Blockchain-based authentication for IoT

Alaa Alsubhi. Jawaher Alhrthi and Wajdi Alhakami
College of Computer and Information Technology,
Taif University, Taif, Saudi Arabia

Summary
Correspondence security between IoT devices is a significant concern, and the blockchain makes the latest difference by reducing this matter. In the blockchain idea, the larger part or even all organization hubs check the legitimacy and precision of traded information before tolerating and recording them, regardless of whether this information is identified with monetary exchanges or estimations of a sensor or a confirmation message. In assessing the legitimacy of a traded information, hubs should agree to play out an uncommon activity. The chance to enter and record exchanges and problematic cooperation with the framework is fundamentally decreased. To share and access the executives of IoT devices data with disseminated demeanour, another confirmation convention dependent on block-chain is proposed, and it is guaranteed that this convention fulfils client protection saving and security. This paper highlights the recent approaches conducted by other researchers to secure the Internet of Things environments using blockchain. These approaches are studied and compared with each other to present their features and disadvantages.

Keywords: *Blockchain, IoT, authentication, security*

1. Introduction

In the past few years, the term blockchain had been repeated frequently. This is due to the popularity of its first application, which is Bitcoin. Although the idea of blockchain is not new but rather dates back to the beginning of the nineties as the emergence of Bitcoin, blockchain returned to the surface. Many researchers, big companies, and financial institutions are investing their time and financial resources to develop a new range for their business by involving blockchain technology [1].

Away from cryptocurrencies and financial transactions, there are good applications are linked with IoT, such as cloud storage, digital ID, and so on [2]. Blockchain is a distributed ledger technology that combines with IoT to make machine-to-machine transactions possible. Also, IoT enabled machines over the Internet to send data to private blockchain networks. So, in our paper, we aim to study the different ways to implement authentication for the blockchain in IoT.

This paper is organised into 5 sections; section 2 presents the background of blockchain technology and its architecture. Section 3 discusses the recent approaches conducted by other researchers for adapting the blockchain for securing the IoT environment. These existing security approaches for protecting the IoT are analysed in section 4. the paper is concluded in section 5.

