JKAU: Comp. IT. Sci., **Vol. 8** No. 1, pp: 71 – 84 (1440 A.H. / 2019 A.D.)

Doi: 10.4197/Comp. 8-1.7

Privacy-aware Decentralized and Scalable Access Control Management for IoT Environment

Abrar O. Alkhamisi and **Fathy Alboraei**

Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, Saudi Arabia

aalkhamisi0034@stu.kau.edu.sa

Abstract. In recent years, the Internet of Things (IoT) plays a vital role in our daily activities .Owing to the increased number of vulnerabilities on the IoT devices, security becomes critical in the untrustworthy IoT environment. Access control is one of the top security concerns, however, implementing the traditional access control mechanisms in the resource-constrained nature of the IoT devices is a challenging task. With the emergence of blockchain technology, several recent research works have focused on the adoption of blockchain in IoT to resolve the security concerns. Despite, integrating the blockchain in the resource-constrained IoT context is difficult. To overcome these obstacles, the proposed work presents a privacy-aware IoT security architecture to ensure the access control based on Smart contract for resource-constrained and distributed IoT devices. The design of the proposed architecture incorporates three main components such as the contextual blockchain gateway, decentralized revocation manager, and non-interactive zero-knowledge proof based validation. By modeling the contextual blockchain gateway, the proposed architecture ensures the dynamic authentication and authorization based on the contextual information and access policies. Instead of integrating the blockchain technology into resource-constrained IoT devices, the smart contract-based distributed access control system with the contextual blockchain gateway provides the scalable solution. With the association of decentralized revocation manager in the smart contract, it prevents the resource access from the unauthorized users by dynamically generating and updating the revoked user list of all the nodes in the smart contract. Moreover, the proposed architecture employs the non-interactive zero-knowledge proof cryptographic protocol to ensure the transaction privacy within the smart contract. Consequently, it maintains the trade-off between the transparency and privacy while ensuring the security for the distributed IoT environment.

Keywords: Internet of Things (IoT), blockchain, smart contract, access control, non-interactive zero-knowledge proof.

1. Introduction

In the past few years, it has witnessed that the Internet of Things (IoT) has gained significant attention across several sectors from business, social media, smart city, and intelligent transportation to the industries. IoT [1] is a network that interconnects the heterogeneous devices having sensors with diverse functionalities, which are established the connection with either a private or a public network. In the IoT environment, the connected devices range from the wearable accessories to large machines comprising sensor chips. However, the massive number of connected IoT devices and data traffic have become the critical factors in accomplishing the Quality of Service (QoS) due to the restricted resources of the IoT devices in computing, bandwidth, and storage. Also, the IoT environment enables anyone to control the IoT devices to perform their required functionality remotely. IoT technology employs the standard protocols to share the information among the IoT devices throughout the network. With the increased deployment and widely accepted standards of IoT systems, the IoT ecosystem often meets security issues such as access control, authorization, and verification. IoT devices generate and exchange the vast amount of safety-critical data and also, privacy-sensitive data, which leads the cyber attacks in the IoT environment [2, 3].

Traditional security methods are expensive for the overhead and energy consumption-rich IoT environment. Although, most of the existing security models are highly centralized, which are inappropriate for the IoT due to the nature of scalability and a single point of failure. IoT technology requires the security method which is to be scalable, lightweight, privacy safeguard, and distributed security [4]. Even though cloud computing technology enables the computation and storage of a vast amount of data in a centralized manner under the monitoring environment, it fails to protect the security and privacy of the data. Blockchain technology [5, 6] has proved its potential in financial applications such as Bitcoin which is the first cryptocurrency system. It empowers the IoT devices to improve the security and provide transparency by offering a scalable and decentralized environment to IoT devices and applications. Blockchain technology offers trustful transactions, cost reduction, and scalable security for the IoT environment [7]. Over the past years, the concept of blockchain technology has attracted as growing Peer-to-Peer (P2P) technology among millions of users for decentralized sharing and distributed computing. With the adoption of the cryptographic technology and without centralized data storage, the blockchain technology avoids the attacks from controlling the entire system [8, 9]. The combination of IoT and Blockchain technology provides several benefits such as lower operational cost, robustness against attacks and threats, and decentralized management [10, 11].

In the resource-constrained and untrustworthy IoT environment, securing access control is a challenging task in which access control solution involves authentication, authorization, and auditing. The existing access control methods such as Attribute-based Access Control (ABAC), Role-based Access Control (RBAC), and Access Control Lists (ACL) lack to provide the efficient and scalable solution for the IoT systems. In addition, the single point of failure due to the traditionally centralized authorization and the lack of transaction privacy due to the expressiveness nature of the decentralized smart contract are the major constraints in providing the access control solution for the IoT environment. However, in this work we use Zero-knowledge proof [12] is one of the cryptographic protocols, which plays a crucial role in preserving privacy without exposing the transactions to the miners in the smart contract. In accordance with, the proposed IoT security architecture focuses on modeling the privacy-aware decentralized and scalable access management with the contextual blockchain gateway, revocation manager, and non-interactive zero-knowledge proof based validation to ensure the resiliency and tamper-resistant access control model. The proposed architecture focuses on the non-interactive cryptographic protocol rather than interactively verifying the proofs to improve the transaction validation process in the distributed blockchain network.

