[1]Umar Albalawi

PUF Assisted Public-Key Based Authentication Using Blockchain for the IoT

Journal of Electrical Systems

Abstract: - In the IoT, authentication, confidentiality and integrity are the three most important criteria that need to be satisfied. Authentication ensures that a device can be trusted in the network, as well as its data. Without authentication, there is no way to know whether data is received from a legitimate device or a malicious device. This paper introduces a pioneering PUF-based device authentication solution for IoT systems using blockchain technology. In this research, elliptic curve cryptography (ECC) is assisted by a physically unclonable function (PUF) to ensure that only legitimate devices access the network; the devices are connected in a peer-to-peer (P2P) network based on the blockchain. Confidentiality ensures that data is shared only with the intended party. For this purpose, an encrypted secure communication channel is established by sharing a secret key between the communicating parties. In addition, the hash-based data structure of the Merkle tree is used for validating the integrity of the data between nodes. The proposed approach significantly enhances the security, privacy, and trustworthiness of information exchange within the IoT network. As a result, authentication, confidentiality and integrity are ensured before communication is conducted in the IoT environment.

Keywords: Blockchain; Internet-of-Things (IoT), Physically Unclonable Function (PUF), Authentication; Security.

I. INTRODUCTION

The Internet of Things (IoT) is a large network of heterogeneous devices equipped with sensing capabilities, which gather information from the surrounding environment and may process this data before transmitting it to the cloud or to nearby devices in an ad hoc environment [1]. Any device with sensors, processors and a wireless network can be a part of the IoT, and these are the basic components that make these devices smart. These devices are intelligent in the sense that they can share data without any human intervention and can effectively merge the physical and digital worlds. Thus, the IoT has the potential to provide life-enhancing services across all sectors of the economy. Often, a large number of sensors are connected to form an integrated network, in which data collection and data sharing are the two inherent features of all IoT devices. These sensors continuously collect data from their environment, and this can lead to vast privacy, security and trust issues. The lack of security and authentication methods in the IoT can be disastrous not only at the personal or enterprise level but also at the national and global levels [2]. The most common type of authentication service can be provided by using a Public Key Infrastructure (PKI). However, this is a centralized scheme and may not be practical for distributed systems such as the IoT.

Blockchain is an open distributed ledger that removes the dependency on a central authority in the PKI [3]. It is a chain of blocks that can be accessed by any node in the network that has the required credential. Each node in the network has a full copy of the blockchain. A node that has the required credential can add a new block to the chain. To add a new block, each node in the network must validate the new block. Once a consensus is achieved, the new block is added to the chain, and each node maintains the full copy of the updated chain. Each of the blocks stores information with a digital signature, and the blocks are added to the chain in chronological order. Depending upon the type of blockchain being used, each block contains some type of encrypted data, and blocks refer to a hash. Each block also refers to the hash of its predecessor block in the chain.

For a bitcoin application, each block in the blockchain contains details about a specific transaction that occurred between two parties, including the sender's identity, the recipient's identity and the amount of bitcoin transferred. If any node makes a change in the block data, this causes a change in its hash. As each block is referenced by the succeeding block using its hash, when there is a change in the hash, the altered block will no longer be referenced by its succeeding block. This breaks the chain, and the chain rejects the altered block. An algorithm could be deployed to recalculate the hash of the altered block and validate the chain, but this would be a very difficult process. Thus, a blockchain is a distributed database that is managed by all nodes in the peer-to-peer (P2P) network [4]. This

[1] *associate Professor, College of Computing and Information Technology, University of Tabuk, Tabuk 71491, KSA

ualbalwi@ut.edu.sa

provides high transparency in the network, and any tampering with the block can be easily identified and rejected. All of these factors make transactions in the blockchain more secure, accurate and tamperproof. Each transaction in the blockchain requires a public and private key. For example, in cryptocurrency, when one party sends a cryptocoin, it is actually sending the hashed version of the public key. The private key is used to generate a signature for each transaction, which can be used to verify the origin of the transaction [5]. This can be used to prevent transactions from being altered. If the private key is released, then a malicious user can receive cryptocurrency intended for another person. Therefore, keeping a private key secret is very important for ensuring that a transaction is secure.

A Physically Unclonable Function (PUF) module can generate a unique private key for a device using the intrinsic properties of the hardware device [6]. It takes advantage of the inevitable process variability that occurs during the device manufacturing process. This makes each module unique and unable to be replicated, as it is not under design or manufacturer control. With the use of a PUF, there is no need to store a private key anywhere in the device, which can improve security. In this paper, a novel PUF-based device authentication mechanism is proposed for the IoT system using blockchain, which addresses the issue of unauthenticated devices trying to connect to the network, thereby resolving the security, privacy and trust issues involved in information exchange and in the network as a whole. To the best of the authors' knowledge, this is the first paper to consider a secure authentication protocol for a PUF-based IoT using blockchain. The unique contributions of this paper are as follows:

1. A key exchange protocol is proposed for an untrusted channel.
2. A mechanism of protection after the device authentication is proposed.

