International Journal of Engineering Trends and Technology
ISSN: 2231 – 5381 / https://doi.org/10.14445/22315381/IJETT-V71I1P214

Volume 71 Issue 1, 152-163, January 2023
© 2023 Seventh Sense Research Group®

Original Article

Blockchain Technology as a Possible Solution to IoT Security Issues

Houda Lhore[1], Kaouthar Bousselam[1], Oussama Elissati[1], and Mouhcine Chami[1]

[1]*Institut National des Postes et Télécommunications, STRS Lab., Rabat, Morocco.*

Corresponding Author : lhore.houda@gmail.com

Received: 27 November 2022 Revised: 14 January 2023 Accepted: 21 January 2023 Published: 24 January 2023

Abstract *- The Internet of things is the new generation of devices that use internet technology to communicate with each other, exchange information, and manage physical objects easily without needing any external intervention. With this novelty, the information generated in the network is massive and critical since it contains confidential information like banking information, personnel credentials, location and geographic information, and other sensitive data. As a result, the essential aspect of this system is ensuring security concerns such as privacy, confidentiality, authentication, and availability in order to implement and guarantee the IoT system's service with a high level of security. This paper provides an overview of the Internet of Things systems, architectures, and security matters. Thus, to address security concerns and get beyond IoT system limitations, a Global hybrid architecture that combines a software solution based on Blockchain technology and hardware security primitive, which is the Physical Unclonable Function (PUF), has been proposed.*

Keywords *- Authentication, Availability, Confidentiality, Physical Unclonable Function, Privacy.*

1. Introduction

Introducing connected devices into our daily lives simplifies things and presents a new perspective on the design and management of the services and applications provided by these devices. This innovation reaches various domains such as healthcare, renewable energy, the automotive industry, smart supply chains, and many others. It is also considered a key to the expanding digital economy.

Initiated in 1999, MIT Auto Identification Center founder Kevin Ashton introduced the idea of "the Internet of Things" [1] [2]. The Internet of Things, according to Ashton, "has the capacity to revolutionize the world, perhaps even more so than the Internet did" [3]. Later, the International Telecommunication Union (ITU) formally introduced the Internet of Things in 2005 [4]. There are numerous definitions of the IoT offered by numerous entities. Instead, the definition used most frequently as of 2012 by the ITU, "a global infrastructure for the information society is described as "allowing advanced services by connecting (physical and virtual) things based on existing and developing interoperable information and communication technologies" [5]. Figure 1 shows a glimpse of the evolution of the IoT architecture. Accordingly, the expectation presumes that communication can be done directly between devices, as shown in the future architecture, and the growth of IoT could well be reached by 2025 by 35 billion devices [6]. However, Gartner presumes that IoT devices may number 50 billion [7] in 2025.

All domains are taking advantage of this new concept. The IoT application lets users manage all objects in a highly intelligent way and in an intuitive manner, with the main goal of maximizing the benefits of data to gain money or make a decision after analyzing the information sent by the IoT ecosystem. In the literature, we can divide the domain applications of the IoT into six domains, as depicted in Table I.

To understand the IoT ecosystem, we must know that it starts from end devices/objects where the information is collected, such as sensors and mobile phones using sensing devices in the objects like RFID tags, smart sensors, and actuators, and ends in the cloud where data is handled, stored, and processed, which is a decentralized system. For some applications of the IoT, fog computing has been defined as an alternative to the cloud to store and analyze data. It is permitted to develop fog applications rapidly [8] [57] and bring the data store closer.

However, using centralized systems like cloud or fog environments represents a vulnerability and a weakness of the IoT ecosystem named a Single Point of Failure (SPF). But, we can find a case where data is analyzed in the

This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/)