The rest of the paper is organized as follows, section 2 discuss the literature review. Section 3 discuss the problem statement.

Section 4 discuss aims and objectives. Section 5 discuss the contribution of this work. Section 6 the design of our proposed solution. The steps involved in the proposed architecture are discussed and illustrates the pseudocode steps for the proposed access control model for the distributed IoT devices in Section 7 & 8 respectively. Sections 9 discuss and comparing the proposed system. The conclude the paper in Section 10.

2. Literature Review

Nowadays, providing the security for IoT is a quite challenging task due to the lack of standardization, the device heterogeneity, minimum resource capabilities, and the immense scale. Traditional security methods are inappropriate for the IoT environment. Hence, several research works have focused on integrating the Blockchain technology with the IoT technology to ensure security and privacy.

This work focuses on combining the blockchain, access control, and IoT to provide the security for the untrustworthy and distributed IoT environment. Accordingly, this section reviews the existing research works carried out the area above. A smart contract-based framework [13] comprises the multiple Access Control Contracts (ACCs), one Register Contract (RC), and one Judge Contract (JC). It provides distributed and trustworthy access control of the resource-constrained IoT environment. CapChain access control framework [14] hides the user identities and delegation information from the public to preserve the user privacy and enables the users to publicly share and delegate their access rights to the IoT devices. In addition, a Digital Asset Management using the blockchain (DAM-Chain) model [15] integrates the Attribute Based Access Control (ABAC) with the blockchain technology. It supports the distributed and flexible permission management and provides the transparent authorization process through the Transaction-based Access Control (TBAC).

The device hardware limitations lead to difficulty of deploying the blockchain technology in the IoT. To overcome this obstacle, an IoT ledger-based architecture [16] ensures the access control by maintaining the hash of the block headers and block ledgers for each IoT device in the resource-constrained IoT gateways. It provides the promising authorization solution with the concept of the information double signed by the gateway. However, dynamically updating the IoT ledger and storing the increased blockchain size in the resource-constrained gateway is critical for the large-scale environment. Moreover, FairAccess framework [17] stores the access control policies in a private blockchain based on the principle of the Role-Based Access Control (RBAC), which manages the access control policies in the IoT environment based on the smart contract operations. However, this access control management is not suitable for the numerous IoT contexts due to the only handling of the policy-based compatible systems. A blockchain-based IoT access control and authentication management solution [18] ensures the integrity, traceability, and accountability in a tamper-proof manner. However, providing the authentication for legitimate users alone among the huge number of end users and the IoT devices is a challenging factor due to the lack of maintaining the identity globally.

Control Chain architecture [19] establishes the secure connection between the users, devices, group of users and a group of the devices based on the assignment of the attributes with the decoder entity for the access control authorization. A blockchain based access control system [20] models the ciphertext-policy attribute-based encryption scheme for the access control with the dynamic attributes in the untrusted cloud environment without the involvement of the cloud service provider. Despite, blindly trusting the IoT-Cloud framework for authorization is an insecure process. To overcome this constraint, the IoT security architecture [21] involves the authorization and delegation model using the blockchain technology for the IoT-Cloud. It enables the users to inspect the operations of the access control and audit the authorization operations. A distributed access management system facilitates the access control of IoT devices in a scalable manner, which avoids the integration of the low-capability IoT devices in the blockchain through the management hubs [22]. However, it handles the direct data exchange between the devices only, which is insufficient for the distributed IoT devices due to the difficulty of receiving the direct request data exchange between devices in the IoT environment. To cope up with this, the blockchain-based dynamic access control scheme [23] dynamically generates the access policies for the data requests between the authenticated devices.

3. Problem Statement

In order to ensure the IoT security, there is an essential need of protecting the resources from the unauthorized access with the access rights of the subject. In the security services, maintaining the integrity and confidentiality of the resources is crucial. Accordingly, focusing on the access control policy is vital to address the security issues in the IoT applications. The traditional access control systems suffer from a single point of failure while adapting to the IoT security due to the existence of the centralized trust domain in the conventional mechanisms. The conventional access control standards and technologies have either adapted to the resource-constrained IoT environment or exploited distributed access control management approach for scalable IoT architecture. Although the blockchain technology ensures the trustworthy and decentralized access control, validating the locking scripts is a critical process in the resource-limited IoT objects. Owing to the low capability of the IoT objects, there is a higher possibility of compromising the devices by the adversaries. Hence, addressing the access control issues in the distributed and untrustworthy IoT environment is a challenging task. Several existing architectures resolve the access rights validation issues with the transparent and decentralized authorization process in IoT using the blockchain network. Despite, the adoption of blockchain technology for the IoT networks leads to the need for lightweight solutions.

4. Aims and Objectives

- To develop the distributed and scalable access control model for the untrustworthy and resource-constrained IoT environment.