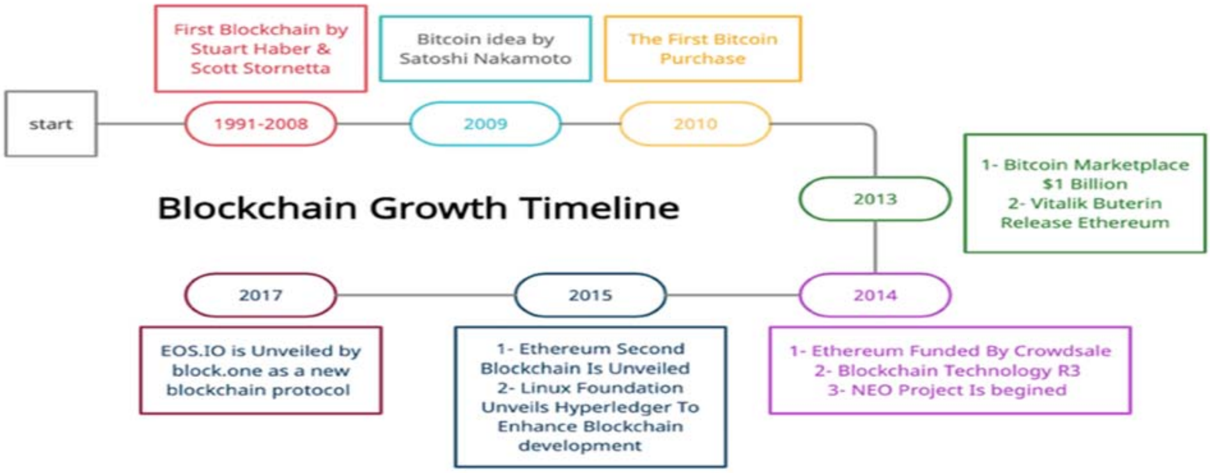
2. Background

Blockchain history starts in the early 1990s. It has caused a revolution in the past years because big blockchain innovation was bitcoin (digital coin), as shown in Fig. 1, exhibiting the Blockchain growth Timeline [3]. So, in simple word, the Blockchain is the digital record for the transactions. Its name comes from its structure where the individual records named blocks are related together in one list named chain. Every transaction added to the blockchain is validated by several devices [4]. Blockchain is a digital technology based on a huge cloud database, through which people can complete transactions or transfer money through a network of decentralized computers scattered around the world. Blockchain is likened to a general ledger in accounting science because it is a public database in which digital information is stored for exchanges. Every cluster of nodes in the Blockchain functioning on a peer-to-peer (P2P) network system. There are 4 different types of blockchains, two of them considered as primary types (Private and Public) while the others recognised as Consortium and Hybrid blockchains [1,5,6].

1) Public: The basic use and anyone can join the network of nodes for mining and exchanging cryptocurrencies (such as Bitcoin).
2) Private: It is limited access; The user needs to have permission to access the blockchain only in a locked network. Client access to it with no need for the third party by executing. Like the public but small and limited network.
3) Consortium: It is semi-decentralized where not just one organization but multiple organizations manage the network (such as R3).
4) Hybrid: It is a collection of the public and the private using the features of both types. This makes the system more flexible..

In general, blockchain has several features listed as following [16]:

Manuscript received May 5, 2024
Manuscript revised May 20, 2024
https://doi.org/10.22937/IJCSNS.2024.24.5.22


start
1991-2008
First Blockchain by Stuart Haber & Scott Stornetta
2009
Bitcoin idea by Satoshi Nakamoto
2010
The First Bitcoin Purchase
Blockchain Growth Timeline
2013
1- Bitcoin Marketplace $1 Billion
2- Vitalik Buterin Release Ethereum
2014
1- Ethereum Funded By Crowdsale
2- Blockchain Technology R3
3- NEO Project Is begined
2015
1- Ethereum Second Blockchain Is Unveiled
2- Linux Foundation Unveils Hyperledger To Enhance Blockchain development
2017
EOS.IO is Unveiled by block.one as a new blockchain protocol

a. Transparency: This means that the information can be viewed anywhere and anytime (unlike the normal encryption methods that completely block the information).

b. Privacy: The sender of the information can conceal his identity to protect himself from anyone that wants to track his transactions.

Fig. 1: Summary of the blockchain Growth [3].

c. Distributed Technology: Unlike traditional databases. Which depends on storing its data on one or several servers, which makes it easy to penetrate. This technology does not allow this to happen because it depends on storing data on distribution. This means that the data is stored in multiple devices on a distributed network by nodes. Each node creates a copy of the data, so the database failure will not occur if the connection is interrupted. Besides, it does not need an intermediary, provides better security and safety, Immutability, etc.

2.1 Blockchain-based architecture

According to [1, 6], they considered blockchain architecture as an IoT architecture with 3 layers. Fig. 2 shows the blockchain layers:

1) The top layer (Application): The final service developed that the company does by using blockchain. It also provides various interfaces for the users by some devices to visualizing the data.

2) The middle layer (Service): It is where blockchain built the application by the distributed ledger and has all significant modules regulated by the common services needed to apply all features. This layer split into the lightweight node and private blockchain [6]:
Lightweight nod: It is also known as Light nodes or thin nodes. It has a similar objective to the full nodes. Still, instead of keeping a full history of a blockchain, it keeps a block header that requires support and inquiry about the validity of the prior transactions. The block's header carries a detailed summary of a specific block and contains information related to the particular previous block linked to it [7]. The lightweight nodes do not store the main data but raise the speed of implementation of the asymmetric cryptographic algorithms. Many new processors exist, but (ARM Cortex-M series) is the best choice [6].

3) Physical layer (Bottom): it is made up of sensors, microcomputers, and actuators. Here is the network represented by some of the nodes that use their power to computational the consensus mechanism or store, refuse, and confirm the new transactions.

