokens without disclosing their actual transactions or account balances. Zero-knowledge proofs are a fundamental concept in cryptographic protocols and are a powerful tool used to ensure security and privacy in various applications (Hasan, 2019).

Related Studies

Perazzo et al. (2021), pointed out in their study that it is difficult to provide access control to data in networks with devices of different operating principles with low computing power and various security levels. They state that although the ABAC model is a very preferred method, it does not support encryption and cannot fully meet data privacy. They say that the ABAC model has the advantage of meeting both user-derived dynamic attributes and static attributes, but that it has privacy and security vulnerabilities. Servos et al. (2017), on the other hand, instead of defining attribute values to users and objects directly one-on-one, they created user groups and object groups and created a hierarchical model. They also assigned attributes to groups. The name of this proposed model is HGABAC. The advantage of this model is the easy management of attributes for users and objects. This model, which is more effective and practical in an administrative sense, is still not able to offer security in its full sense.

Hamsanandhini et al. (2022) pointed out that ABAC alone is not safe in their study, propose a framework they call Multi-Authorization Attribute-based encryption (MA-ABE) for secure sharing and access of patients' personal health information in cloud storage. In order to provide fine-grained and secure data access through health records, this encryption (MA-ABE) technique helps to encrypt each person's health record. According to Liu et al. (2022) on the other hand, by drawing attention to the security vulnerabilities in the blockchain information processing model, they propose a new multi-identity attribute-based access control model instead of using the classical ABAC in their work.

Method

Although encryption is considered the most effective solution method to strengthen ABAC, unfortunately it causes various difficulties when calculating attributes and this reduces the ability to apply access policies. Homomorphic encryption, which allows calculations on encrypted data without decrypting it, is the method needed at this point. The attributes used in the ABAC model are encrypted using a homomorphic encryption scheme. Thus, it is ensured that sensitive attributes are protected while allowing calculations to be made on encrypted data. Based on the results of zero-knowledge proofs and homomorphic calculations, the access control system makes a decision to grant or deny access without disclosing the basic attribute values.

In this study, zero information proof (ZKP) along with homomorphic encryption techniques were used to make ABAC, an attribute-based access control model, strong against cyber-attacks. Privacy and security have been further enhanced by allowing secure calculations on encrypted attributes without the need to disclose sensitive information. In cyber security, threats from within the system are characterized as problematic to predict and control more than threats from outside. By allowing access control decisions to be made based on encrypted data and verified using ZKPs, the system becomes more resistant to insider threats. Even if malicious insiders have access to encrypted data, they cannot change or interfere with access control decisions without providing valid evidence. The definitions of the components that need to be included into the account in the algorithm are as follows:

Description 1 (Entity): The object is embodied as two parts of the source and operation. In total, there is a tetrad (S, R, O, E) in which four entities and ABAC can be abstracted, where S, R, O and E represent the entity set consisting of subject attributes, resource attributes, process attributes and environment attributes, respectively. These four sets of entities can be expressed as follows: S = {s1, s2, s3, ..., sm}, R = {r1, r2, r3, ..., rn}, O = {o1, o2, o3, ... , oj}, E = {e1, e2, e3, ... ,Oct},where n, m, k, $j \geq 1$.

Description 2 (Attributes): These are used to describe the internal properties of entities. The set of attributes can be represented as A = {a1, a2, a3, ... , as}. TU, RA, OA and EA, respectively, TU = {crypto checkpoint for, sA2, sA3, ..., sAm}, RA = {rA1, rA2, rA3,..., rAn}, OA = {oA1, OA2, OA3,...,oAj}, EA = {eA1, eA2, eA3,...,eAk} represents the set of all subject attributes, resource attributes, process attributes, and environment attributes shown as. Let's take SA as an example, for the subject si, sAi represents the set of attributes, where $sAi \subseteq A$.