- To ensure the resilient IoT security and to manage the unique identity of devices in a tamper-resistant manner**.**

- To maintain the trade-off between the transparency and privacy in the distributed IoT environment**.**

5. Contribution of the Work

- This work presents the IoT security architecture with a privacy-aware decentralized and scalable access management model that heavily relies on the blockchain gateway, decentralized revocation manager, and non-interactive zero-knowledge proof.

- The proposed architecture designs the blockchain gateway with the gateway administrator, context manager, and smart blockchain proxy, which ensures the dynamic authentication in the untrustworthy IoT environment.

- By utilizing the Smart contract that expresses the contextual access control policies, the proposed architecture takes authorization decision along with the knowledge of the revoked user list generated by the decentralized revocation manager.

• Instead of validating the transaction information in the public ledger, the proposed architecture applies the non-interactive zero-knowledge proof cryptographic protocol to improve the transaction privacy with the resilience among the blockchain nodes for the distributed and resource-constrained IoT devices.

6. Proposed Privacy-aware Decentralized and Scalable Access Management with Blockchain Gateway

Figure 1 shows the blockchain based access control model for the IoT devices.

With the aim of providing access control in IoT, this work presents an architecture with the principles of the decentralization, resilience, and scalable. As the rapid increase of the blockchain size over the time, storing the blockchain information in the constrained nature of IoT environment is difficult. Hence, the proposed decentralized and scalable access management system stores the access control information using the blockchain technology rather than accessing from the resource-constrained IoT devices. The proposed architecture involves a smart contract that enables all the operations of the access control system with the contextual blockchain gateway, decentralized revocation manager, and non-interactive zero-knowledge proof based validation. The architecture of the proposed system is illustrated in Fig. 2.

The access control involves three entities such as authentication, authorization, and auditing. The proposed approach only focuses on improving the works [16, 22] to model the IoT security architecture. The proposed model supports the IoT security for the large-scale environment with the decentralized and dynamic authentication, public ledger, and transaction validation. The proposed approach enhances the IoT ledger-based architecture [16] by maintaining the public ledger within the blockchain network rather than integrating the blockchain technology in the resource-constrained IoT gateway. The proposed approach directly connects the IoT devices with the blockchain network through blockchain gateway to ensure the dynamic authentication and auditing in the public ledger. The main component of the ‘Management hub’ in work [22] only transfers the data of the IoT devices to the blockchain nodes. Whereas, the proposed approach models the blockchain gateway with the ‘gateway administrator’, ‘context manager’, and ‘smart blockchain proxy’ instead of modeling the IoT security architecture with the ‘management hub’ interface. The blockchain gateway intends to prevent both the user preferences and unauthorized access of the resources. The access control policies rely on the device manager and the blockchain gateway, which targets on improving the authorization. The user preferences and privacy are inter-linked with each other, include the restrictions on the exchanged personal information, specific rules to the subjects, and the context parameters such as location details.

The proposed architecture considers a set of features such as resource-constrained IoT device, gateway usage, and multi-layer IoT security architecture. In the context of the proposed architecture, the perception layer includes the IoT devices, the transportation layer manages the IoT gateways and blockchain gateways, and the application layer represents the IoT applications and cloud database storage which is integrated with the blockchain network of the transportation layer [16]. The components of the proposed architecture included the IoT network, IoT gateway, blockchain gateway, blockchain network.

