Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 45 No. 2 (2024)

Review on Physically Unclonable Functions and Chaotic Maps in Providing Authentication in Blockchain Based Internet of Things

[1]Bharati B Pannyagol , [2] S. L. Deshpande

[1]*Research Scholar, Department of Computer Science and Engineering, VTU, Belagavi, Karnataka, India*

[2]*Professor, Department of Computer Science and Engineering, VTU, Belagavi, Karnataka, India*

Abstract The IoT is the latest generation of Internet technology that promises to drastically improve life in several areas, including clever homes and intelligent transit, smart cities, and smart health. With all these applications it introduces several problems, including data integrity, security, privacy, and single points of failure. Future advancements in IoT applications are hampered by these difficulties. Recently, BC has drawn an abundance of scholarly interest from researchers outside of the financial sector. IoT's applications can benefit from the use of BC technology to establish a decentralized, dependable, and secure environment. IoT applications using BC are still in their infancy, especially when it comes to tiny computing devices. Given that prior to engaging in communication, every component of an Internet of Things network needs to authenticate itself, authentication is the foundation of the system. As a result, protecting authentication is crucial. This paper offers a thorough analysis of integration of BC technology with IoT systems. We have concentrated on IoT security, specifically on their authentication protocols. It provides an analysis of the available literature on IoT and BC integration and authentication by using Chaotic maps, Physically Unclonable Functions (PUF). In this paper, we first attempt to explore the key problems of IoT protocol stack and investigated the different chaotic maps, PUF used so far to overcome the authentication challenge in IoT.

Keywords*:* Internet of Things, Blockchain, Physically Unclonable Functions, Chaotic maps, Authentication.

1. Introduction

1.1 Introduction to IoT

The Internet of Thins (IoT) is a rapidly developing and highly promising technological advancement that facilitates the mechanisation of corporate and academic activities via streamlined and user-friendly operations. The underlying principle of this technology is the interconnection of a vast array of intelligent devices, facilitating the seamless flow of services and data over the internet, without requiring assistance from humans [1], [2][3]. IoT networks facilitate collaboration and enable individuals to make meaningful contributions without direct involvement in the associated processes. Streamlining human activities through intelligent application is the main goal of the IoT. The IoT has emerged as a vast network including a multitude of linked devices, making it the largest network to date[4], [5]. Illustrative instances of such entities include automobiles, mobile gadgets, computers, edifices, and even garments that are furnished with sensory apparatus [6]. The intention behind these sensors is the conversion of physical phenomena into digital representations via the transmission of data. Growing evidence in recent years indicates interest among individuals in using IoT enabled smart networks, encompassing many domains such as smart homes, intelligent workplaces, and intelligent markets. The prevalence of data, propensity for sharing, and efficient time management contribute to this phenomenon. The utilisation of IoT-based smart networks is impeded or restricted by several weaknesses

that consist of, but are not restricted to data falsification, privacy concerns, integrity issues, and the participation of third parties. The various IoT layer technologies and applications are seen in Figure 1.

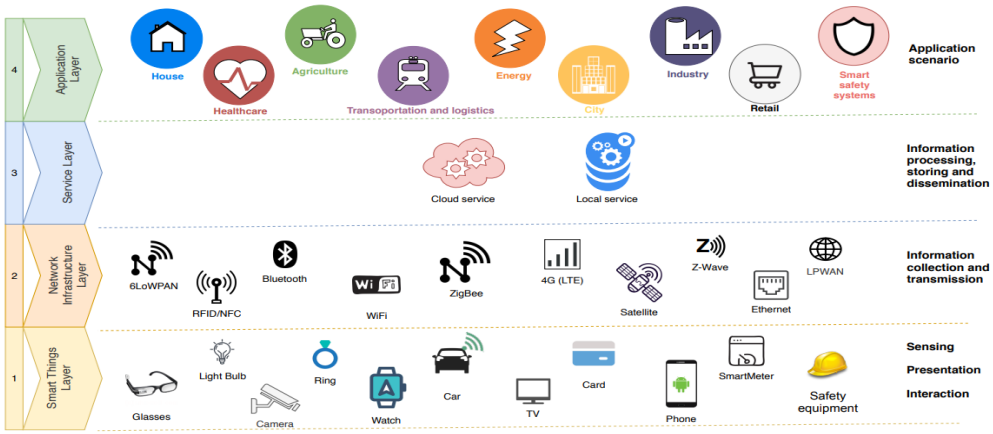

Figure 1: IoT layer technologies and applications

1.2 Fundamentals of BC

A distributed ledger system called BC can be used to safely store and manage keys. BC is tamper-proof and transparent, which means that it is difficult to forge or modify stored keys. The BC is composed of several components that fulfil diverse roles, including transaction processing, block propagation, mining, consensus finding, and ledger storage for associated cryptocurrencies. The BC has many tiers that bear resemblance to the well-recognized TCP/IP technology. The classification of these components may be determined by their inherent features. Numerous conceptual frameworks exist for building a BC network with a hierarchical structure. Figure 2 explains different kinds of BC, consensus methodology, and application areas.