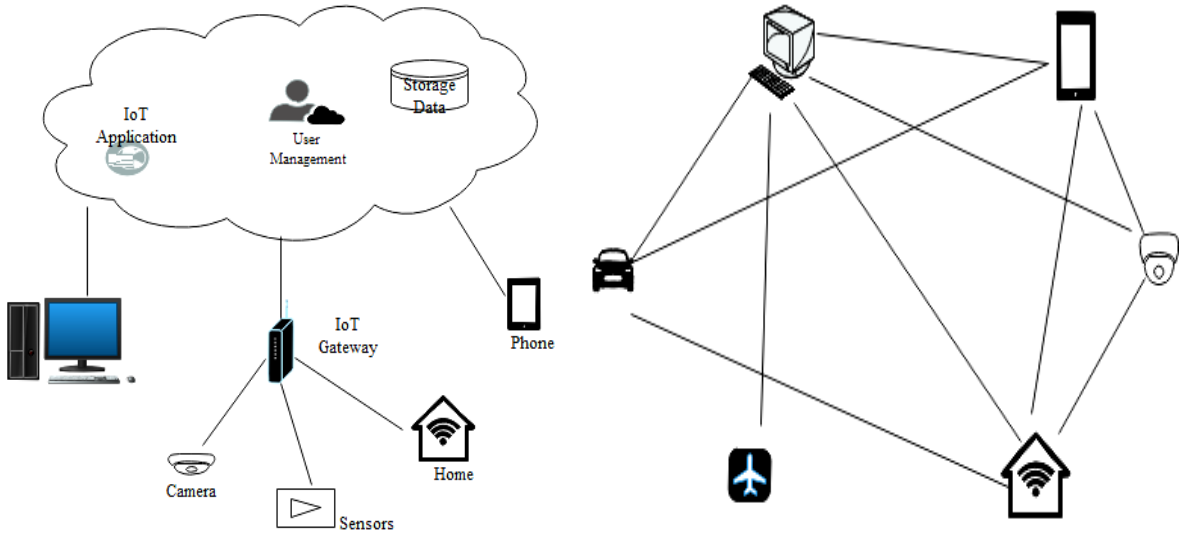

Fig. 1 Present and Future architecture of IoT

Table 1. Domain application of IoT

Domain	Application
Health Care	Remote patient monitoring is the most popular application to collect health data like: Temperature, blood pressure, heart rate, etc. So, an alert can be regenerate to inform the hospital.
Supply Chain	Real Time location tracking: in production also in transportation environment let have an efficient monitoring of product.
Food Industry	Most ailments need to be stored at a particular temperature. Thus, storage condition monitoring and smart refrigerator are the most important factors to insure.
Smart Grid	Using a smart metering system to supervise energy consumption in real time and automatically respond to the need.
Smart Manufacturing	Quality control, inventory management, Predictive Maintenance, smart metering and smart packaging are the most important axe in the manufacturing system.
IoV and UAV	With GPS navigation, a dash cam, a connection with a mobile permit to load more applications and a smart Driving Assistant the person can drive safer and easier. And also have visibility which road.

IoT itself by retaining useful data and removing unnecessary data. This time, the IoT application is built on hardware platforms such as Arduino and software platforms such as the following operating systems: Android, Lite OS [9], and Tiny OS [10], which give this ability.

Additionally, the IoT system incorporates a variety of technologies for communication like Near Field Communication (NFC) [11], Wireless Sensor Networks (WSN) [13], Radio Frequency Identification (RFID) [12], Bluetooth [14], Wi-Fi [58], Long Term Evolution [16] which are specified by a short range technology that facilitates the communication.

From where the Internet of Things is considered a heterogenic network that combines various devices with different technologies. In light of this, the IoT ecosystem is characterized by the network's complexity, a variety of devices, a diversity of IoT data and a centralized system.

Consequently, the above description of the IoT ecosystem led me to say that this wide diversity in the IoT system brings different issues which must be considered. Thus, the most important challenge is to get this data securely while guaranteeing privacy, availability and authenticity.

Hence, the security challenges of these “Things” are a crucial issue and the most difficult part to ensure in this ecosystem. Each security solution must consider the limitations of the resources of the connected objects “Things”, which can be summarized as follows: limited energy source, storage and computation.

This introduction aims to present a comprehensive discussion of the Internet of things ecosystem, its widespread features and constraints of IoT. The remaining of this article is written as follows: Section 2 gives an overview of different architecture of IoT systems in state of the art; Section 3 presents security issues and challenges of

the Internet of Things; Section 4 Introduces the Blockchain technology, there features and Types; Section 5 Describes the integrate of Blockchain technology into the IoT system and the new global architecture, and Section 6 concludes the paper.

2. IoT Architecture

Since its introduction, researchers have developed various architectures to represent the IoT system. The standard and basic ones are defined with only three layers according to the pile of TCP/IP. Thus, we also have a proposition of architecture that describe the network of IoT systems with 4 and 5 layers [59] due to the evolution of the IoT application and requirements. Figure 2 displays different architectures projected.