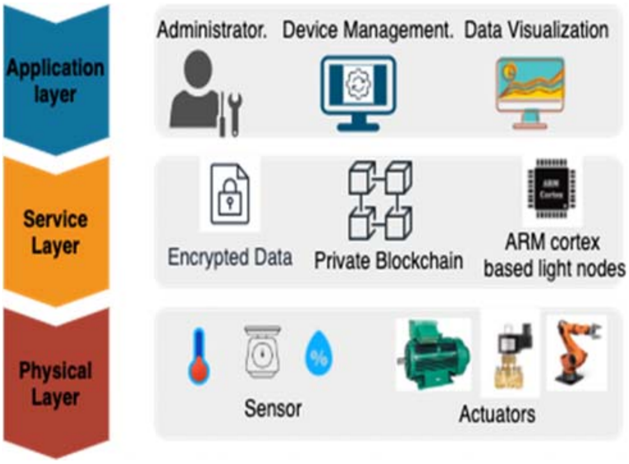


Fig. 2: Architecture of the Blockchain [6].

2.2 System Model

The Blockchain model is an open, secure, and appropriated exchange record innovation that can deftly adjust to complex and change organisational conditions. The disappointment of a few nodes doesn't influence the steady activity of the framework. Appropriated confirmation between nodes forestalls noxious nodes from attacking the organization. Regardless of whether few nodes are undermined, the record won't be altered. In a multi-hub organization, the character data of the devices should be enlisted in the blockchain each time a new device is added. Every device's ID, public key, the hash of basic information, and other data are put away in the blockchain record. Simultaneously, every device is a hub in the blockchain network, and the agreement instrument makes sure that every hub stores similar data. When distributed correspondence happens, public-key cryptography can be utilized for character validation between IoT devices [8].

1) Roles of nodes: Nodes are separated into consensus nodes and non-consensus nodes as per the various capacities in the consent chain. Consensus nodes take part in agreement measure, create squares, and broadcast squares to non-consensus nodes.
2) Device roles: In the IoT, each node should be involved in the blockchain. Every device produces a vital pair from its security key module. The private key is scrambled and put away locally, and the public key is put away in a blockchain record. In the wake of accepting the enrollment data, the agreement hub sees it as an enlistment occasion, produces a block after consensus with other consensus nodes, and synchronizes to other non-consensus nodes. Simultaneously, enlistment needs to store the hash estimation of basic information, for example, the neighbourhood arrangement records and firmware in the blockchain, to get ready for the resulting information honesty check [9].
3) Data transmission of blockchain: The communication among devices and square chain is completed as exchange. We characterized three various types of exchanges by shrewd agreements. The brilliant contracts get demands from devices and perform various activities like composition and perusing in the block-chain as per various solicitations.

3. Literature Review

Many researchers have conducted several recent studies to secure the IoT environment by adopting Blockchain techniques to ensure successful communication. These approaches are discussed as follow:

In [6], authors use blockchain with IoT to improve the overall system's security, especially in modern industry. In this architecture, the focus will be on how to access the valuable sensor and actuator data, private and lightweight blockchain. The body of the system using blockchain draws on the performance of ARM Cortex-M processors for asymmetric cryptography. However, the usage of the PoAh algorithm to implement a resource- and energy-efficient authentication mechanism. All network devices can create blocks in PoAh, but only trusted nodes can authenticate them. Findings from a study of blockchain with IoT technology which used User clients and associated IoT devices are registered in the blockchain network during the initialization process to show that the cumulative results of service execution time suggest that the proposed blockchain platform performs satisfactorily for each activity. The advantages of this system are that using IoT with blockchain is easy and stable for implementation. In addition, the blockchain mechanism allows the users that have access to a private network, not any unknown party can alter the blockchain. Finally, build this system with ARM Cortex M4 processors with STM32F427 development boards consume low power.

In [10], Blockchain technology is being developed by P. Houshyar et al. to address the privacy and security challenges in the IoT. The proposed solution for the security challenges in the IoT is the architecture based on a multi-layer blockchain that depends on the concept of K-unknown clusters within IoT network through many algorithms, like the clustering algorithm and that enhances the coverage, minimizes the network load, and energy. In addition, the open-source Hyperledger Fabric Blockchain framework findings from a study of this model, which used to communicate with each other securely, base stations use a global blockchain. Furthermore, this model is a proposed great option for supporting ultra-reliable low latency massive machine type communication while using the capabilities and effectiveness of the cellular system under 5G networks. Besides, this implementation for this model shows many advantages like using the algorithms (K-unknown clusters within IoT network and open-source Hyperledger Fabric), which improve the efficiency of communications through the peer-to-peer nature of blockchain communication and maps it with enhanced integrity and protection. Moreover, In the security domain, using this model is the best solution for framework confidentiality, authentication, heterogenicity, availability, and network scalability. Unfortunately, this study has a drawback; it is affected by blockchain configuration like the number of users, endorsing nodes, the number of channels, and block size. Hence, finding a solution for latency affected by blockchain configuration will help improve the proposal.