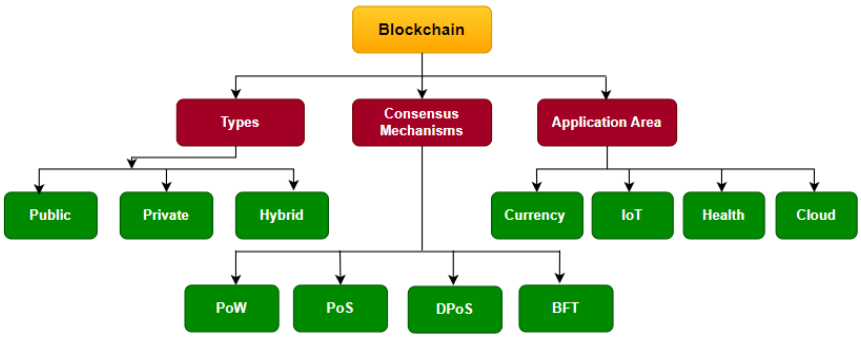

Figure 2: BC Types, Consensus, and application

Key Features:

Most noteworthy features of BC technology are covered in the following.

Decentralization and Immutability:

It operates on a mutually exclusive network, eliminate the middleman or central authority. So, the potential for a one single area of vulnerability is decreased and security is improved by this decentralisation. Data kept in the BC is almost impossible to remove or change after that. Cryptographic hashes are accustomed to join each block to the one before it, forming a safe and impenetrable chain of data.

Smart Contracts (SC):

SC are agreements or business logic that run on their own and are written on the top layer of the BC. They automatically operate and enforce the terms when predetermined criteria are satisfied.

Consensus Mechanisms:

Several consensus algorithms are available for incorporating fresh deals into the ledger and verifying existing ones. To ensure agreement among participants, four strategies are used: Delegated Proof of Stake (DPoS), Proof of Work (PoW), Proof of Stake (PoS), and Byzantine Fault Tolerance (BFT).

Cryptocurrencies:

The foundation of cryptocurrencies like Bitcoin and Ethereum is BC technology, which allows for safe, peer-to-peer transactions without the participation of traditional financial institutions.

Decentralized Applications (DApps)

BC makes it easier to create decentralised applications that run on peer-to-peer networks as opposed to centralised servers. More resiliency and resistance to censorship may result from this.

Transparency and Security:

Every transaction on the BC is accessible to every network user. Consensus techniques, like Proof of Stake (PoS) and Proof of Work (PoW), protect the network's integrity and stop malicious activity.

Tokenization

BC makes it possible to create digital tokens that stand in for ownership of items like property or artwork. This has the power to completely change how assets are moved, traded, and managed.

Identity Management:

Digital identity management is made safe and decentralised by BC technology. Users can choose which personal information to share with others and possess greater authority over it, which lowers the chance of identity theft.

2.Blockchain -Iot Architecture

The BC technology is rapidly evolving into a reliable and secure means of facilitating secure data transfer across several sectors: economy, supply-chain management, nutrition, energy, and healthcare. One potential remedy has been the incorporation of BC technology to address or mitigate certain challenges affiliated with the IoT. Figure 3 illustrates the BC based IoT architecture.

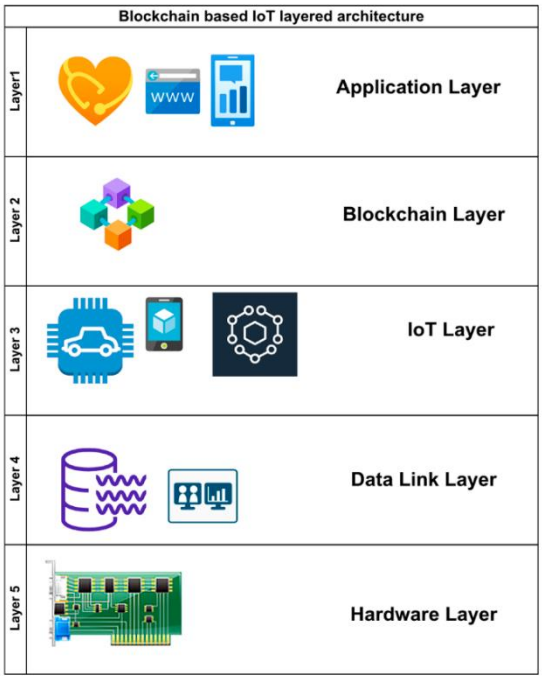

Figure 3. BC based IoT layered Architecture

2.1 Application Layer

Apps developed using BC technology, SC, and chain codes are all included in this layer. The aforementioned layer consists of two separate sections, namely application and execution. Within the context of the BC system, end users actively engage with apps to facilitate communication and exchange of information. The scope of the subject matter includes software, web-based applications, user interfaces, and protocols. The BC system functions as the underlying infrastructure for such applications. However, these applications often engage in interactions with the BC system via interfaces. The 2nd layer encompasses the setup level, including smart contracts, fundamental regulations, and a hybrid ledger. The software adheres to rigorous code and execution protocols [7], [8]. The length of the bytecode decreases throughout the compilation process. Consequently, it exhibits superior performance on the Ethereum platform. The Ethereum programme operates in a state of isolation from both network and the file system.