2.1. IoT Architecture with 3 layers

This architecture is considered a proposition at the beginning of the Internet of things [35], [36]. It contains the physical layer as the first, the network layer as the second and the application layers as the third:

- The Physical layer is known as the perception or sensing layer. It uses different technologies, such as RFID, to distinguish devices and gather information. The target of the attackers is the sensors that contain this information. In the literature, numerous types of sensors are picked according to the system's use case.

- The network layer is referred to transmission layer. It is located between the physical layer and the application layer. The role is to transmit the information gathered from physical objects via sensors using wireless or wired transmission support. It is also responsible for connecting intelligent objects, network devices, and networks between them.

- The Application Layer This layer designates the set of applications used by IoT technology. his functionality is to produce services to the software programs that depend on the data transmitted by sensors. The applications of IoT can be one of the domains set in table 1: smart homes, smart health, etc.

2.2. IoT Architecture with 4 layers

In this architecture, we find many suggestions with different placements of the fourth layer. The research presented in [37], [38], and [60] add a middleware layer between the Network layer and Application layer to define a software gateway/bridge that serves as an interface.

It can offer the application the necessary services. [38].

In other research, it is proposed as a supported layer responsible for the security of this architecture [59]. It is located between perception and network layers in a way to enhance the security of the IoT system by ensuring two functionalities: 1/- identify the sender of the information by authentication of the device and 2/- Send the information over the network layer.

2.3. IoT Architecture with 5 layers

In addition to the basic architecture, they add processing and business layers to provide more security for IoT systems.

Processing Layer: It receives data delivered from the Network layer, known as the Middleware layer. It treats the information gathered by eliminating additional information that does not make sense and extracting useful information. [59].

Business Layer: it is in charge of a variety of tasks. As a start, it administers the IoT system, including its services, applications and business models. Furthermore, it uses the information obtained from the application layer to create business models, etc. Additionally, it gives customers privacy [40]. Each layer of this architecture can be affected by various attacks.

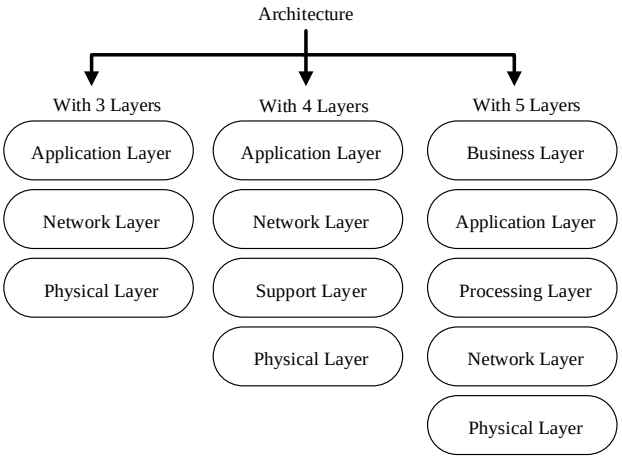

Fig. 2 Architecture of IoT 3,4 and 5 Layers

Table 2. Summary of attacks by Layers

Layer	Attacks	Impact	References
Business	Business attack, Zero-day attack	Integrity, Confidentiality	[17][18][19]
Application	Cross-Site Scripting, Malicious code	Integrity, confidentiality	[20]
Processing	Exhaustion attacks, Malwares	Integrity, confidentiality	[21][22]
Network	DoS attacks, Main in the Middle, storage attacks and exploitAttack, replay attack	Availability, integrity, confidentiality	[23][24] [25]
Supported	unauthorized access, Malicious insider, Dos Attacks	Authentication, Privacy, Confidentiality	[26][27]
Physical	Eavesdropping, Node capture, Fake node and malicious, replayattacks, Timing attacks	Authentication, Privacy, Integrity, Confidentiality	[28] [29] [30] [31][32][33]

Table 2 summarises these attacks and their impact on the system. Therefore, we must secure every layer to assure the security of the IoT system and provide different requirements to guarantee security matters.