In [11], A. Ahmed, and M. Aabid provided a solution to solve the balance between the device's security in the IoT and the IoT network openness by the blockchain technology. They suggested a system that designed lightweight IoT devices and extra security measures by deployed difficulty parameters using java language. Their experiment goes through 3 factors:

a) Difficulty Parameter and Mining the Complexity: Via calculation, the true hashing value is specified by the value of the difficulty parameter. To make it easy and get free error results, they published one transaction block for the following results. According to the number of mined blocks (500 blocks), the average number of iterations also increased as the increased of difficulty parameter. And the average number of iterations appropriate with the equation domain.
b) Block Size and Mining Complexity: The block size is the decisive factor that impacts both mining complexity and processing time. As the block size increased, the hashing time complexity of mining blocks (100) also increased. And the average number of iterations appropriate with the equation domain.
c) Comparative Analysis of different Hashing Algorithms: By choosing a proper hashing algorithm, it is hard to work because it affects different network parameters. Their system looks at various factors to avert some issues since they work with lower memory and lower power of IoT devices. They try various algorithms to mining 8000 blocks like SHA-224, SHA- 256, SHA-512 (took more execution time), and SHA-384. Setting the hashing algorithm aside, as the increased difficulty parameter, the time complexity of mining blocks also increased. In the end, they found that higher difficulty parameters joint with the algorithm of the faster hashing produce the best solution and that because the devices together with the minimum computational power and the requirements of the memory. So, there is a barter between the output size of the hashing algorithm and security. They noticed smaller hash size is more suitable for the storage memory, but it can be easy to calculate and breached. According to that, hashing algorithms and smaller output sizes must be linked by larger difficulty parameters for the time complexity reduced.

In [12], M. Sudip et al. introduce a lightweight consensus algorithm called Proof-of-Authentication (PoAh), since the blockchain network calculation requests a great amount of energy also the typical transactions are slow than leads to some problems. They implemented on resource-constrained IoT edge nodes and evaluated in terms of latency and energy consumption. PoAh used the MAC address of every node in the network to reach the consensus. They evaluate the PoAh performance according to the consumption during block validation, latency, energy, and addition. They classified the nodes (N) of the blockchain into (Sensor-nodes (S), Aggregator-nodes (A), and Trusted-nodes (T)). Every N= 1 A/T and K number of S where S carried the MAC address. A/T has a list of authenticated S. The A creates a block holding the data, identical timestamps, and its MAC address, then send it over to the network. The main defy is computationally expensive operations implicated with consensus algorithm. The main effect of lightweight PoAh is minimum latency and energy consumption. According to their experiment results, the average latency during block validation was 29.35 ms. The energy used through block validation was 44.31 mJ. which is an improvement compared to classical methods of validates the blocks. Proof of Stakes (PoS) in the better case need 1second (slower 20 times compering to the maximum latency). As a result, the blockchain ingrained quality support on raising the security and translucent in several applications and services. Additionally, both the energy consumption and latency are reduced notably. The decrease in the latency allows many applications and services that time is important.