2.2 Blockchain Layer

The process of reaching an agreement is a basic and essential aspect within the context of BC technology. A consensus technique is employed to determine a verified set of entity commitments. Based on the prevailing view, a significant majority of the nodes exhibit a high degree of accurate alignment. The consensus processes used in BC systems exhibit variations contingent upon the specific sort of BC being utilized. The consensus method may be classified as deterministic when it is implemented inside an uncontrolled BC network, such as Ethereum, Bitcoin, and other similar platforms. While it is possible for several parties to have divergent perspectives on a block inside the BC's, the presence of consensus mechanisms guarantees the integrity and precision of the ledger. Permitted BCs, like as Hyperledger, use deterministic methodologies.

2.3 Network Layer

It is responsible for the identification and dissemination of transactions, as well as the distribution of blocks, inside the IoT ecosystem. This implies that the nodes will autonomously identify one another and establish connections, facilitating the exchange and transmission of data to improve the BC system as it stands right now. The P2P platform is a decentralised network that facilitates the sharing of devices and the redistribution of system burdens. Endpoints are responsible for the execution of transactions inside a BC system. Two different kinds of nodes within a network: full nodes and light nodes. 1st nodes provide much functionality such as

exchange confirmation, identification, processing, and adherence to consensus rules. The responsibility of these nodes is to maintain the integrity and reliability of the system. The 2nd nodes have the capability to transmit the header of the BC as well as perform actions for submitting data.

2.4 Data Link Layer

The BC may be developed as a sequential data structure composed of interconnected blocks, each of which captures an assortment of systematically arranged transactions. The Merkle tree is a binary tree structure that employs hash codes. Every block on the BC has a Merkle root hash along with many bits of information, comprising the block versions, timestamp, nonce, hash of the previous block, and difficulty level at that moment. Merkle trees, the use of cryptography and methods for consensus are essential components that underpin distributed ledger system. The use of root hashing possesses the ability to include the whole of the tree network. Every block comprises a comprehensive record of several transactions that have happened after the prior transaction. The present condition of the BC is reflected in the root hashing when these transactions are recorded.

2.5 Hardware Layer

BC are potentially useful for the purpose of systematically quantifying, validating, and archiving transactions inside a decentralised database. In a P2P system, each computer is an endpoint. The endpoints serve the purpose of validating transactions, arranging them into blocks, and then uploading to the BC system, among other functions. To create said layer, a virtualized layer is utilised. The nodes play a crucial role inside this layer. Within the framework of a BC system, a computer is often denoted as a node. The aforementioned nodes are key components of a decentralised and distributed BC infrastructure.

3. Current Trends In Bc-Iot Development

The BC technology has garnered a great deal of interest because to its safe method of conducting transactions between several organisations without relying on a trusted intermediary, as well as its capacity to verify the veracity of information. despite the prevailing consensus among analysts regarding the potential of BC technology to mitigate various challenges in the intrinsically insecure realm of the internet, particularly in relation to privacy and security, there appears to be a dearth of extensive scholarly inquiry that rigorously examines and evaluates BC from diverse vantage points [9] . The advent of BC technology transpired in the year 2009, during a very brief span of less than a decade. The worldwide scene underwent a rapid transition as a consequence of this notable discovery. The use of BC technology is becoming prevalent throughout many professional sectors, including retail, healthcare, and scientific domains.

3.1 Federated BC

The concept of federated BC has emerged as a prominent and efficacious breakthrough within the realm of BC technology in recent times. This enhanced approach to the fundamental BC foundation makes it very suitable for a diverse range of pertinent applications. The increasing popularity of federated BC may be attributed to its the capacity to supply a more flexible approach for private BC. Federated BC's exhibit similarities to private BC's in several aspects, while also possessing some marginal benefits. These BC's exhibit enhanced speed (increased scalability) as well as enhanced transaction privacy. A number of industries have federated BCs, including the banking sector (R3), the energy sector (EWF), the insurance sector (B3i), and other similar industries.

BC Interoperability

Interoperability pertains to the seamless communication between various BC networks and infrastructure frameworks for information and other types of content. The accessibility of information stored on several BC's was facilitated by this particular feature[10], [11] . This technology facilitates the seamless and expeditious transmission of payments across different BC networks for subscribers. In addition, this feature incorporates supplementary capabilities, including cross-chain transactions. Furthermore, the enhancement of multi-token transactions may be achieved via the creation of wallet services with multiple tokens.