II. Related Works

In [7], blockchain and PUF has been used for Internet of Everything (IoE). The authors in the paper have proposed simplistic device enrollment and authentication steps. Authors in [8] proposed PUF based Authentication model for smart home using private blockchain. A blockchain based authentication and security mechanism is proposed for IoT in [9]. It stores the private key in the device, which makes the device more susceptible to attacks. In [10], access control mechanism is proposed for permissioned blockchain engaging all stakeholders on the consensus. In [11], authors have addressed the trust issues in blockchain based supply chain applications by using three-layers of trust management framework by assigning trust and reputation scores to the supply chain participants based on their interaction. In [12], authors proposed a protocol consisting of key agreement and communication phase. PUF is used for device authentication with an objective to minimize the risk of exposing authentication key and reduce the load of authentication server.

The research [13] explores the integration of blockchain technology into Content Delivery Networks (CDNs) to address the dual challenges of content transparency and user privacy. The authors propose a novel approach that leverages blockchain to enhance the transparency of content delivery while preserving user privacy. The paper delves into the technical aspects of how blockchain can be implemented in CDNs, its impact on content distribution, and the measures taken to ensure user privacy. The synthesis of blockchain and CDN technologies is anticipated to provide a more secure and transparent environment for content delivery, fostering a balance between transparency and user privacy in the digital ecosystem.

The primary emphasis of the paper [14] is expected to be on how blockchain can provide a secure and decentralized framework for handling access control in IoT environments. The authors explore the potential of utilizing blockchain's key features, including immutability, transparency, and decentralization, to address issues related to authentication, authorization, and accountability within IoT applications. The proposed techniques involve the implementation of smart contracts, cryptographic methods, or other blockchain-based mechanisms to enhance the overall security and reliability of access control in IoT ecosystems.

Another research [15] focuses on the development and implementation of a blockchain-based authentication framework tailored for IoT networks. The proposed framework incorporates the decentralized and tamper-resistant nature of blockchain to establish secure and reliable authentication processes within the IoT ecosystem. The authors explore the use of smart contracts or other blockchain mechanisms to ensure the integrity of authentication data and to mitigate potential threats.

In [16], the central theme involves thorough analysis of the security mechanisms embedded in the PUF-based authentication and key exchange protocol. This assessment involves identifying potential weaknesses,

vulnerabilities, or exploitable points in the protocol that could compromise the overall security of IoT devices using this authentication method.

The research [17] focus on presenting and exploring a decentralized authentication framework built on blockchain principles. This model is designed to address the authentication challenges within IoT-based educational platforms, emphasizing the benefits of decentralization, transparency, and tamper resistance offered by blockchain technology. The authors delve into the technical details of the proposed model, potentially discussing the integration of smart contracts or other blockchain mechanisms to establish secure and reliable authentication processes.

In [18] the authors discuss the inherent security advantages of using PUFs, which are difficult to clone or replicate, making them suitable for authenticating embedded devices. The scheme may involve the generation and verification of cryptographic keys derived from the device's PUF, enhancing the security of the authentication process. They demonstrate the effectiveness of PUFs in providing a secure and reliable authentication mechanism for embedded systems.

In [19] the authors explore the application of PUF as a means of authentication to enhance the security of Internet of Things (IoT) devices. The authors discuss the theoretical foundation of PUFs, their characteristics, and how these physical traits can be leveraged to establish a secure and robust authentication mechanism.

The authors in [20] develop and implement a mutual authentication method that involves PUFs. They explain the theoretical foundation of PUFs, discuss their unique physical characteristics and how these traits can be employed for secure mutual authentication. The mutual authentication process involves two or more PUFs verifying each other's authenticity, adding an additional layer of security to the authentication protocol.

The paper [21] contributes to the field of IoT security by proposing a joint heterogeneous PUF-based authentication method. By leveraging diverse PUFs, the authors aim to enhance the overall security of IoT devices and systems. The paper delves into the technical details of implementing this joint heterogeneous PUF-based authentication and discuss its potential advantages in terms of resistance to attacks and improved security for IoT authentication processes.

The [22] presents a novel authentication framework for securing the Internet of Medical Things (IoMT). The proposed framework integrates machine learning techniques with PUF to enhance the authentication process in the IoMT ecosystem. This integration aims to provide a robust and adaptive authentication mechanism tailored specifically for medical IoT devices. The authors may discuss how machine learning algorithms can analyze and adapt to patterns in PUF responses, improving the accuracy and reliability of authentication.

Lastly [23] is a comprehensive survey that explores the use of PUFs in authentication and key agreement protocols across diverse domains, including the Internet of Things (IoT), Wireless Sensor Networks (WSNs), and Smart Grids. The primary objective of the paper is to provide an extensive review of existing authentication and key agreement protocols that incorporate PUFs within the contexts of IoT, WSNs, and Smart Grids. The authors analyze and categorize different approaches, highlighting their strengths, weaknesses, and suitability for specific applications. The survey encompasses various PUF types and their integration with cryptographic protocols to secure communication and data exchange within these domains.