In [14], the authors propose a decentralized authentication and access control system for lightweight internet of things devices that can be used in various scenarios. They propose a novel authentication and access control framework for IoT, allowing safe communication between devices from the same IoT system and devices from different IoT systems. The proposed mechanism is built on blockchain technology to take advantage of its cryptographic properties and distributed existence, and fog computing is used to fix latency issues. Security specifications and an attack model, in particular, are defined to evaluate and test the approach's ability to meet these requirements. The system refers to two layers, device layer and fog layer, depending on three types of communications device-to-fog, fog-to-fog, and device-to-device communication. The results are analyzed; confidentiality, integrity, identity, no repudiation, authentication, and mutual authentication are among the criteria. It was also assessed for both power consumption and execution time. There are two interesting advantages to this approach. Firstly, the mechanism is fast, taking only 69 ms to generate and submit the authentication request. Secondly, it scales well in terms of the number of devices; since fog nodes perform the registration process and the calculation complexity is independent of the number of devices, the model is unaffected by an increase in the number of connections and registration requests. However, one drawback of the proposed solution is using the Ethereum blockchain for the assessment, which adds additional delay.

In [15], the authors mentioned that when a device connects to the network, it requires authentication and authorization before the access succeeds. Even though the device circling from one network to another, it can't access that network area until it authenticates once more. This repetition leads to increase operation costs, make the network hacked easily, and safety is quite reduced. Most authentication used is the classic KPI technology and digital certificates, but it has some disadvantages as the rising cost and management complexity. So, they suggested a cross-domain authentication strategy for the blockchain and made blockchain networks created from multiplied blockchains through IBC (inter-blockchain communication protocol). When devices move from one network to another network, blockchains communicate and transfer the information (reduce the number of authentication).

They proposed Cosmos network architecture: a heterogeneous network that helps cross-chain interactions. It is collected of a lot of independent blockchains in parallel. The created network is named zones, and various zones are communicated via IBC. The first blockchain is called a cosmos hub. Zones need to connect only to the Hub, not to the other zones because when Zone started a connection with Hub, it can automatically access other Zones in the same Hub. They did two experiments on the cosmos network model:

1- By implementing a multichain system and performed cross-domain arrival, the throughput of the system can deal with unit time with several authentication cross-domain.
2- They measured the desired transmission overhead when multiple cross-area authentications extradited the identical quantity of information at the exact time.
They compared the costs that the network required from one scene by comparing the transmission overhead. It has been noticed that blockchain connection increased the throughput and minimized the cost of the network, which means the scheme highly improved both of them.

In [16], P. Soumyashree et al. claim that suggested mechanisms are centralized (one power managing the whole system), which caused many scalability problems or lack of privacy or SPOF. For that reason, the need for decentralized came where the main point for their research is to develop a decentralized model. And because authentication along with access control is important security. So, they proposed decentralized authentication with their model. One of the blockchain's main challenges is that it reduced a computer with very high power and big storage. In reality, IoT devices are the worked by the lower power devices. Their proposed model works with a gateway node (that is, routers or gateways or high-power computers), an interface in the middle of Blockchain and IoT devices (every device has a unique address). The system architecture depended on the next members (manager, users, IoT devices, and a gateway node). These members connected by Ethereum (every IoT device will have an Ethereum address) by using Solidity language and Remix IDE platform for testing. A smart contract has been developed to manage the entire system. The authors developed a smart contract to run the whole system, this contract controlled everything in the network beginning from initialized and started the functionality to the authentication. The whole system Interactions and exchange information goes through two stages:

1) Authentication:

The manager first prepared the smart contract, posted it in the network, then registers another manager if needed, IoT devices (Give it devise ID), and then appointed the devices to the Gateway node. Also, the manager can add a list of the access control to the contract by utilizing the authentication of the user and the device. To get the information gathered by the IoT device. The user picks the function "request-Permission" if the user gets "Decline", then "Permission ticket" will be published.

2) Information Exchange:

It is communication that happens abroad of the network to minimize the transaction latency and raised the system throughput. Users dispatch the permission ticket and random number encrypted by using the Gateway node public key. When The Gateway node receives a ticket, Gateway will authenticate the user if it is correct. Also, the user will decrypt and compare the first section of the message according to the result it accepted or denied the session. By this, they supported the two-way authentication (among the user and Gateway node). Since the model uses two-way authentication, it fights against various security threats (Replay Attack, MITM, DoS, and Sybil Attack). This model showed more safety against threats, and it can be used in different IoT applications to provide both device and user authentication.