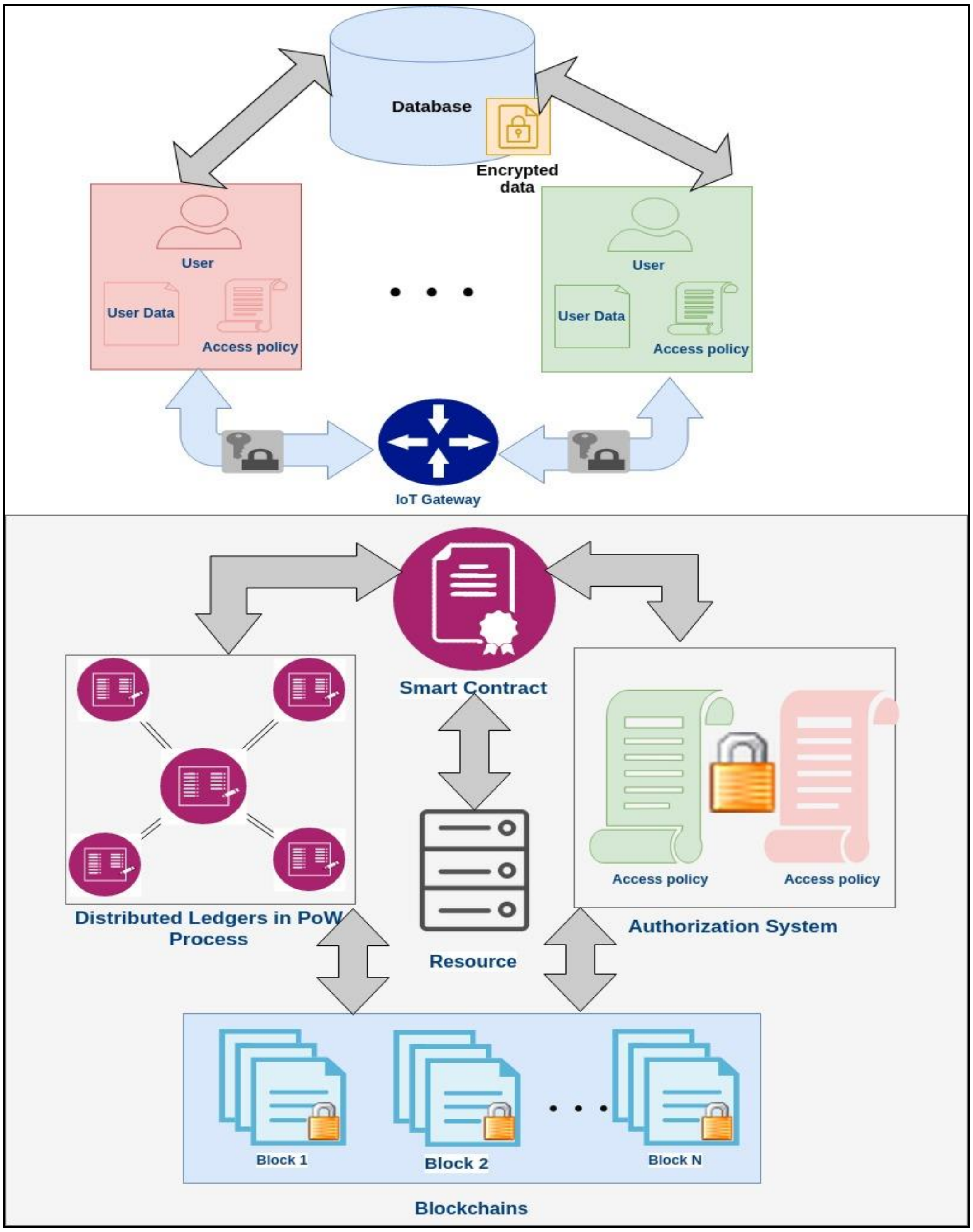

Fig 1. Blockchain based access control model for the IoT devices.