III. The Proposed Framework

In this section, we highlight the framework of the proposed system. Table 1 lists the symbols and their definitions used in the paper.

Table 1: List of Abbreviations

Symbol	Definition
ECC	Elliptical Curve Cryptography
PUF	Physically Unclonable Function
P2P	peer-to-peer
IoT	Internet of Things
PKI	Public Key Infrastructure (PKI).
IoE	Internet of Everything
IoMT	Internet of Medical Things
WSNs	Wireless Sensor Networks
TTP	Trusted Third Party

CRP	Challenge-Response Pair
y	Helper Data
SK_{nc}	Non-Consensus Node Secret Key
PK_{nc}	Non-Consensus Node Public Key
PK_{server}	Server Public Key
SK_{server}	Server Secret Key
SK_c	Consensus Node Secret Key
PK_c	Consensus Node Public Key
SRAM	Static Random Access Memory
BCN	Blockchain Network

In the IoT, authentication, confidentiality and protection are the three most important criteria that need to be satisfied. Authentication ensures that a device can be trusted in the network, as can its data. Without authentication, there is no way to know whether data is received from a legitimate device or a malicious device. To ensure that only legitimate devices access the network, public key cryptography assisted by the PUF is used. In this paper, the devices are connected in a peer-to-peer (P2P) network based on the blockchain without using a third party. Confidentiality ensures that the data is shared only with the intended party. For this purpose, an encrypted secure communication channel is established by sharing a secret key between the communicating parties. A key exchange protocol is used whereby the devices agree on the shared secret key, ensuring that communication takes place safely in an untrusted channel. Sharing an authentication key between devices ensures the identity of the claimed devices in the network. Protection ensures that the devices are well protected even after they have passed the authentication phase. This paper assumes that devices can be altered by an intruder after the authentication phase and that the intruder can modify the key configuration file in the device, leaving a backdoor for network disruption.

Fig. 1 shows the system process. Authentication verifies the identity of the user or device. Certificate-based authentication ensures that nonconsensus nodes can access servers securely by accessing certificates instead of conventional usernames and passwords. Since a nonconsensus node can access the server without a username and password, this prevents phishing, keystroke logging and man-in-the-middle attacks. Certificate authentication provides mutual authentication between a nonconsensus node and a server by using a consensus node. When the consensus node wants to connect to the server, the server asks for the certificate issued by the consensus node. When the certificate is signed, it ensures that only a legitimate node can connect to the server. Similarly, when a nonconsensus node wants to connect to the server, it needs to know whether the server to which it connects is an honest server.

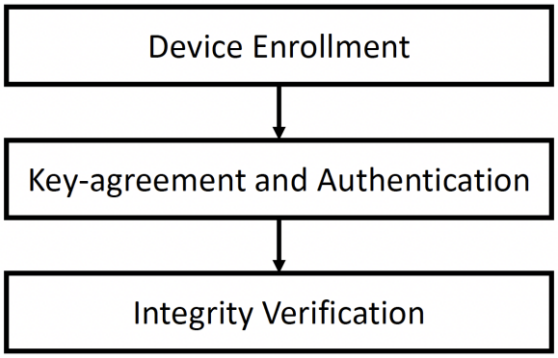

Fig. 1: System Process

A. Mutual Authentication Between the IoT Device and the Server

The consensus node is used for authentication between a nonconsensus node and the server. A two-way handshake is established so that the nonconsensus node knows that it has been authenticated by the authentication node and the consensus node knows that only legitimate nodes are authenticated. Therefore, this process is performed in two stages:

1. In the first stage, the nonconsensus node is enrolled by the consensus node because this is the first time the nonconsensus node has joined the P2P network.

2. In the second stage, key agreement and node authentication occur between the nonconsensus nodes before communication.

The IoT device needs to be registered before it attempts to communicate with the consensus nodes. Registration is performed by a trusted third party (TTP), which has a database with challenge-response pairs for the IoT devices. It is the responsibility of the TTP to indicate that only legal devices are registered. The TTP is required to establish secure and authenticated communication between the server and the consensus node as well as between the consensus node and the devices. For this purpose, the consensus node needs to authenticate the device as well as the server. This is done in the authentication phase.