3. Security Issues/ Challenges of the Internet of Things

As mentioned before, the biggest challenges in IoT systems are privacy and security concerns. Furthermore, several aspects of challenges exist:

- Heterogeneity: The IoT system reveals heterogeneity of devices, communication protocols and IoT data exchange.
- Poor interoperability: as a result of the heterogeneity of the IoT system, collaboration with different objects and exchanging information are very difficult and low to manage.
- Complexity of networks: the network contains different communication protocols like Bluetooth, 6Lowpan, Sigfox, LoRa, and NB-IoT give diverse services in the network.
- Privacy vulnerability: the exposing of private user data by devices in the IoT network leads attackers to manipulate and control the system and private life. So, we must guarantee the usage of IoT Data without revealing users' private information. Besides, using a cloud-like environment to store and compute the data generated by IoT seems to empower the IoT system. However, sending data to a third party can jeopardize the confidentiality of the data [41].
- Resource Constraints of Devices: The devices in the IoT system, like RFID tags, smart meters and sensors, have many limitations in resources: low storage, low power consumption and energy.
- Security vulnerability: Despite the system's heterogeneity and the complexity of the system IoT the security matter is the major element to ensure. Despite several mechanisms to ensure authentication, encryption communication and authorization, it is difficult to implement in the IoT device due to these resource limitations [42].

Consequently, the ultimate question is how we can deal with the limitation of IoT devices and get a secure and private system. Many solutions are proposed to deal with the computing task, like using edge computing in a device. To increase the benefit of using IoT devices, we must enforce the security of IoT systems and mitigate the risk. With the outcoming of Blockchain technology, the integration of this solution seems to be a solution to these challenges, as we saw before, like poor interoperability, "all devices can speak the same language", privacy and security.

4. Blockchain

4.1. Blockchain Concepts

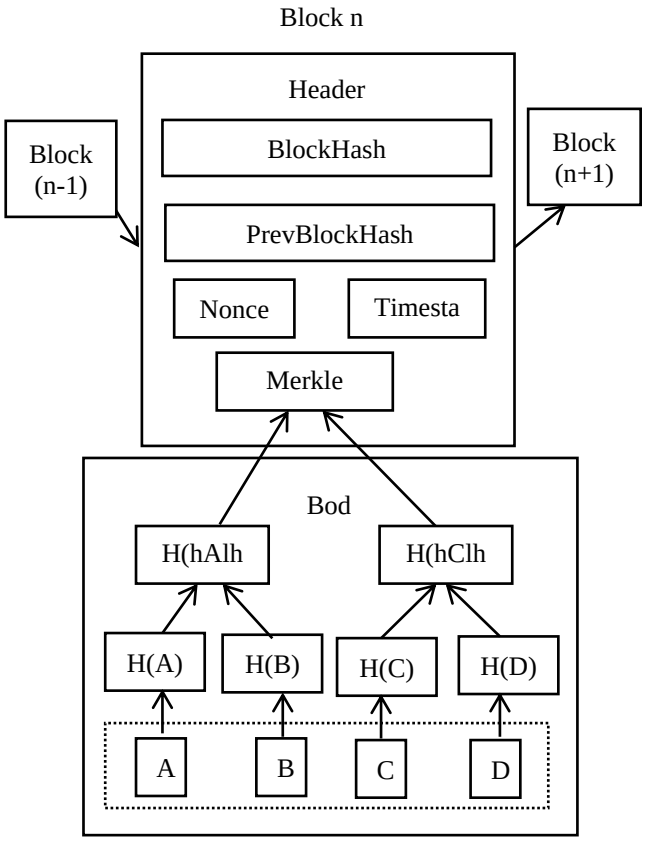

Fig. 3 Representation of block and his field

Recently, the blockchain has been rising as a new technology that ensures privacy, immutability, integrity, and availability of information while providing a distributed and decentralized system that does not depend on a third party. To begin, it was dedicated to the Bitcoin cryptocurrency to ensure transactions between actors and user anonymity. Based on a Peer-to-Peer network (P2P), blockchain is also defined as an immutable Distributed Ledger that shares the same database with all Blockchain network members named "NODE". This database stores a set of chained blocks; the first one is called a genesis block, with a previous hash of it being 0000 [43]. A single block contains two elements named "header" and "body," as shown in Figure 3. The body stores the transaction under a specific structure defined by the Merkle tree as a method. The main goal of using the Merkle Tree is to facilitate the transaction verification by verifying the Merkle Tree Root stored in the block's header.