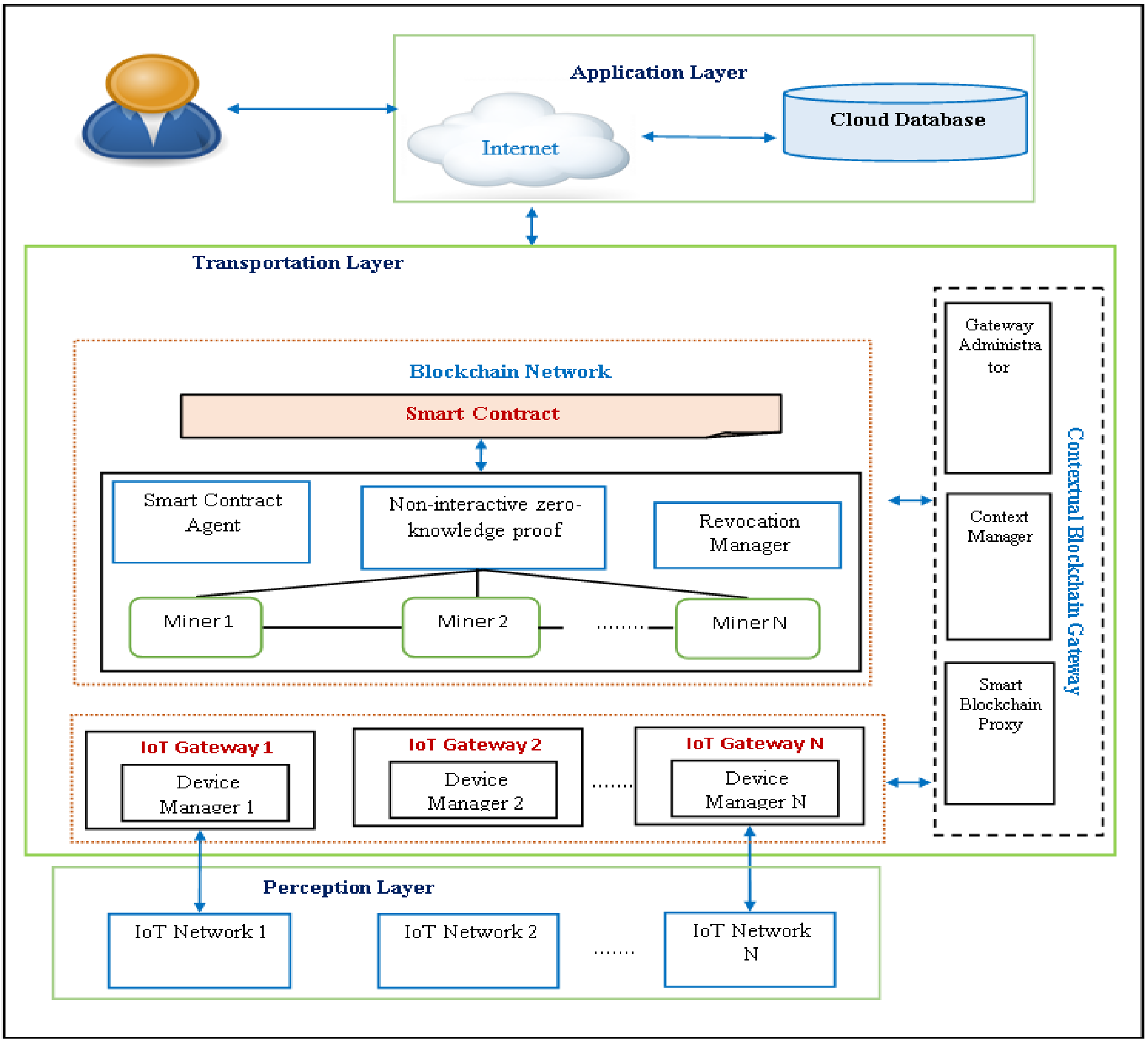

Fig 2. The architecture of the proposed system privacy-aware decentralized and scalable access control management for IoT environment.

A. IoT network: An IoT network includes sensors or actuators, which transmits the data to temperature, humidity, and motion sensors or receives the information from the gateway. The perception layer enables the full-duplex communication between the IoT devices and gateways. The devices in the IoT network have limited computational memory, energy, and power resources. With the aim of maintaining the global uniqueness for each IoT device in the blockchain network, the architecture employs the existing cryptographic techniques that generate a public key for each device.

B. IoT gateway: IoT gateways play a crucial role in interconnecting the heterogeneous IoT devices, which stores the data acquired from the devices. In the IoT network, Constrained Application Protocol (CoAP) ensures the secure communication channel using the Datagram Transport Layer Security (DTLS) protocol. In the proposed architecture, IoT gateway manages the devices with the blockchain gateway with the help of device manager. The device manager establishes the direct connection of the devices with the blockchain network to maintain the chain of nodes with transaction validation. In essence, the device manager is responsible for managing user preferences and the addresses of the device. After obtaining the address of the smart contract, the device manager provides the obtained address to the gateway administrator in the blockchain gateway for attaching the device with its unique identity.

C. Blockchain gateway: Blockchain gateway is responsible for protecting the maintained user preferences to prove the tamper-resistant transaction on the blockchain network. After receiving the user preferences of the devices from the IoT device manager, the blockchain gateway stores and also, preserves the preference information in the blockchain network. In the proposed architecture, the blockchain gateway comprises the gateway administrator, context manager, and smart blockchain proxy.

1) *Gateway administrator:* In the blockchain gateway, the administrator creates a smart contract and establishes the connection between the gateway and an IoT device. The gateway administrator connects the smart contract of the gateway with the device manager of the IoT gateway to fetch the user preferences and the device information.

Context Manager: In the blockchain gateway, the context manager is responsible for storing the contextual information of the inputs, IoT devices, and the processed data to facilitate the authorization decision. In accordance with, the context manager finds the information requested by the device with the access rules of the corresponding device stored in the gateway to allow or deny the access.

2) *Smart blockchain proxy:* In the blockchain gateway, the smart proxy server is an interface to transmit the data acquired from the devices to the blockchain network. It establishes the connection with the nearest node such as miner in the blockchain-based infrastructure. The miner node stores a copy of the blockchain and allows the Remote Procedure Call (RPC) to listen to the requests. The smart blockchain proxy translates the CoAP messages of the IoT devices into understandable JSON-RPC messages for the miner. The IoT devices request the access information from the blockchain network through blockchain gateway especially, the smart blockchain proxy. Compared to the IoT gateway, the blockchain gateway contains the nodes with high-performance characteristics, which can process the multiple simultaneous requests.

D. Blockchain network: The proposed architecture employs Ethereum private blockchain to provide reliable and secure transactions. In the blockchain network, the miners maintain the network stability and security by validating the transactions and maintaining the multiple copies of the blockchain. The miners in the blockchain network employ the blockchain interface to globally access the access control policy of the IoT device, which is decentralized in nature.

Smart contract: In the blockchain network, the smart contract contains all the operations allowed in the access management system and triggers the operations through the blockchain transactions. The blockchain network provides the global access of the operations in the access management system and the smart contract.

Smart contract agent: In the proposed architecture, the smart contract agent is one of the blockchain node, which is responsible for deploying the smart contract in the blockchain network. The smart contract agent receives the address of the smart contract in the blockchain network and acts as the owner of the smart contract throughout the processing of the access control system.

Revocation manager: In the blockchain network, revocation manager is responsible for managing a certain number of mined blocks and time of the operations in the smart contract. To avoid the revocation in terms of accessing the restricted information by the unauthorized attacker, the revocation manager spreads the revoked operation to the miner nodes of the blockchain network rather than waiting for the permission from the edge of the network. It automatically updates the revoked user list in the smart contract operations by repeatedly validating the transactions using the PoW consensus algorithm with the help of the context manager.