Description 3 (Attribute-value pair): The definition and custom value of an attribute are represented by an attribute-value pair (avp), which is defined as a binary (attribute, value) (i.e. attribute = value). Savp, Ravp, Oavp, and Eavp are used to represent attribute-value pairs of the subject, resource, process, and environment attributes, respectively.

Description 4 (Policy): This is denoted by p and describes a subject with certain attribute values that allows or rejects operations on the resources of the corresponding attribute values in a given environment. Its official description can be expressed as follows: ← (SA, RA, OA, EA Tu) and this ← the result value will be allowed or reject. It shows positive authorization and negative authorization, respectively. The set of principles is expressed as follows: P = {p1, p2, p3, ..., pn}.

Description 5 (Rule): This is indicated by r and is the basic unit of the policy and the smallest unit that conducts the policy evaluation. The value of the domain element is the allow or reject element, which represents the authorization result of the rule (Hao et al., 2013; Liu et al., 2020).

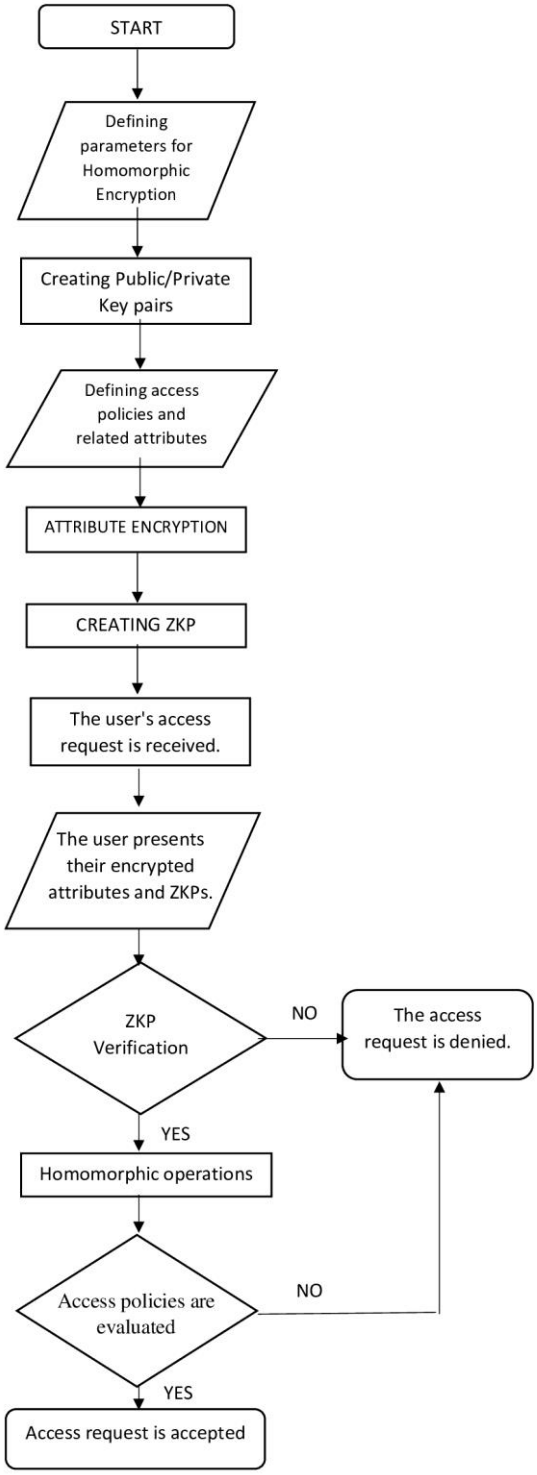

Figure 3. Flow diagram of the algorithm

Table 2. Algoritm of ABAC

Algorithm - The process of applying homomorphic encryption and Zero-Knowledge Proof method with ABAC
Input: Entities, Attributes, Attribute Value Pairs, Policies, Rules **Output:** Allowed / Denied **1.** The parameters for the homomorphic encryption scheme are defined. **2.** Public / private key pairs are created for the encryption scheme. **3.** Access policies and the attributes associated with these policies are defined. **4.** Attributes are encrypted using homomorphic encryption. **5.** ZKPs are created to prove without explanation that they have certain qualifications. **6.** When a user requests access, he presents his encrypted attributes and ZKPs. **7.** The ZKPs submitted by the user are verified to ensure that they have the necessary attributes. **8.** Homomorphic operations are performed to evaluate access principles. **9.** Access is granted or denied according to the evaluation result