PHASE 1: IOT DEVICE REGISTRATION PHASE

The **TTP** contains the challenge-response pair **(CRP)** of each IoT device

*IoT device **sends** the device **ID** (MAC address) to the **TTP***
***while (ID is legal) do** //check if the ID is legal or not*
    *__TTP__ contains the challenge-response pair **(CRP)** in the database*
    *TTP **sends** the corresponding challenge to the IoT device*
    *IoT device **feeds** the challenge to the PUF module*
    *PUF module **generates** the response*
    *IoT device then **sends** back the response to TTP*
    If (the response match corresponding response in its database)
        IoT device is registered
    else
        IoT device is not authenticate
        It fails the registration phase
end

PHASE 2: ENROLLMENT PHASE

Certificate for non-consensus node:

*PUF module in non-consensus **generates** a secret key **(SK_{nc})** and helper data **(y)***
*non-consensus node **generates** public key **(PK_{nc})** from **(SK_{nc})** based on ECC*
*non-consensus node **sends** → **device ID, y, (PK_{nc}) to** consensus node*
*consensus node **signs** the certificate using its PUF based secret key **(SK_c)***
*certificate used to **link** the device with its **(PK_{nc})***

Certificate for server:

*server **generates** public key **(PK_{server})** and secret key **(SK_{server})** based on ECC*
*server **sends** → its device ID and **(PK_{server}) to** consensus node*
*consensus node **generates** the certificate using its **(SK_c), server ID, (PK_{server})***
*certificate used to **link** the server with its **(PK_{nc})***

Consensus node sends the certificate and its public key (PK_c) to the server
Server needs to store this certificate securely to later verify the server

B. Data Integrity Verification in the Blockchain

Nodes in the blockchain network are responsible for generating new blocks, verifying new blocks and participating in consensus. Therefore, these nodes have large responsibilities in the overall system, and if they are compromised, then they can bring down the whole network. Therefore, there should be a verification mechanism to ensure the integrity of critical data, such as node configuration files or firmware [24]. A Merkle tree is a data structure used in distributed systems such as blockchain networks to verify data efficiently. The Merkle tree uses a hash value instead of a complete file, which makes it an efficient data verification mechanism in peer-to-peer networks.

In distributed and peer-to-peer systems, the same data exists in multiple locations [25]. A change in data at one location needs to be reflected at all locations. It would be very time-consuming and computationally expensive to verify the integrity of the data in each file over the entire system. This approach would require large amount of data to be transmitted over the network, which could easily congest the entire network. In the Merkle tree, instead of

sending an entire file over the network, the hash value of the entire file is sent. Therefore, a Merkle tree produces a digital fingerprint of a block by summarizing all the transactions in it. This ensures that the transaction is a part of the block. A leaf in a Merkle tree is the hash of an individual transaction. These nodes are combined and hashed again to form nonleaf nodes. The process repeats until only one hash is left, and this forms the root of the tree, which is called the Merkle root.

A consensus node may be tempered after receiving a certificate from the TTP. This can cause a change in the underlying configuration file and can compromise the blockchain network. To solve this problem, the last transaction in each block contains the configuration information of each consensus node. Therefore, it is necessary to periodically check the integrity of this critical data at the consensus node. For this purpose, every n^{th} block in the blockchain contains the critical information, and each transaction in the block is a file containing critical information about the consensus node. As shown in Fig. 2, block 1 contains the configuration files m_0, m_1 and so on, one for each device in the blockchain network. The hash value of these configuration files is computed. This process continues until a root hash value is obtained. The server periodically verifies each consensus node to determine whether it contains a similar configuration file or not. Therefore, after *n* regular blocks (which contain regular transactions), there is a special block that contains a configuration.

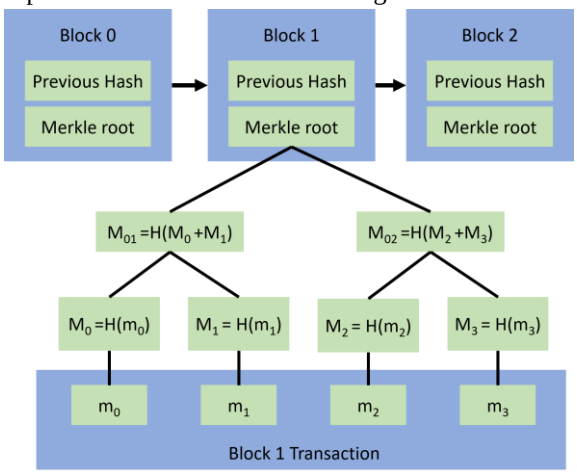

Fig. 2: Block Transaction

PHASE 3: DATA INTEGRITY PHASE

Consider A, B, C and D are transactions:

1. *A, B, C, and D separately hashed then stored as leaf node*
2. ***consecutive pairs of leaf*** *nodes hashed as* ***parent node***
3. ***consecutive pairs of parent nodes*** *hashed to produce the* ***Root Hash (Merkle Root)***
4. ***consecutive blocks*** *can be hashed until there is only one node at the top*
5. ***Merkle Root*** *summarizes all of the data in the related transactions*
6. *Merkle Root is stored in the block header*
7. ***end***

C. Protocol Description

1. An IoT device needs to be registered before it attempts to communicate with consensus nodes.
2. Registration is performed by a trusted third party (TTP), which has a database with challenge–response pairs for the IoT devices. It is the responsibility of the TTP to indicate that only legal devices are registered.
3. The role of the nodes in the blockchain clients is to collect data and relay the data to the consensus node in the blockchain network for processing through a trusted third party (TTP).
4. The TTP is required to establish secure and authenticated communication between the server and the consensus node as well as between the consensus node and the devices. For this purpose, the consensus node needs to authenticate the device as well as the server. This is done in the authentication phase.
5. In addition, each block contains the configuration information of each consensus node. A Merkle tree is used to periodically ensure the integrity of this critical data at the consensus node.