3.4 Social Networking

BC's integration into social networks has promise in tackling several issues, such as heated discourse, privacy breaches, manipulation of information, and content significance. As a result, the incorporation of BC technology into the architecture of social media platforms is now being recognised as an innovative technical phenomenon. Tokens are used by social networks for a multitude of functions. As a result, media firms are motivated by financial incentives to provide content and improve network efficiency. Token transactions, which are enabled by the use of BC technology, exhibit high efficiency and near-instantaneous execution, while also being free from any accompanying transaction costs

4. Concerns At Every Level

Three levels are usually present in an IoT standard design: the network layer, the perception layer, and the application layer [12]. The importance of the support or middleware layer increases with the importance of data processing and intelligent decision making at the network and application levels. Cloud computing has been used as the foundational infrastructure in various research investigations pertaining to IoT systems [13]. Here we will discuss different security issues at each IoT layer [14], [15]

4.1 Perception or sensing layer

Sensors and other devices are part of this layer, also referred to as the sensing layer. This layer has restricted memory, processing, storage, and communication capabilities. To increase security in the Internet of Things network, this layer mainly uses node authentication and access control with weak encryption. [16], [17]. Examples of privacy breaches that target the perceiving layer are common in modern society.One method of implementation involves assuming control of a certain node. Other approaches include malware, data injection, replay attacks, and side-channel attacks. In the event that an assailant gains control of a node, it will cease transmitting legitimate network data and perhaps discontinue use of the IoT security protocol. The functionality of the IoT application may be hindered if it gets inaccurate data or experiences a security breach due to the introduction of malicious code. Eavesdropping, also known as sniffing or snooping, allows a perpetrator to intercept and review the data being transferred between two devices. [11] .

4.2 Networking and Data Communications Layer

Integrity, confidentiality, and privacy are this layer's primary objectives. Illicit activities such as phishing, DDoS attacks, and attacks on identity authentication, data transit, routing, and encryption are expected to appear at this specific layer. IoT under consideration is particularly susceptible to phishing attempts, which are designed to illicitly acquire confidential data, including passwords and login credentials. The occurrence of an access assault, sometimes referred to as a continuous advanced threat, takes place when an unauthorised user or hacker effectively gains access to the Internet of Things network while collecting and sending private information using IoT apps.

Middleware or Support Layer

Performance and reaction time have improved as distributed computing technologies replace centralised cloud environments. This must be done thoroughly examination of every transmitted data in order to ensure its correctness, conciseness, and confidentiality.

The act of intentionally modifying or pilfering data or information by an individual inside a network is an example of malicious insider attack [12]. A virtualization assault occurs when the harm inflicted against one virtual machine extends to affect another. Through the use of cloud malware injection techniques, an unauthorised individual may gain control over a cloud service, introduce harmful code, or perhaps fabricate a counterfeit virtual machine. The potential ramifications would be substantial if the intensity of assaults reaches a level where cloud infrastructure experiences profound frustration.

4.3 Application Layer

The application layer encompasses the definition and management of IoT applications, as well as their interactions with individual customers. One method of using IoT services involves the use of a user interface. Any Internet-capable smart device, like a computer or smartphone, can serve as an interface. The middleware layer processes data, which is then used by the application layer. The security requirements of an application may vary based on its operational characteristics. In the context of transmitting climate change projections vs engaging in online banking activities, it is reasonable to anticipate a higher standard of security. The application layer is confronted with a multitude of security concerns, encompassing but not restricted to assaults on access control, the presence of malicious code, programming-related issues, data leakage, disruptions in service provision, vulnerabilities inside applications, and faults in software [18].

5.1 Authentication Techniques in IoT:

- **Password-Based Authentication:** Simple username/password combinations can be used for authentication. However, this method is vulnerable to password-related issues such as weak passwords, password sharing, and eavesdropping.
- **Public Key Infrastructure (PKI):** PKI involves the use of public and private key pairs for secure communication. Devices are issued digital certificates, and the authenticity of these certificates can be verified during communication. **OAuth (Open Authorization):** OAuth is commonly used for third-party authentication, allowing devices to access resources on behalf of the user. It's widely used in IoT scenarios where devices need to interact with cloud services. **Biometric Authentication:** Biometric information, like facial recognition or fingerprints, can be used to authenticate users or devices. This method is more secure as it relies on unique biological characteristics.
- **Token-Based Authentication:** Tokens can be used to authenticate devices. A token is typically a unique identifier issued by an authentication server, and it can be used for a specific duration or until the session is terminated.