4. Discussion and analysis

As is evident after studying the previous research's the main defy that the developer faced all the time, IoT devices deal and work with the devices that have lower power and, on the contrary, when we want to embed the blockchain required a powerful computer, the collision occurs. It better to build the applications with a decentralized mechanism instead of the centralized because the centralized most of the time went through scalability problems and proved a shortage of privacy.

Therefore, developers and researchers always strive to find a better solution by minimizing the cost of the network, latency, and energy consumption

we found many authentication algorithms that the research's discussed.

- Proof of Authentication algorithm (PoAh) and the lightweight consensus algorithm [6, 12].
- K-unknown clusters and open-source Hyperledger Fabric [10].
- The system with the lightweight IoT devices adding to difficulty parameters [12,13].
- Cross-domain authentication strategy for the blockchain [14].
- The decentralized model with an access control system [13,15].

According to the research's result, we can say that there is hope for developing and improving Blockchain authentication in IoT. Table 1 gives an outline of the advantages and disadvantages of all research papers that we discussed.

Table 1: The advantages and disadvantages of the existing recent IoT security based on blockchain approaches

Ref. Number	Year	Advantages	Disadvantages
Shahid Latif et al. [6]	2021	• illegal user can't alter on the blockchain. • ARM Cortex M4 processors with STM32F427 helped to consume low power.	• It used the resources which imposes some expense.
P. Houshyar et al. [10]	2021	• The model is good for the supporting low latency machine type communication. • The communications efficiency was improved. • Enhanced integrity and protection • The best solution for the confidentiality, authentication, heterogenicity, availability, and the scalability.	• It is affected by the blockchain configuration as number of users, endorsing nodes and etc.
A. Ahmed, and M. Aabid. [11]	2020	• Higher difficulty parameters with algorithm of the faster hashing produce are good solution. • Smaller hash size is more suitable for the storage memory.	• Easy to calculate and breached the difficulty parameters. • Small sizes output produced more time complexity.
M. Sudip et al. [12]	2020	• It is produced the minimum amount of the latency and energy consumption. • More improvement comparing it to classical methods of validates the blocks. • Raised the security and translucent. • The energy of consumption and latency were reduced. • Good solution for applications that time is important in them.	N/A
Umair Khalid et al [13]	2020	• Fast mechanism to generated and submit the authentication request • The model does not unaffected by the devices number.	• Using the Ethereum for the assessment that caused additional delay.
D. Shuai et al [14]	2019	• Reduced the number of the device's authentication • Blockchain connection increased the throughput and minimize the cost of the network	N/A
P. Soumyashree et al [15]	2019	• Supported the two-way authentication • This model is more safety against the popular security threats.	N/A

5. Conclusion

In this paper, we examine the downsides of the conventional IoT in personality confirmation and security. The general blockchain-based model for IoT verification and security assurance is introduced. The paper has demonstrated the blockchain background and infrastructure, how based authentication works, and its needs square chain innovation. Its decentralized nature can give an alternate way to deal with library stockpiling. Our examination has the benefits of conventional nature and effortlessness in correlation with different works. Finally, securing access to IoT devices is a difficult errand as IoT devices are asset obliged devices regarding handling, stockpiling, and systems administration limit. Because of their quick spreading and organization, critical impediments are found in the present confirmation and access control plans on lightweight devices like IoT.

References

[1] De Rossi, L., Salviotti, G. and Abbatemarco, N., 2019. Towards a Comprehensive Blockchain Architecture Continuum. In: Proceedings of the 52nd Hawaii International Conference on System Sciences | 2019. HICSS.

[2] G. Salviotti, L. De Rossi, N. Abbatemarco "A structured framework to assess the business application landscape of blockchain technologies" in The 51st Hawaii International Conference on System Sciences, 2018.

[3] Iredale, G., 2020. Blockchain Technology History: Ultimate Guide. [online] 101 Blockchains. Available at: <https://101blockchains.com/history-of-blockchain-timeline/#prettyPhoto> [Accessed 7 April 2021].

[4] Techterms.com. n.d. Blockchain Definition. [online] Available at: <https://techterms.com/definition/blockchain> [Accessed 7 April 2021].

[5] DataFlair. n.d. Types of Blockchains - Decide which one is better for your Investment Needs - DataFlair. [online] Available at: <https://data-flair.training/blogs/types-of-blockchain/> [Accessed 7 April 2021].