D. PUF

The PUF is essentially a function that accepts a challenge as input and generates a random response. There is no mathematical relation between the challenge and the response. The response is generated based on the process variation that occurs during the device manufacturing process. Therefore, it is not possible to clone the PUF to produce the same response for the given challenge set. One of the most important requirements for a PUF is that it can generate the same response for a given challenge. This ensures that the device has a unique and stable fingerprint that can be used as a secret key or device identifier.

Among the various types of PUFs studied, the SRAM PUF has received particular interest because it is memory-based and hence readily available in modern devices [26]. In the SRAM PUF, the start-up values of random cells are used as the response. The SRAM can be based on standard 6-cell transistors, as shown in Fig. 3. Transistors *M1* through *M4* constitute two pairs of inverters connected via cross-coupling. These inverters are connected to the bitline (BL) and its complement bitline bar (BLB) using pass transistors *M5* and *M6*, which are controlled by the wordline (WL). These lines are used to access a cell that stores a logical *'1'* or *'0'*. Although the two inverters in the SRAM cells are designed to be symmetric, small and random process variations during the manufacturing process make them behave slightly differently. Therefore, each cell in the SRAM prefers a logical *'0'* or logical *'1'* state during powerup, which is used as a one-bit fingerprint of that cell.

In this paper, a 6T SRAM-based PUF is used to obtain the secret key that will be used to authenticate IoT devices. Since the key generated from the PUF module must be stable and reliable, a fuzzy extractor is used [27].

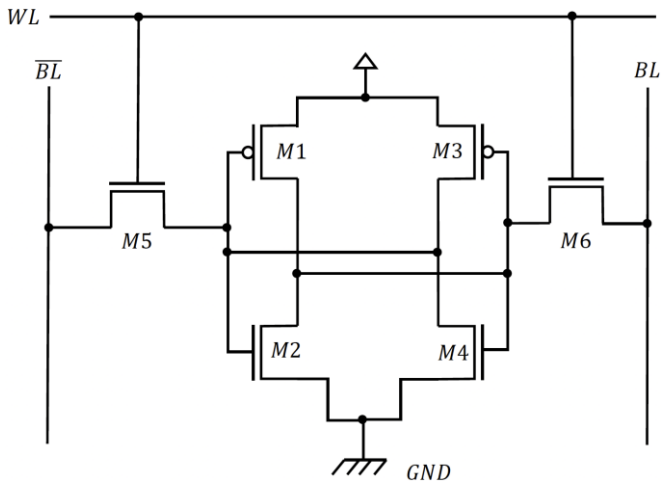

Fig. 3: 6T SRAM Circuit

IV. System Model

All the devices in the blockchain network as well as the blockchain clients have a PUF module to generate a secret key. The nodes in the blockchain network host the ledger and are capable of participating in blockchain transactions. The IoT devices in the blockchain client have limited hardware resources: limited computational power, storage and connectivity.

The nodes in the blockchain network require high computational power, memory and energy for performing computations. Therefore, due to the limited hardware resources of these IoT devices, they do not store distributed ledgers. The role of the nodes in the blockchain clients is to collect data and relay the data to the consensus node in the blockchain network for processing through a trusted third party (TTP). Before the IoT devices can communicate with consensus nodes, they need to be verified as legitimate nodes and need to be enrolled by the TTP. The IoT devices sign the data with their private keys. To ensure secure communication between the IoT devices and the consensus node, it is necessary to ensure trust between them. For this purpose, a separate trust agreement is required [13]. The system under consideration consists of 4 major components, as shown in Fig. 4:

1. Nodes: The nodes are divided into two categories: consensus nodes and nonconsensus nodes. Consensus nodes are nodes that are responsible for generating new blocks, verifying any new blocks and participating in consensus to register a new node in the network. Nonconsensus nodes, on the other hand, conduct transactions, including data transfer. It is assumed that the consensus nodes are secured.

2. Blockchain network: The blockchain network (BCN) is the core entity that provides decentralized services. All the nodes are part of the BCN.
3. Devices: All the devices (either legitimate or malicious) have a PUF module and want to be part of the BCN to add transactions. However, only legitimate devices should be allowed to join the BCN, and malicious devices should be prevented from joining. For a device to be a nonconsensus node, it first needs to verify its identity and enroll, which is performed by a consensus node.
4. Server: Consensus nodes store all relevant information about nonconsensus nodes in the server and are susceptible to attacks.