7. Process of the Proposed access Control Model in the IoT Architecture

The proposed architecture ensures the privacy-aware decentralized and scalable access management for the IoT devices. The steps involved in the proposed architecture are discussed as follows:

Step 1: IoT device as the producer establishes the connection in the blockchain network.

Step 2: In the IoT gateway, the device manager manages the corresponding device address and user preferences.

Step 3: In the contextual blockchain gateway, the gateway administrator establishes the connection between the device and smart contract and fetches the corresponding address of the smart contract.

Step 4: Smart contract registers the device and assigns the access control rule for the device regarding the resource.

Step 5: Consumer or User sends the access request to the device through the blockchain gateway for accessing the resource.

Step 6: The IoT device or producer sends their smart contract ID to the user to access the smart contract for accessing the requested resource

Step 7: By utilizing the smart contract address received from the producer, the user sends the access request to the blockchain gateway to receive access from the blockchain network.

Step 8: In the blockchain gateway, the context manager analyzes the user preferences using the information stored in the device manager.

Step 9: After analyzing the user preferences and also, using the blockchain Public Key Infrastructure (PKI), the blockchain gateway provides authentication for the requested user.

Step 10: In the blockchain network, the blockchain gateway stores and updates all the transactions with a unique identification of the device in the public ledger of the smart contract.

Step 11: With the help of the PoW algorithm, the proposed architecture validates the authorization token that comprises the contextual access control policies. During the validation of the transaction within the smart contract, it employs the non-interactive zero-knowledge proof protocol to balance the trade-off between the transparency and confidentiality.

Step 12: According to the proposed access control flow, the proposed architecture provides the resource access to the user after verifying the access rights of the corresponding user.

Step 13: If any revocation occurs in the blockchain network, the decentralized revocation manager monitors the transaction and generates the revoked user list. After generating the list, it dynamically updates the revoked user list in all the nodes of the smart contract and the blockchain gateway.

```
Input: IoT device as producer and consumer (i), Access Request
Output: Secure access response
While the IoT devices require the decentralized and secure transaction do
for all the IoT devices belongs to the smart contract ID  do
    Smart contract generate access control policies for each device
        if the request is from the user then
            Verify the credentials (Cr(i)) and contextual factors (C(i))
                if (Cr(i)&&C(i)==Info(i) in Device manager) then
                    Provide authentication using PKI
                else
                    Deny the user
                endif
        endif
endfor
for all the authenticated users do
    Perform the transactions in smart contract
    Add the new block for transaction of each device with unique identity
        for all the transactions stored in the public ledger do
            Apply non-interactive zero-knowledge proof protocol
                if (access policies(i)==policies(i) in smart contract) then
                    if any revocation occurs then
                        Generate revoked user lists
                        Update the revoked user lists to all the miners
                    endif
                        if (new block is added) then
                            Apply PoW consensus method
                            Validate transaction by miner to prove the ownership
                        endif
                    Provide authorization for the requested resource
                else
                    Deny the request
                endif
        endfor
endfor
endwhile
```

Fig 3. Pseudocode for the Proposed Access Control Model.

8. Pseudocode Steps for the Proposed

Figure 3 illustrates the pseudocode steps for the proposed access control model for the distributed IoT devices. Initially, the proposed algorithm explains the dynamic authentication based on the credentials, contextual factors, and PKI in the decentralized smart contract through the contextual blockchain gateway. After authenticating the users, the proposed architecture validates the access policies generated by the smart contract with the PoW consensus algorithm. In order to prove the data ownership, the consensus model enforces the miners to validate the transaction in the smart contract repeatedly. According to the proposed privacy-aware architecture, the transaction validation process relies on the non-interactive zero-knowledge proof protocol. Finally, the proposed architecture provides the authorization to the user for accessing the requested resource alone on the blockchain network.

9. Discussion and Comparison

The proposed approach enhances the existing access control management system [22] by modeling the IoT security architecture with the contextual blockchain gateway, decentralized revocation manager, and the zero-knowledge proof based validation. The proposed approach employs the smart contract that becomes a promising platform to accomplish the distributed and trustworthy access control in the resource-constrained IoT environment.

The contextual blockchain gateway incorporates the gateway administrator, context manager, and smart blockchain proxy, which enforces the dynamical authentication based on the contextual factors and blockchain PKI scheme. Moreover, the proposed architecture models the revocation manager that dynamically updates the list of revocation users in the distributed blockchain network. With the assistance of non-interactive zero-knowledge proof protocol, the proposed approach hides the transaction information among the nodes in the blockchain network. Thus, it ensures the trade-off between the transparency and confidentiality by partially trusting the nodes in the smart contract. We discussion and compared the performance between the proposed and existing access control management models from the perspective of the research objectives or performance metrics like Security, Scalability, Transparency and Privacy. In existing access control management system [22] ensures the IoT security with limited communication overheads through decentralized access control system in light-weight IoT scenarios while proposed system provides the tamper-resistant resource access through revocation manager and Blockchain gateway that ensures context-based dynamic authentication and authorization in light-weight IoT scenarios. In addition, existing system [22] ensures scalability access management using decentralized management hubs and consensus process while proposed system provides scalability access management using decentralized blockchain gateway, consensus process, and unique identifier. Moreover, the transparency in the existing access control management system [22] eventhough the system hides the location of the IoT devices, there is a possibility of learning the transaction patterns by the nodes in the smart contract while proposed system supports the resilience by partially trusting the manager during the transaction validation with the Zero-knowledge proof protocol. The privacy in existing access control management system[22] lacks to focus on the data confidentiality constraint in the public blockchain while proposed system ensures the trade-off between the transparency and privacy by employing the Zero-knowledge proof protocol in the smart contract.