➢ **Authentication Techniques in BC:**

- **Public and Private Key Cryptography:** Similar to PKI in IoT, BC relies heavily on cryptographic techniques. Participants in a BC network use public and private keys to sign transactions and prove ownership. **Smart Contracts**: Self-executing contracts, or smart contracts, have their terms encoded directly into the code. Smart contracts can incorporate authentication to automate certain tasks in response to predetermined parameters. Consensus Mechanisms: Proof of Work (PoW) and Proof of Stake (PoS) are two examples of consensus mechanisms that are used in BC for transaction authentication. Security is ensured by nodes in the network coming to an agreement regarding the legitimacy of transactions.
- **Multi-Signature (Multisig) Wallets:** Several private keys are needed in multisig wallets in order to approve a transaction. This adds an extra layer of security, especially in enterprise and financial applications. Permissioned BC s: In permissioned or private BC s, access is restricted to authorized participants. Participants are authenticated before they can join the network, providing a controlled environment.
- **Decentralized Identity (DID):** DIDs allow individuals and entities to have control over their identities. This is achieved by creating verifiable, self-sovereign identities that can be used for authentication without relying on central authorities.

BC technology plays a pivotal role in enhancing authentication and confidentiality within IoTnetworks, particularly when coupled with chaotic maps and Physical Unclonable Functions (PUFs).

5.1 Chaotic map

Initial circumstances affect chaotic maps, nonlinear dynamical systems. Thus, even slight modifications in chaotic map beginning conditions might produce very different results. This property makes chaotic maps well-suited for cryptography, as they can be used to generate keys that are difficult to predict or reverse engineer.

5.1.1 Chaotic map-based Anonymous User Authentication

The concept of chaotic maps in security often involves the use of chaotic systems, which are highly sensitive to initial conditions, making them unpredictable. This unpredictability can be harnessed for cryptographic

applications. Anonymous user authentication typically focuses on verifying the identity of a user without revealing sensitive information. Mathematical chaotic maps are susceptible to initial conditions. Therefore, even a slight change in a chaotic map's initial conditions can modify its output. This property can be used to generate highly secure random numbers, which can then be used to authenticate IoT devices.

Here's a broad outline of how a chaotic map-based anonymous user authentication system might work:

5.1.2 Key Generation:

Users get cryptographic keys from chaotic maps.

- **Anonymous Credentials:**

The system would create anonymous credentials for users, possibly based on the chaotic properties of the map. These credentials might not directly reveal the identity of the user but could be used for authentication.

- **Authentication Process:**

During authentication, the user presents their credentials, and the system employs the chaotic map to verify the authenticity of these credentials.

- **Unlikability:**

The chaotic nature of the map may contribute to making the authentication process unlinkable, meaning that even if the authentication is successful, it does not reveal the user's actual identity.

- **Secure Communication:**

Once authenticated, the user can communicate securely within the system without revealing sensitive information.

- **Dynamic Systems:**

Chaotic maps are often dynamic systems, and their parameters may change over time. This dynamism could make it harder for unauthorised access, adding security entities to predict or manipulate the authentication process. It's important to note that the details and effectiveness of such a system would depend on the specific implementation, the characteristics of the chaotic map used, and the cryptographic protocols applied.

5.1.3 Comparative Study of Chaotic Maps

When it comes to hardware security, healthcare, the IoT's, and autonomous vehicles, the research that has been presented demonstrates an exhaustive investigation of a variety of cryptography and authentication approaches that have been applied to these different fields. There is a huge research gap in the process of synthesizing these different techniques into a coherent framework that addresses the broader difficulties connected with the rising complexity and diversity of secure communication systems. This is despite the fact that each study makes a significant contribution to its respective field. In spite of the fact that different research delves into specific facets of cryptography, authentication, and security, there is an opportunity to bridge these discoveries into an overall framework that is capable of catering to the myriad of requirements that current applications have. To ensure compatibility, scalability, and robustness across a wide range of use cases, it is necessary to conduct exhaustive research prior to integrating and expanding the solutions that have been suggested. Furthermore, such an integrated framework has the potential to give insights into the interaction between various cryptographic primitives and authentication mechanisms, which would greatly facilitate the creation of security solutions that are both more robust and versatile for developing technologies.

Table 1: Comparison of Chaotic Maps

Author	Focus	Finding
[19]	Highly secured hardware authentication designs using PUFs or POKs, exploring chaos theory for	PUF cryptographic keys have a small, straightforward design that makes them suitable for low-cost reprogrammable