[6] Latif, Shahid & Idrees, Zeba & Ahmad, Jawad & Zheng, Li-Rong & Zou, Zhuo. (2020). A blockchain-based architecture for secure and trustworthy operations in the industrial Internet of Things. Journal of Industrial Information Integration. 21. 10.1016/j.jii.2020.100190.

[7] Seba.swiss. 2020. Classification and importance of nodes in a blockchain network. [online] Available at: <https://www.seba.swiss/research/Classification-and-importance-of-nodes-in-a-blockchain-network> [Accessed 7 April 2021].

[8] Helo, Petri & Hao, Yuqiuge. (2019). Blockchains in operations and supply chains: A model and reference implementation. Computers & Industrial Engineering. 136. 10.1016/j.cie.2019.07.023.

[9] Abougalala, R. A., Amasha, A., Areed, M. F., Alkhalaf, S., & Khairy, D. (2020). Blockchain-enabled smart university: A framework. Journal of Theoretical and Applied Information Technology, 98(17), 3531-3543.

[10] Honar Pajooh H, Rashid M, Alam F, Demidenko S. Multi-Layer Blockchain-Based Security Architecture for Internet of Things. Sensors (Basel). 2021 Jan 24;21(3):772. doi: 10.3390/s21030772. PMID: 33498860; PMCID: PMC7865640.

[11] A. Alrehaili and A. Mir, "POSTER: Blockchain-based Key Management Protocol for Resource-Constrained IoT Devices," 2020 First International Conference of Smart Systems and Emerging Technologies (SMARTTECH), Riyadh, Saudi Arabia, 2020, pp. 253-254, doi: 10.1109/SMART-TECH49988.2020.00065.

[12] S. Maitra, V. P. Yanambaka, A. Abdelgawad, D. Puthal, and K. Yelamarthi, "Proof-of-Authentication Consensus Algorithm: Blockchain-based IoT Implementation," 2020 IEEE 6th World Forum on Internet of Things (WF-IoT), New Orleans, LA, USA, 2020, pp. 1-2, doi: 10.1109/WF-IoT48130.2020.9221187.

[13] Khalid, Umair & Asim, Muhammad & Baker, Thar & Hung, Patrick & Tariq, Muhammad Adnan & Rafferty, Laura. (2020). A decentralized lightweight blockchain-based authentication mechanism for IoT systems. Cluster Computing. 23. 10.1007/s10586-020-03058-6.

[14] S. S. Panda, U. Satapathy, B. K. Mohanta, D. Jena and D. Gountia, "A Blockchain Based Decentralized Authentication Framework for Resource Constrained IOT devices," 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kanpur, India, 2019, pp. 1-6, doi: 10.1109/ICCCNT45670.2019.8944637.

[15] S. S. Panda, U. Satapathy, B. K. Mohanta, D. Jena and D. Gountia, "A Blockchain Based Decentralized Authentication Framework for Resource Constrained IOT devices," 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kanpur, India, 2019, pp. 1-6, doi: 10.1109/ICCCNT45670.2019.8944637.

Alaa Alsubhi received the B.Sc. Degree in Computer Science from Umm Al-Qura University, Saudi Arabia, in 2019. She is currently a master student in Cyber Security, Taif University, Saudi Arabia. The research interests include the Cyber Security, Artificial intelligence, IoT.

JAWAHER ALHARTHI received the B.Sc. degree in Computer Engineering from Taif University, Saudi Arabia, in 2019. She is currently a master student in Cyber Security, Taif University, Taif,Saudi Arabia. Her research interests include the Cyber Security, Blockchain-based authentication for IoT , and Internet of Things.

WAJDI ALHAKAMI received the B.Sc. degree in Computer Science, Saudi Arabia, in 2007. the M.Sc. degree in Computer Network, and the Ph.D. degree in Network Security from the University of Bedfordshire, United Kingdom in 2011 and 2016 respectively. He is currently an Associate Professor with department of Information Technology, College of Computers and Information Technology, Taif University, Taif, Saudi Arabia. His research interests include the Internet of Things, Cyber Security, and Computer Networking.