Sample Application and Security Analysis

Application

We decided according to the base scenario on the healthcare sector, where the use of IoT devices is in vogue. In the health information system environment, a large number of people are involved, including patients, patient relatives, research assistants, administrative personnel to solve patient cases, emergency workers, specialist doctors, professors, assistant doctors, foreign health care providers and other health professionals. An example of a simple access control permissions list can be configured as Figure 4.

```
Role: PROFESSOR# Patient_record: write#Context:Hospital->Permit
Role: DOCTOR# Patient_record: write#Context:Hospital->Permit
Role: ASST_DOCTOR# Patient_record: read#Context:Hospital->Permit
Role: NURSE# Patient_record: read#Context:Hospital->Permit
Role: NURSE# Patient_record: write->Deny
Role: MANAGER# Patient_record: read#Context:Hospital->Permit
Role: MANAGER# Patient_record: write->Deny
Role: TECHNICIAN# Biling_Information: write#Context: Hospital->Permit
Role: TECHNICIAN#Patient_record:write->Deny
```

Figure 4. Example of access control list

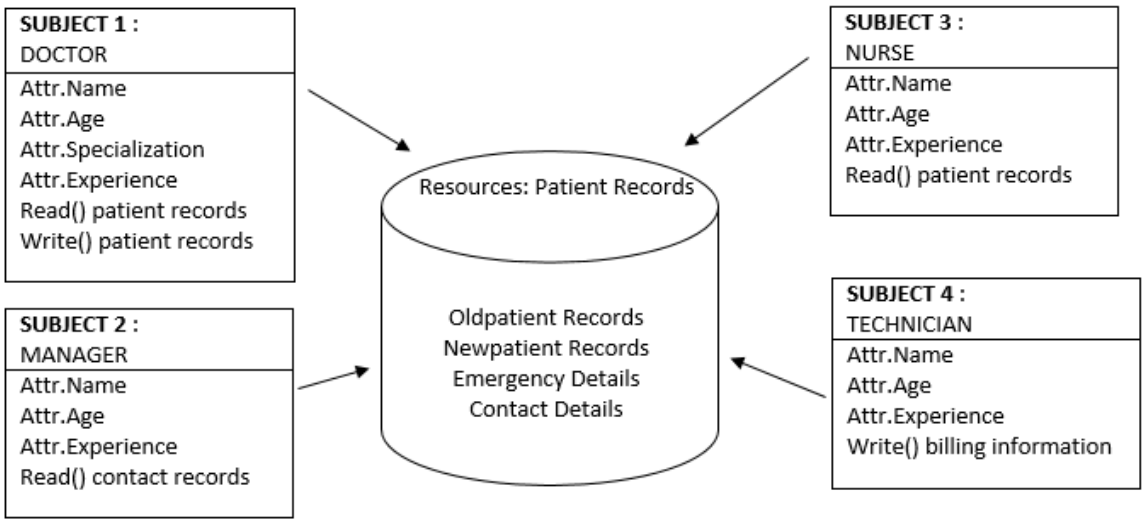

Figure 5. Sample health ınformation system subjects and resource repository

The attributes of doctors are name, age, work experience, department knowledge, etc. the attributes of the objects are the sources of patient records (medical reports, contact information, emergency information, etc.). The information contained in the medical reports are attribute values such as the patient's blood type, the permanent list of medications he/she uses, the surgeries he/she has undergone, the treatment applied, and his/her allergic condition. Emergency information, on the other hand, is the contact information of the patient's relative, information about whether the patient has a possible life-risk condition or not. The hospital director, who is the subject, has the right to access the personal and financial information of patients, the content of the treatment he is undergoing in the hospital. However, these rights are not in unlimited authority. Even if he/she makes a new medical record entry, he/she cannot view private notes about that patient unless it is signed by the relevant doctor. In addition, they can delete patient information. For example, a laboratory employee acting as a technician can add new information about the patient, add the invoice of the procedure to the system, but it cannot enter other areas. Figure 5 shows the resource repository relationship with the subjects in this scenario as an example (Figure 5).

In the example scenario, a request for access to the relevant records was created through four subjects, and authentication was performed using the zero-knowledge proof method, and then permission to access the authorized record was obtained after attribute verification. If the transaction is not authorized, it will be rejected.

Theoretical Analysis

The theoretical safety of the proposed method is based on the discrete logarithm problem on the elliptic curve algorithm. In the code used, Pairing Group was used, which represents a curve called SS1024. the 1024-bit long key again corresponds to the 1024-bit key in the RSA and Diffie Hellman algorithms.

Considering the number of bits representing the large prime number required to determine the finite field in the N discrete logarithm problem, the method has an O(2N) exponential complexity. As an example, a 2.2 GHz, 8-core processor can solve a 768-bit discrete logarithm problem in 825 years (Kleinjung et al., 2017).