The header in his text contains this information: 1/Block hash that defines the ID of the transaction 2/the previous block hash, which permits it to be linked with the previous block like a chain. Hence, it helps to guarantee the integrity and immutability of its contents. 3/Timestamp, which defines the recording time of the transaction 4/Nonce, is a random value that starts from 0 and increases for every hash calculation [6]. 5/MerkleRoot is the hash of all the hashes of all the transactions that are part of a block in a Blockchain network, which guarantees the integrity of the transaction. With those fields, it is easy to detect a tampered transaction without needing a computational effort since we compare the hashes produced.

In some situations, the Blockchain network's nodes can create a valid block at once, leading to a forked Blockchain. In such a case, we consider the correct one the longest chain that must be maintained while the other chain must be discarded or orphaned [44]. Blockchain technology uses two important mechanisms of security. The first one is the use of cryptography asymmetric based on two keys, private and public-key, to provide a digital signature and specify the owner of the message sent. We encrypt data with a private key that is kept confidential, and we share a public key in the network to be used in the verification of the provenance of the data [45]. The second mechanism is a cryptographic hash function to realize consensus between network nodes on Blockchain data. As a result, by utilizing these mechanisms, Blockchain technology provides a powerful system with a high level of security.

4.2. Consensus Algorithms

The consensus algorithm is a decision-making process for a group and a common agreement among the nodes without a need for centralized authorities, where group members create and support the beneficial decision for the group as a whole. These algorithms' fundamental goal is to choose a leader who will validate and broadcast the new data block via the network. Thus, all nodes belonging to the network participate in the validation process. With this mechanism, we ensure that the next added block is good. In state of the art, we find several kinds of consensus algorithms shown in figure 4; the most popular are:

- Proof of Work "PoW" is the vast consensus mechanism deployed on the public Blockchain platform. It is introduced by Bitcoin [13] and presumes that each peer votes based on his Computing Power to solve a proof of work, calculating the hash function to find the nonce value and constructing the appropriate blocks [18], and the node receives a reward after resolving the puzzle. The nodes participating in this process are named "Miners", and the entire process is called "Mining." So, after finding the correct hash, the miner broadcasts the message to the other node for verification of the hash value found. Once it is accepted, the other network nodes set the next block. Despite his powerful ability to keep attackers from intruding with the sequence of blocks [46], the ultimate challenge of this consensus needs a large power consumption to complete the process, and the nodes which dispose of the intensive resources may monopolize the network as well as the reward.

- Proof of Stuck "PoS": is considered an alternative consensus approach for public blockchain with low power consumption for solving puzzles. Proof of stack aims to have an economic share in the network. In PoS, we replaced the term miners with validators. Like proof of work, the validators choose to add or broadcast a block into the blockchain. So, the validator selection is based on how many coins are held in the node wallets. However, the proof of stack system also uses randomization or a coin age-based strategy to ensure that those with the biggest stakes do not always receive preference and priority [45].

- Delegated Proof of Stuck "DPoS" is another form of proof of stake. It is extensively used in Ethereum technology. It provides a voting system in which users are called to vote to elect users who will validate the blocks in their place "with salary". In this algorithm, minors are called delegates. In the event that the validators add a wrong transaction or lose blocks, they are voted out by the other members of the network, and the rest of the token holders and new delegates are selected. When it comes to performance, DPoS Blockchains are more scalable and can handle numerous transactions per second than PoW and PoS. [47].

- Practical Byzantine Fault Tolerance "PBFT" is employed in a private Blockchain. The PBFT algorithm provides safety and liveness properties given that at most