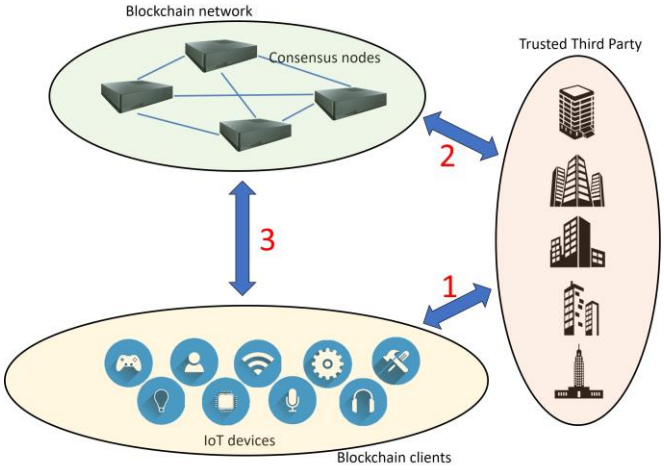

Fig. 4: System Model

A device that wants to be a part of the BCN needs to be verified first by a consensus node. The consensus node ensures mutual authentication using certificates stored on the device side as well as the server side. Since the servers are susceptible to attack and malicious nodes can be involved in enrollment, certificates are stored on both the server and device sides. In a blockchain network, each device is a node that stores the same information. Any node that is connected to the blockchain for the first time needs to register its identity. Thus, the block contains the node ID along with the public key, the hash value of the critical data and other relevant information. Table 2 gives the numbers of bits used in the experimental setup, which is shown in Fig. 5.

Table 2: Number of bits used

Parameters	Values
Device ID	48 bits
PUF based secret key (SK_{nc})	256 bits
Helper Data **(*y*)**	752 bytes
Consensus node public key (PK_c)	256 bits
Digital public key	256 bits
Server public key (PK_{server})	256 bits

Table 3 illustrates the comparison with state-of-the-art PUF and Blockchain for IoT Authentication mechanisms. In security Evaluation column, SE1, SE2, and SE3, indicate Authentication, Integrity, and Confidentiality, respectively.

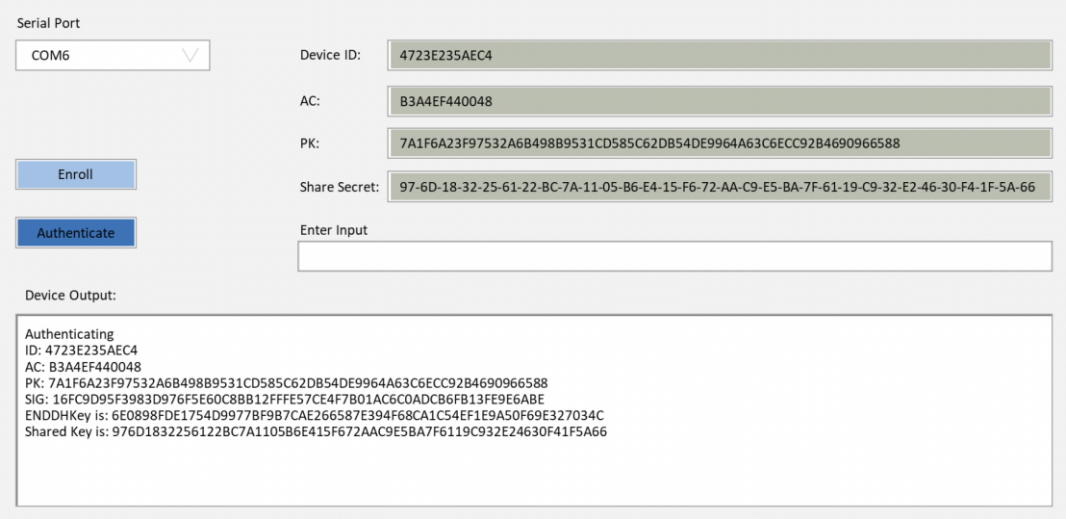

Fig. 5: Proposed Experiment setup

Table 3: Comparision with the state of the art PUF and blcokchain for IoT Authentication mechanisms. SE1, SE2, and SE3, indicate Authentication, Integrity, and Confidentiality, respectively