Application Security Analysis

In the study, virtual working environments offering the opportunity to work with versatile security analysis tools were used. Controls such as sensitive data protection, data loss prevention, key management are provided. It is rezist against session hijacking attacks, password cracking, phishing attacks because zero information proof is used in the authentication phase of this study. The fact that homomorphic encryption has been used against possible threats such as cryptanalytic, side channel, frequency and coincidence attacks also provides an advantage. It seems to be leading the way again to eliminate attacks that can be carried out by targeting key production.

Conclusion

In this work, it is proposed that homomorphic encryption should be preferred to make ABAC strong. The approach of using homomorphic encryption and zero information proof together has been revealed by the literature study as the most accurate method. Attribute-Based Access Control using zero-knowledge proofs with homomorphic encryption is a state-of-the-art security model with a large number of potential applications in various fields. While there are currently no widely publicized real-life examples of organizations using this particular model, there are researchers and organizations actively working to advance the field of secure access control with techniques such as ABAC, ZKPs, and homomorphic encryption.

The research for solutions to ABAC's problems such as administrative, scalability, auditability, and correct configuration continues on the academic field without slowing down. One of the main challenges of ABAC is that it requires more resources and expertise to design, implement and manage. ABAC involves defining and maintaining a large number of attributes, principles, and rules, which can be time-consuming and error-prone. ABAC also requires more processing power and network bandwidth to evaluate and implement access decisions that can affect performance and availability. Because attributes may contain sensitive or personal information that needs to be protected and controlled, ABAC may also pose an increased security and privacy risk.

The development of an access control model in big data, cloud computing and blockchain based on the internet of things, one of the rapidly rising issues of today, have been identified as future areas of study. It has been revealed by research that the data stored publicly on the blockchain is still under the threat of privacy leakage. As future studies, new studies on systems that also integrate homomorphic encryption and zero-knowledge proof on attribute-based access control blockchain information sharing, especially for supply chain management, are expected to continue to be conducted.

Scientific Ethics Declaration

The authors declare that the scientific ethical and legal responsibility of this article published in EPSTEM journal belongs to the authors.

Acknowledgements or Notes

* This article was presented as oral presentation at the International Conference on Basic Sciences, Engineering and Technology (www.icbaset.net) held in Alanya/Turkey on May 02-05, 2024.

References

Bandyopadhyay, D. & Sen, J. (2011). Internet of Things: Applications and Challenges in Technology and Standardization. *Wireless Personal Communications*, *58*, 49-69.