	PUFs, novel design of chaotic circuit.	devices. They are generated from a chaotic circuit by using time in a feedback loop. Chaotic circuit PUFs provide notably different keys and operate in both sophisticated FPGAs and basic CPLDs.
[20]	Lightweight cryptography-based authentication framework (CMAF-IIoT) for IIoT using ASCON, addressing privacy concerns and computational constraints.	CMAF-IIoT enables secure communication in IIoT, utilizes chaotic map and ASCON for authentication. The framework's security is confirmed by both official and informal security analyses. Comparing CMAF-IIoT to other frameworks, it demonstrates low costs for computation, storage, and communication.
[21]	Healthcare information system security using extended chaotic map, ID-based key negotiation, and BC for data integrity.	Proposed mechanism protects data storage process, complies with HIPAA regulations, and ID-based key exchange utilising expanded chaotic map capabilities. uses BC for non-tamperability, which requires less computing power than multiplication of elliptic curve points.
[22]	Chaotic map-based authenticated key agreement (CMAKA), a model for the Internet of Autonomous Vehicles (IoAVs), allows for secure remote control of AVs.	CMAKA method establishes a secure communication channel through session key negotiation, employs a PUF for authentication. Outperforms other three-factor authentication schemes in both security and total cost.
[23]	Biometric Authentication Frameworks (BAFs) for IoT security, HAES-CM scheme with Chaotic Map Encryptions.	BAFs use fingerprint authentications on edge devices, HAES-CM scheme ensures private and secure communications. Evaluation shows the proposed encryption strategy outperforms others in processing speeds.
[24]	User-authenticated key agreement scheme for IIoT using fuzzy extractor technique, three-factor authentication, and lightweight nature.	The suggested system allows for smart card revocation, password and biometric changes, and the addition of new devices. Security analysis, both formal and informal and AVISPA tool verification demonstrate the scheme's efficiency and superior security.
[25]	CLIENT system for secure and energy-efficient communication in IoT using BC , chaotic Elgamal authentication using maps, grouping, and deep learning.	The processes included in the proposed system are signature-based enroute filtering, credit score-based clustering, packet routing based on capuchin search optimisation, chaotic map-based Elgamal authentication, and anomaly packet detection based on deep learning.

		Achieves superior performance in various metrics compared to existing works.

IoT authentication using chaotic maps and BC offers several benefits over traditional authentication schemes, including:

- **High security:** Chaotic maps are difficult to predict or reverse engineer, and BC is tamper-proof and transparent.
- **Scalability:** BC can be used to manage a large number of keys, making it well-suited for IoT applications.
- **Decentralization:** BC is decentralised. The assault resistance increases.

5.2 Classification of malicious nodes using PUF technique

PUF exploits physical variances in silicon chips to create unique identifiers or cryptographic keys. The use of PUFs for the classification of malicious nodes in a network can enhance security by providing a hardware-based, unique fingerprint for each device. Here's a general classification process using PUFs:

- **PUF Enrolment:**

During the manufacturing process or device initialization, each node's PUF is characterized, and a unique identifier is generated based on the inherent variations in the hardware.

- **PUF Response Generation:**

When the device needs to prove its identity, it generates a response from the PUF. The response is derived from the unique physical characteristics of the device.

- **Secure Communication:**

PUF responses can be cryptographic keys or a part of a secure communication protocol. This ensures that the communication is not only authenticated but also linked to the unique physical characteristics of the device.

- **Challenge-Response Mechanism:**

To prove its authenticity during communication, the device may be challenged with a random input, and it must provide the corresponding PUF response. This challenge-response mechanism adds an extra layer of security.

- **PUF-Based Classification:**

During network operation, the PUF responses can be used to classify nodes as legitimate or potentially malicious. Deviations in PUF responses may indicate tampering or the presence of a malicious node.

- **Machine Learning Integration:**

Machine learning algorithms can be employed to analyze the patterns in PUF responses. By training a model on known responses from legitimate nodes, the system can identify anomalies and classify nodes as potentially malicious based on deviations.

- **Behavioral Analysis:**

PUF responses can be used not only for authentication but also for behavioral analysis. Deviations in the behavior of PUF responses over time may indicate malicious activities.

- **Real-time Monitoring:**

Continuous monitoring of PUF responses allows for real-time detection of potential threats. Sudden changes or irregularities in PUF behavior can trigger alerts for further investigation.

➢ **Integration with Existing Security Measures:**

PUF-based classification can complement other security measures within the network, such as firewalls, intrusion detection systems, and encryption protocols.

It's important to note that while PUFs provide a unique and hardware-based approach to authentication and classification, their effectiveness depends on the implementation and the security measures integrated into the overall system. Furthermore, to address potential vulnerabilities and guarantee the resilience of the PUF-based security solution, continuous research and evaluation are required.

5.3.1Comparison and Application of different types of PUFs for IoT authentication

Physically unclonable function is a tangible apparatus that produces "digital fingerprints" by using the inherent physical variances derived from the manufacturing process, based on device intrinsic factors. The aforementioned phenomenon may be described as a tangible entity that is manifested inside a tangible framework. This entity, when subjected to certain input, circumstances, or challenges, generates a digitally-defined fingerprint output or reaction. Ideally, the desired characteristic of the function is to possess cryptographic security and operate as a one-way function, producing a response in response to a provided challenge.