Proposed Mechanism	Ref	Implementation Platform	Security Evaluation			Performance Evaluation
			SE1	SE2	SE3	
Hardware-assisted blockchain for data security in IoE	[7]	Altera & raspberry Pi	√	√	×	×
Private blockchain for smart home authentication	[8]	Simulation	√	×	×	×
Blockchain-based authentication for IoT	[9]	Simulation	√	√	×	×
Blockchain access control for IoT	[10]	Simulation	×	×	×	×
Trust management in blockchain and IoT	[11]	Simulation	×	×	√	×
PUF based IoT device authentication scheme	[12]	STM32F4-MCU	√	√	×	×
Blockchain-based content transparency for privacy	[13]	Simulation	√	×	√	×
Blockchain-based access control for IoT application	[14]	Simulation	√	×	×	×
Blockchain-based authentication framework for secure IoT network	[15]	Simulation	√	×	×	√
PUF-based authentication and key-exchange protocol for IoT network	[16]	Simulation	√	×	√	×
Blockchain-based decentralized model for IoT based E-learning	[17]	Simulation	√	√	√	×
PUF based authentication for embedded devices	[18]	Simulation	√	√	√	×
PUF-based authentication for the security of IoT device	[19]	Simulation	√	×	×	×
Integrating radio frequency (RF) and PUF to enhance security for IoT	[21]	raspberry Pi and Arduino	√	√	√	×
PUF-based ToT mutual authentication	[28]	Arduino mega	√	√	×	√
PUF-based authentication for smart meters	[29]	FPGA	√	√	√	×
The proposed work		Simulation	√	√	√	×

V. CONCLUSION

The Internet of Things (IoT) encompasses a vast network of diverse devices, each of which is outfitted with sensors that enable it to collect information from its immediate surroundings. These devices can process the data they gather and either send it directly to the cloud or share it with other nearby devices in an ad hoc manner. Essentially, any

device equipped with sensors, computing capabilities, and wireless connectivity qualifies as an IoT device, and these components are fundamental to its smart nature. These devices are deemed intelligent due to their ability to autonomously exchange information, thereby seamlessly integrating the physical and digital realms. Consequently, the IoT holds the promise of delivering transformative services that are beneficial to all sectors of the economy, enhancing quality of life on a global scale. A lack of robust security and authentication measures in the Internet of Things (IoT) could lead to catastrophic consequences not only for individuals and businesses but also at the national and global levels. Without proper safeguards, IoT devices become vulnerable entry points for cyberattacks, potentially compromising personal privacy, corporate data, and critical infrastructure. This vulnerability poses significant risks, ranging from unauthorized access of sensitive information to the disruption of essential services and even threats to national security. This research proposes a novel PUF-based device authentication solution for IoT systems using blockchain technology. In this study, we employ elliptic curve cryptography (ECC) supported by physically unclonable functions (PUFs) to guarantee that network access is restricted to authorized devices that are interconnected within a peer-to-peer (P2P) blockchain network, eliminating the need for intermediary third parties. To ensure confidentiality, data is shared exclusively with intended recipients through an encrypted secure communication channel established via the exchange of a secret key between parties. Furthermore, we utilize a Merkle tree, a hash-based data structure, for the verification of data integrity among nodes, ensuring the authenticity and reliability of the exchanged information. Future research could also examine ways of ensuring reasonable power consumption in the blockchain.

REFERENCES

[1] Y. Liu, W. Yu, W. Rahayu, T. Dillon, "An evaluative study on IoT ecosystem for smart predictive maintenance (IoT-SPM) in manufacturing: Multiview requirements." IEEE Internet of Things Journal 2023, vol. 10, pp. 11160-11184.

[2] I. Wassem, A. Haider, M. Daneshmand, B. Rauf, Y. Bangash, "An in-depth analysis of IoT security requirements, challenges, and their countermeasures via software-defined security." IEEE Internet of Things Journal 2020, vol. 7, pp. 10250-10276.

[3] Z. Sun, D. Han, X. Wang, C. Chang, Z. Wu,"A blockchain-based secure storage scheme for medical." EURASIP Journal on Wireless Communication and Networking 2022, vol. 1, pp. 1-25.

[4] H. Khan, M. Sohail, S. Nazir, T. Hussain, B. Shah, F. Ali, "Role of authentication factors in Fin-tech mobile." Journal of Big Data 2023, vol. 10, pp.1-37.

[5] O. Younes, A. Alharbi, A. Yasseen, F. Alshareef, F. Albalawi, U. Albalawi, " CeTrivium: A stream cipher based on cellular automata for securing real-time multimedia transaction." Computer System Science and Engineering 2023, vol. 27, pp. 2895-2920.

[6] L. Pang, H. Kim, B. Yang, X. Wang, Y. Gao, " Security evaluation of n-choose-k-sum PUFs against modeling." IEEE Access 2021, vol. 9, pp. 168193-168206.

[7] S. P. Mohanty, V. P. Yanambaka, E. Kougianos, P. Deepak, " PUFchain: a hardware-assisted blockchain for sustainable simultaneous device and data security in the Internet of everything." IEEE Consumer Electronic Magazine 2020, vol. 9, pp. 8-16.

[8] K. Rahim, H. Tahir, N. Ikram, " Sensor based PUF IoT authentication model for a smart home with private blockchain." In Proceedings 2018 International Conference on Applied and Engineering Mathematics (ICAEM), Taxila, Pakistan, 2018, pp. 102-108

[9] D. Li, W. Peng, F. Gai, "A blockchain-based authentication and security mechanism for IoT." In 2018 27th International Conference on Computer Communication and Network (ICCCN), Hangzhou, China, 2018, pp. 1-6.