Baskaran, S. B. M. (2019). Internet of things security. *Journal of ICT Standardization*, *7*(1) 21-40.

Beydemir A., & Sogukpınar, I. (2017), Lightweight zero knowledge authentication for Internet of things, *In Computer Science and Engineering (UBMK)*(pp.360-365). IEEE.

Bhatt, P., Bhatt, S., & Ko, M. (2020). Poster: IoT Sentinel-An ABAC approach against cyber-warfare in organizations. In *Proceedings of the 25th ACM Symposium on Access Control Models and Technologies*, 223-225.

Cebi, G. (2019). *Homomorphic encryption in cloud computing*. (Master's thesis, Bahcesehir University).

Domingo-Ferrer, J. (2002). A provably secure additive and multiplicative privacy homomorphism. *In International Conference on Information Security* (pp.471-483). Berlin, Heidelberg: Springer.

Gentry, C. (2009). *A fully homomorphic encryption scheme*. (Doctoral dissertation, Stanford University).

Hamsanandhini, S., Eswaran, M., & Varanambika, V. (2022). Health record maintenance using cloud computing and multi authority attribute based encryption. In *Proceedings of the 2022 International Conference on Computer Communication and Informatics (ICCCI)* IEEE. (pp.1-8).

Hasan, J. (2019). Overview and applications of zero knowledge proof (ZKP). *International Journal of Computer Science and Network*, *8*(5), 2277-5420.

Hao, V. C., Ferraiolo, D., Kuhn, R., Friedman, A. R., Lang, A. J., Cogdell, M. M. & Scarfone, K. (2013). Guide to attribute based access control (ABAC) definition and considerations. *NIST Special Publication*, *800*(162), 1-54.

Hoscoskun, R. E. (2020). *Homomorfik sifreleme yontemi uzerine bir inceleme*. (Master Dissertation, Trakya University).

Hu, V. C., Ferraiolo, D. F., Chandramouli, R., & Kuhn, D. R. (2017). *Attribute-based access control*. Artech House.

Kleinjung, T., Diem, C., Lenstra, A. K., Priplata, C., & Stahlke, C. (2017). Computation of a 768-bit prime field discrete logarith. In *Advances in Cryptology–EUROCRYPT 2017: Proceedings of the 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques* (pp.185-201). Springer International Publishing.

Liu, M., Yang, C., Li, H., & Zhang, Y. (2020). An efficient attribute-based access control (ABAC) policy retrieval method based on attribute and value levels in multimedia networks. *Sensors*, *20*(6), 1741.

Liu, C., Xiang, F., & Sun, Z. (2022). Multiauthority Attribute-based access control for supply chain information sharing in Blockchain. *Security and Communication Networks*, *2022*, 1-18.

Mahmoud, R., Yousuf, T., Aloul, F., & Zualkernan, I. (2015). Internet of things (IoT) security: Current status, challenges and prospective measures. In *Proceedings of the 10th International Conference for Internet Technology and Secured Transactions (ICITST)* (pp.336-341). IEEE.

Perazzo, P., Righetti, F., La Manna, M., & Vallati, C. (2021). Performance evaluation of attribute-based encryption on constrained IoT devices. *Computer Communications*, *170*, 151-163.

Servos, D., & Osborn, S. L. (2017). Current research and open problems in attribute-based access control. *ACM Computing Surveys (CSUR)*, *49*(4), 1-45.

Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in internet of things: The road ahead. *Computer Networks*, *76*(15), 146-164.

Author Information

Melike Kukut
Gebze Technical University
Kocaeli, Turkiye
Contact e-mail: *m.kukut2021@gtu.edu.tr*

Ibrahim Sogukpinar
Gebze Technical University
Kocaeli, Turkiye

To cite this article:

Kukut, M., & Sogukpinar, I. (2024). Attribute-based access control in internet of things security. *The Eurasia Proceedings of Science, Technology, Engineering & Mathematics (EPSTEM), 28*, 23-33.