10. Conclusion

This work has presented the IoT security architecture with the distributed and scalable access control management. The proposed architecture heavily relies on three components include the contextual blockchain gateway, decentralized revocation manager, and non-interactive zero-knowledge proof based validation. The contextual blockchain gateway model ensures the dynamic authentication and authorization by analyzing the contextual factors of the users and self-enforcing policies in the smart contract. The revocation manager updates the revoked user lists in the blockchain network to avert the resource accessed by the unauthorized users. Moreover, to ensure both the transparency and the confidentiality, the proposed architecture employs the non-interactive zero-knowledge proof cryptographic protocol in the smart contract. Thus, the proposed system provides the privacy-aware distributed and scalable access control management for the resource-constrained IoT devices.

References

[1] **Miorandi, Daniele, Sabrina, Sicari, Francesco De Pellegrini** and **Chlamtac**, **Imrich,** "Internet of things: Vision, applications and research challenges", *Ad hoc networks*, **10**(7):1497-1516, 2012.

[2] **Sabrina, Sicari, Rizzardi, Alessandra, Grieco, Luigi Alfredo** and **Coen-Porisini**, **Alberto,** "Security, privacy and trust in Internet of Things: The road ahead", *Computer networks*, 76:146-164, 2015.

[3] **Rodrigo, Roman, Zhou, Jianying** and **Lopez**, **Javier,** "On the features and challenges of security and privacy in distributed internet of things", *Computer Networks*, **57**(10): 2266-2279, 2013.

[4] **Alaba Fadele Ayotunde**, **Mazliza Othman, Ibrahim Abaker Targio Hashem** and **Faiz Alotaibi**, "Internet of things security: A survey", *Journal of Network and Computer Applications*, **88**:10-28, 2017.

[5] **Puthal, Deepak, Nisha Malik, Saraju P. Mohanty, Elias Kougianos** and **Gautam Das**, "Everything You Wanted to Know About the Blockchain: Its Promise, Components, Processes, and Problems", *IEEE Consumer Electronics Magazine*, **7**(4):6-14, 2018.

[6] **Miraz, Mahdi H.** and **Maaruf Ali**, "Applications of Blockchain Technology beyond Cryptocurrency", *arXiv preprint arXiv* 2018.

[7] **Ali, Dorri, Kanhere, Salil S.** and **Jurdak**, **Raja,** "Blockchain in internet of things: challenges and solutions", *arXiv preprint arXiv*, 2016.

[8] **Ali, Dorri, Kanhere, Salil S.** and **Jurdak**, **Raja,** "Towards an optimized blockchain for IoT", *ACM Proceedings of the Second International Conference on Internet-of-Things Design and Implementation*, pp.173-178, 2017.

[9] **Miraz, Mahdi H.** and **Maaruf, Ali,** "Blockchain based Enhanced IoT Ecosystem Security", *arXiv preprint arXiv*, 2018.

[10] **Amine, Ferrag Mohamed, Derdour, Makhlouf, Mukherjee, Mithun, Derhab, Abdelouahid, Maglaras, Leandros** and **Janicke**, **Helge,** "Blockchain Technologies for the Internet of Things: Research Issues and Challenges", *arXiv preprint arXiv*, 2018.

[11] **Ana, Reyna, Martín, Cristian, Chen, Jaime, Soler, Enrique** and **Díaz**, **Manuel,** "On blockchain and its integration with IoT. Challenges and opportunities", *Future Generation Computer Systems*, 2018.

[12] **Tommy, Koens, Ramaekers, Coen** and **Wijk**, **Cees van,** "*Efficient Zero-Knowledge Range Proofs in Ethereum*", 2017.

[13] Zhang Yuanyu, Shoji Kasahara, Yulong Shen, Xiaohong Jiang, and Jianxiong Wan, "Smart Contract-Based Access Control for the Internet of Things", *arXiv preprint arXiv*, 2018

[14] **Le, Tam** and **Matt W. Mutka**, "CapChain: A Privacy Preserving Access Control Framework Based on Blockchain for Pervasive Environments", *IEEE International Conference on Smart Computing (SMARTCOMP)*, pp.57-64, 2018.

[15] **Yan, Zhu, Qin, Yao, Zhou, Zhiyuan, Song, Xiaoxu, Liu, Guowei** and **Chu**, **William Cheng-Chung,** "Digital Asset Management with Distributed Permission over Blockchain and Attribute-Based Access Control", *IEEE International Conference on Services Computing (SCC)*, pp.193-200, 2018.