[10] M. A. Islam, S. Madria, "A permissioned blockchain based access control system for IoT." In 2019 IEEE International Conference on Blockchain, Atlanta, Ga, USA, 2019, pp. 469-476.

[11] S. Malik, V. Dedeoglu, S. S. Kanhere, R. Jurdak, "Trustchain: Trust management in blockchain and IoT supported supply chains." In 2019 IEEE International Conference on Blockchain, Atlanta, Ga, USA, 2019, pp. 184-193.

[12] B. Kim, S. Yoon, Y. Kang, D. Choi, "PUF based IoT device authentication scheme." In 2020 International Conference on Information and Communication Technology Conference(ICTC), Jeju, South Korea, 2020, pp. 1460-1462.

[13] V. Thang, S. Chatzinotas, B. Ottersten, " Blockchain-based control delivery networks: content transparency meets user privacy." In Proceedings IEEE Wireless Communication and Networking Conference (WCNC), Marrakesh, Morocco, 2019, pp. 1-6.

[14] S. Namane, I. B. Dhaou, “Blockchain access control techniques for IoT applications.” Electronics 2022, vol. 11, pp. 1-29.
[15] A. K. Alhwaitat, M. A. Almaiah, A. Ali, S. Alotaibi, R. Shishakly, A. Ltfi, M. Alrawad, “A new blockchain-based authentication framework for secure IoT networks.” Electronics 2023, vol. 12, pp. 1-25.
[16] D. Sun, Y. Gao, Y. Tian, “On the security of a PUF-based authentication and key exchange protocol for IoT devices.” Sensors 2023, vol. 23, pp. 1-21.
[17] O. A. Kjasjan, S. Alamri, W. Alomoush, M. K. Alsmadi, S. Atawneh, U. Mir, “Blockchain-based decentralized model for IoT-based E-learning and education environments.” Computers, Materials and Continua 2023, vol. 75, pp. 3133-3158.
[18] M. Deutschmann, L. Iriskic, S. L. Lattacher, M. Munzer, O. Tomashchuk, “A PUF based hardware authentication scheme for embedded devices.” White paper 2018.
[19] A. Oun, M. Niamat, “PUF-based authentication for the security of IoT devices.” In Proceedings of the 2023 IEEE International Conference on Electro Information Technology (eIT), Remeoville, IL, USA, 2023, pp. 067-070.
[20] Y. Choi, J. Lee, H. Shin, W. Sun, “Mutual authentication method between PUFs.” In Proceedings of the 2022 International Conference on Electrical, Computer and Energy Technologies (ICECET), Prague, Czech Republic, 2022, pp. 1-5.
[21] S. Yoon, S. Han, E. Hwang,“Joint Heterogeneous PUF-based security-enhanced IoT.” IEEE Internet Things Journal 2013, vol. 10, pp. 18082-18096.
[22] P. K. Sadhu, A. Baul, V. P. Yanambaka, A. Abdelgawad, “Machine learning and PUF based authentication framework for Internet of medical things.” In 2022 International Conference on Microelectronics (ICM), Casablanca, Morocco, 2022, pp. 160-163.
[23] P. Mall, R. Amin, A. K. Das, M. T. Leung, K. R. Choo, “Puf-based authentication and key agreement protocols for IoT, WSNs, and smart grids: A comprehensive survey.” IEEE Internet of Tings Journal 2022, vol. 9, pp. 8205-8228.
[24] J. Yang, J. Wen, B. jiang, W. Wang, “Blockchain-based sharing and tamper-proof framework of big data networking.” IEEE Network 2020, vol. 34, pp. 62-67.
[25] X. Xiao, F. Wang, M. Shahidehpour,Y. Zhai, Q. Zhou, “Peer-to-peer trading in distribution system with utility’s operation.” CSEE journal of Power and Energy Systems 2021, pp. 1-9.
[26] L. Lu, T. T. Kim, “A high reliable SRAM-based PUF with enhanced challenge-response space.” IEEE Transactions on Circuits and Systems II: Express Briefs 2021, vol. 69, pp. 589-593.
[27] Y. Gao, Y. Su, L. Xu, D. C. Ranasinghe, “Lightweight (reverse) fuzzy extractor with multiple reference PUF responses.” IEEE Transactions on Information Forensics and Security 2018, vol. 14, pp. 1887-1901.
[28] K. Lounis, M. Zulkernine, “T2T-MAP: a PUF-based thing-to-thing mutual authentication.” IEEE Access 2021, vol. 9, pp. 137384-137405.
[29] B. Harishma, P. Mathew, S. Patranabis, U. Chatterjee, U. Agarwal, M. Maheshwari, S. Dey, D. Mukhopadhyay, “Safe is the new smart: PUF-based authentication for load modification-resistant smart meters.” IEEE Transactions on Dependable and Security Computing. 2022, vol. 19, pp. 663-680.