Table 2 illustrates several PUFs categorized by their categories and unique characteristics, which contribute to the improvement of authentication for the IoT context. Increasing the security of nodes and entities within a network is the aim of PUFs. To do this, PUFs may use both physical and application-based mechanisms to increase security. These systems require the application of error correction algorithms to obtain a consistent response from the PUF for the purpose of authenticating the digital signature.

Table 2: Comparison of different types of PUFs for IoT authentication

	Type	Name	Weak/strong	Reference	Comment
Special fabrication	Coating		Weak	[26]	fewer CRPs
	Optical		Strong	[27]	Hard to assess the uniqueness
Silicon PUF	Delay based	Arbiter	Strong	[27]	Vulnerable to attacks
		Ring oscillator	Weak	[28]	Needs large powder and space
	Memory based	Re-RAM	Strong	[29]	Very sensitive to environmental and voltage fluctuations
		Butterfly	Weak	[30]	Instable neighbouring will impact PUF reaction.
		SRAM	Weal	[31]	prone to side-channel assaults

Conclusion

Security issues are emerging as a result of the growing usage of IoT in our daily lives. Among the main issues is authentication. Conventional methods of authentication are inadequate and may result in a single point of failure. By facilitating efficient identification and authentication and avoiding single points of failure, BC technology can assist in resolving this problem. This review looked at the most recent advancements in BC technology integration in IoT. This work aimed to assess various PUF-based authentication mechanisms and Chaotic maps in IoT.

References

[1] S. Saxena, B. Bhushan, and M. A. Ahad, "Blockchain based solutions to secure IoT: Background, integration trends and a way forward," Journal of Network and Computer Applications, vol. 181. Academic Press, May 01, 2021. doi: 10.1016/j.jnca.2021.103050.

[2] S. Aldhaheri, D. Alghazzawi, L. Cheng, A. Barnawi, and B. A. Alzahrani, "Artificial Immune Systems approaches to secure the internet of things: A systematic review of the literature and recommendations for future research," Journal of Network and Computer Applications, vol. 157. Academic Press, May 01, 2020. doi: 10.1016/j.jnca.2020.102537.

[3] R. Vishwakarma and A. K. Jain, "A survey of DDoS attacking techniques and defence mechanisms in the IoT network," Telecommunication Systems, vol. 73, no. 1. Springer, pp. 3–25, Jan. 01, 2020. doi: 10.1007/s11235-019-00599-z.

[4] S. Singh, P. K. Sharma, B. Yoon, M. Shojafar, G. H. Cho, and I. H. Ra, "Convergence of blockchain and artificial intelligence in IoT network for the sustainable smart city," Sustain Cities Soc, vol. 63, Dec. 2020, doi: 10.1016/j.scs.2020.102364.

[5] B. D. Deebak and F. AL-Turjman, "Privacy-preserving in smart contracts using blockchain and artificial intelligence for cyber risk measurements," Journal of Information Security and Applications, vol. 58, May 2021, doi: 10.1016/j.jisa.2021.102749.

[6] T. Nepomuceno, T. Carneiro, P. H. Maia, M. Adnan, T. Nepomuceno, and A. Martin, "AutoIoT: A framework based on user-driven MDE for generating IoT applications," in Proceedings of the ACM Symposium on Applied Computing, Association for Computing Machinery, Mar. 2020, pp. 719–728. doi: 10.1145/3341105.3373873.

[7] C. Oham, R. Jurdak, S. S. Kanhere, A. Dorri, and S. Jha, "B-FICA: BlockChain based Framework for Auto-Insurance Claim and Adjudication," in 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), IEEE, Jul. 2018, pp. 1171–1180. doi: 10.1109/Cybermatics_2018.2018.00210.

[8] R. K. Perrons and T. Cosby, "Applying blockchain in the geoenergy domain: The road to interoperability and standards," Appl Energy, vol. 262, Mar. 2020, doi: 10.1016/j.apenergy.2020.114545.

[9] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," Future Generation Computer Systems, vol. 107, pp. 841–853, Jun. 2020, doi: 10.1016/j.future.2017.08.020.

[10] Savelyev, "Copyright in the blockchain era: Promises and challenges," Computer Law and Security Review, vol. 34, no. 3, pp. 550–561, Jun. 2018, doi: 10.1016/j.clsr.2017.11.008.

[11] Sullivan and E. Burger, "E-residency and blockchain," Computer Law and Security Review, vol. 33, no. 4, pp. 470–481, Aug. 2017, doi: 10.1016/j.clsr.2017.03.016.

[12] "https://www.statista.com/statistics/647523/worldwide-bitcoin-blockchain-size/".

[13] M. Ebrahim, A. Hafid, and E. Elie, "Blockchain as privacy and security solution for smart environments: A Survey."

[14] T. Nandy et al., "Review on Security of Internet of Things Authentication Mechanism," IEEE Access, vol. 7, pp. 151054–151089, 2019, doi: 10.1109/ACCESS.2019.2947723.