[16] **Castagna, Lunardi Roben, Michelin, Regio Antonio, Neu, Charles Varlei** and **Zorzo**, **Avelino Francisco,** "Distributed access control on IoT ledger-based architecture", In *NOMS 2018-2018 IEEE/IFIP Network Operations and Management Symposium*, pp.1-7, 2018.

[17] **Ouaddah, Aafaf, Anas Abou Elkalam** and **Abdellah Ait Ouahman**, "Towards a novel privacy-preserving access control model based on blockchain technology in IoT", In *Europe and MENA Cooperation Advances in Information and Communication Technologies*, pp.523-533, Springer, Cham, 2017.

[18] **Ourad Abdallah Zoubir, Boutheyna Belgacem** and **Khaled Salah**, "Using Blockchain for IOT Access Control and Authentication Management", In *International Conference on Internet of Things*, pp.150-164, Springer, Cham, 2018.

[19] **Ahlert, Pinno Otto Julio Abed Gregio, Andre Ricardo** and **De Bona**, **Luis CE,** "ControlChain: Blockchain as a Central Enabler for Access Control Authorizations in the IoT", IEEE Global Communications Conference on *GLOBECOM*, pp.1-6, 2017.

[20] **Ilya, Sukhodolskiy** and **Zapechnikov**, **Sergey,** "A blockchain-based access control system for cloud storage", *IEEE Conference of Russian on Young Researchers in Electrical and Electronic Engineering (EIConRus)*, pp.1575-1578, 2018.

[21] **Nachiket, Tapas, Merlino, Giovanni** and **Longo, Francesco,** "Blockchain-Based IoT-Cloud Authorization and Delegation", *IEEE International Conference on Smart Computing (SMARTCOMP)*, pp.411-416, 2018

[22] **Novo Oscar,** "Blockchain Meets IoT: an Architecture for Scalable Access Management in IoT", *IEEE Internet of Things Journal*, 2018.

[23] **DongYeop, Hwang, Choi, JungYong** and **Kim, Ki-Hyung,** "Dynamic Access Control Scheme for IoT Devices using Blockchain", *International Conference on Information and Communication Technology Convergence (ICTC)*, pp.713-715, 2018.

الخصوصية – وإدارة التحكم في الوصول اللامركزية والقابلة للتطوير لبيئة عمليات إنترنت الأشياء

أبرار عمر الخميسي و **فتحي البرعي**

كلية الحاسبات وتقنية المعلومات، جامعة الملك عبدالعزيز، جدة، المملكة العربية السعودية

aalkhamisi0034@stu.kau.edu.sa

المستخلص. في السنوات الأخيرة، تلعب إنترنت الأشياء دورًا حيويًا في أنشطتنا اليومية. وبسبب زيادة عدد نقاط الضعف في أجهزة إنترنت الأشياء، يصبح الأمن أمرًا حاسمًا في بيئة إنترنت الأشياء غير الجديرة بالثقة. ويعتبر التحكم في الوصول أحد أهم الشواغل الأمنية، ومع ذلك، فإن تنفيذ آليات التحكم في الوصول التقليدية في الطبيعة المحدودة الموارد لأدوات إنترنت الأشياء يعتبر مهمة صعبة. مع ظهور تكنولوجيا blockchain، ركزت العديد من الأبحاث الحديثة على تبني blockchain في إنترنت الأشياء لحل مشكلات الأمان. على الرغم من أن دمج blockchain في سياق إنترنت الأشياء محدودة الموارد أمر صعب. للتغلب على هذه العقبات، يقدم العمل المقترح بنية أمان لإنترنت تقنيات علم الخصوصية لضمان التحكم في الوصول استنادًا إلى عقد ذكي لأجهزة إنترنت الأشياء المقيدة والموزعة. يشتمل تصميم البنية المقترحة على ثلاثة مكونات رئيسية، مثل بوابة blockchain السياقية، ومدير الإلغاء اللامركزي، والتحقق من عدم الإثبات على أساس المعرفة التفاعلي. من خلال نمذجة بوابة blockchain السياقية، تضمن البنية المقترحة المصادقة الديناميكية والترخيص استنادًا إلى المعلومات السياقية وسياسات الوصول. مع ارتباط مدير الإبطال اللامركزي في العقد الذكي، فإنه يمنع الوصول إلى الموارد من المستخدمين غير المصرح لهم عن طريق إنشاء وتحديث قائمة المستخدمين المبطونة بشكل ديناميكي لجميع العقد في العقد الذكي. علاوة على ذلك، تستخدم البنية المقترحة بروتوكول التشفير غير التفاعلي ذو المعرفة الصفرية لضمان خصوصية المعاملة داخل العقد الذكي. وبالتالي، فإنه يحافظ على المفاضلة بين الشفافية والخصوصية مع ضمان الأمن لبيئة إنترنت الأشياء الموزعة.

الكلمات المفتاحية: إنترنت الأشياء، blockchain، عقد ذكي، والتحكم في الوصول، التشفير غير التفاعلي ذو المعرفة الصفرية.