[15] IEEE Computer Society et al., IEEE 2018 International Congress on Cybermatics ; 2018 IEEE Conferences on Internet of Things, Green Computing and Communications, Cyber, Physical and Social Computing, Smart Data, Blockchain, Computer and Information Technology : iThings/GreenCom/CPSCom/SmartData/Blockchain/CIT 2018 : proceedings : Halifax, Canada, 30 July - 3 August 2018.

[16] S. Deep, X. Zheng, A. Jolfaei, D. Yu, P. Ostovari, and A. Kashif Bashir, "A survey of security and privacy issues in the Internet of Things from the layered context," Transactions on Emerging Telecommunications Technologies, vol. 33, no. 6, Jun. 2022, doi: 10.1002/ett.3935.

[17] B. B. Pannayagol and S. Deshpande, "Security in Internet of Things: An Overview," in Proceedings - IEEE International Conference on Device Intelligence, Computing and Communication Technologies, DICCT

2023, Institute of Electrical and Electronics Engineers Inc., 2023, pp. 243–248. doi: 10.1109/DICCT56244.2023.10110070.

[18] P. K. Donta, S. N. Srirama, T. Amgoth, and C. S. R. Annavarapu, "Survey on recent advances in IoT application layer protocols and machine learning scope for research directions," Digital Communications and Networks, vol. 8, no. 5. KeAi Communications Co., pp. 727–744, Oct. 01, 2022. doi: 10.1016/j.dcan.2021.10.004.

[19] K. Gołofit and P. Z. Wieczorek, "Chaos-based physical unclonable functions," Applied Sciences (Switzerland), vol. 9, no. 5, 2019, doi: 10.3390/app9050991.

[20] M. Tanveer, A. Badshah, A. U. Khan, H. Alasmary, and S. A. Chaudhry, "CMAF-IIoT: Chaotic map-based authentication framework for Industrial Internet of Things," Internet of Things (Netherlands), vol. 23, Oct. 2023, doi: 10.1016/j.iot.2023.100902.

[21] T. F. Lee, I. P. Chang, and T. S. Kung, "Blockchain-based healthcare information preservation using extended chaotic maps for hipaa privacy/security regulations," Applied Sciences (Switzerland), vol. 11, no. 22, Nov. 2021, doi: 10.3390/app112210576.

[22] J. Cui, J. Yu, H. Zhong, L. Wei, and L. Liu, "Chaotic Map-Based Authentication Scheme Using Physical Unclonable Function for Internet of Autonomous Vehicle," IEEE Transactions on Intelligent Transportation Systems, vol. 24, no. 3, pp. 3167–3181, Mar. 2023, doi: 10.1109/TITS.2022.3227949.

[23] Altameem, P. P, S. T, R. C. Poonia, and A. K. J. Saudagar, "A Hybrid AES with a Chaotic Map-Based Biometric Authentication Framework for IoT and Industry 4.0," Systems, vol. 11, no. 1, Jan. 2023, doi: 10.3390/systems11010028.

[24] J. Srinivas, A. K. Das, M. Wazid, and N. Kumar, "Anonymous Lightweight Chaotic Map-Based Authenticated Key Agreement Protocol for Industrial Internet of Things," IEEE Trans Dependable Secure Comput, vol. 17, no. 6, pp. 1133–1146, Nov. 2020, doi: 10.1109/TDSC.2018.2857811.

[25] S. Ramamoorthi, B. Muthu Kumar, and A. Appathurai, "Energy aware Clustered blockchain data for IoT: An end-to-end lightweight secure & Enroute filtering approach," Comput Commun, vol. 202, pp. 166–182, Mar. 2023, doi: 10.1016/j.comcom.2023.02.010.

[26] Institute of Electrical and Electronics Engineers., Hardware-Oriented Security and Trust, 2009, HOST '09, IEEE International Workshop on : date, 27-27 July 2009. IEEE, 2009.

[27] ACM Special Interest Group on Design Automation., IEEE Council on Electronic Design Automation., and IEEE Circuits and Systems Society., Design Automation Conference, 2007, DAC '07, 44th ACM/IEEE : 4-8 June 2007. IEEE, 2007.

[28] Shamsoshoara, "Ring Oscillator and its application as Physical Unclonable Function (PUF) for Password Management," 2019.

[29] Cambou and M. Orlowski, "PUF designed with resistive RAM and ternary states," in Proceedings of the 11th Annual Cyber and Information Security Research Conference, CISRC 2016, Association for Computing Machinery, Inc, Apr. 2016. doi: 10.1145/2897795.2897808.

[30] Proceedings, Design, Automation & Test in Europe : Dresden, Germany, March 24-28, 2014.

[31] S. Chakrabarti et al., 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC) : 7th-9th January, 2019, University of Nevada, Las Vegas, NV, USA.