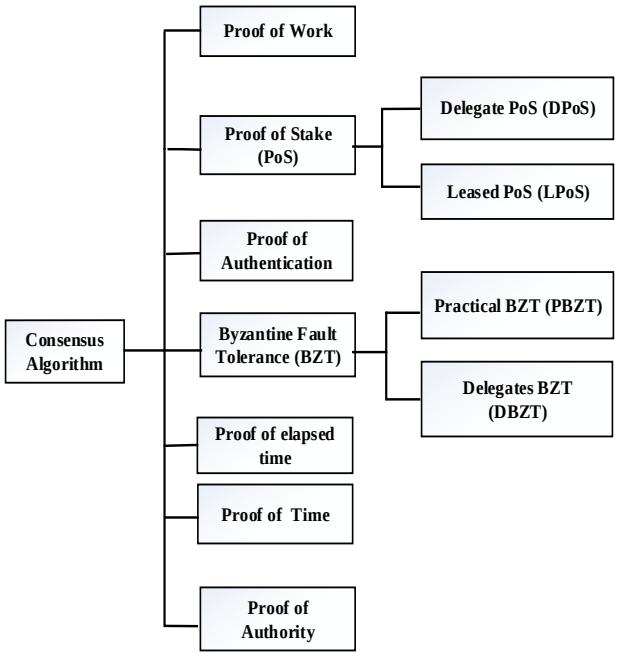

Fig. 4 Consensus Algorithm

[(m-1)/3] of m nodes are Byzantine. Several cryptocurrency platforms employ PBFT consensuses like Hyperledger Fabric, Tendermint and Ripple platrorms [48].

4.3. Smart Contract

Stored on the blockchain, a Smart Contract is a kind of code/program that might be executed automatically to the terms of contracts, unlike traditional contracts that are enabled by a centralized authority. This concept has existed in literature since 1994. This functionality's main objective is to codify contractual terms and implement them in software or hardware to minimize the need for intermediary parts, such as production in the supply chain [49] [50]. With this functionality, the blockchain gains immutability and decentralization features.

4.4. Features of Blockchain

Blockchain is a distributed ledger with high-security performance, as illustrated in figure 5:

- Decentralization: The validation transaction in a traditional system can be conducted by a trusted authority (such as a bank or government). The centralization of this action is the genesis of a bottleneck in the network and the single point of failure (SPF). However, blockchain allows transactions to be validated between network nodes without any validation by tiers, reduces the single point of failure risk, minimizes the service cost, and mitigates the performance bottleneck.
- Traceability: Each block in the blockchain contains a field named “Timestamp.” This field records when the transaction occurs. Thus, a timestamp is associated with every transaction stored in the blockchain. That is why it is easy for users to know the transaction's origin.
- Immutability: Each block in the blockchain has a hash of the one before it. So, any change to a block causes all the following blocks to be rejected. Therefore, The Merkle tree's root hash stores the hash of all committed transactions. Every minor change in any transaction results in the creation of a new Merkle root.
- Non-repudiation: it is realized by the secret key employed to encrypt and sign the transaction, which the other nodes can verify by the associated public key. Consequently, the transaction initiator cannot reject the cryptographically signed transaction [6].
- Pseudonymity: By making Blockchain addresses anonymous, blockchain can provide a certain level of privacy. [6] demonstrates the use of Blockchain technology to protect user privacy.
- Transparency: every user on the Blockchain network has equal rights to access data. The blockchain offers transparency to all participants of the network. Meanwhile, the new transaction is verified by all nodes of the network.
- Fault tolerance: by sharing the database with all nodes in the network, you can easily identify data leaks. A consensus mechanism can detect any alteration of data.
- Exchange automation: with smart contracts, the exchange of messages between vehicles can be automated.

4.5. Types of Blockchain

Blockchain technology is divided into three types: public, private, and consortium [54] [56]. Each one is used in a different context or situation:

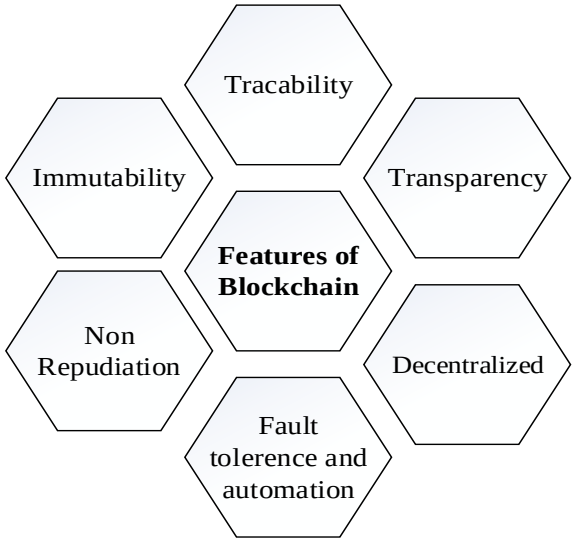

Fig. 5 Features of Blockchain Technology

Table 3. Summary of Blockchain-type comparisons

	Type of Blockchain		
	Public	Private	consortium
Participation in consensus	All participants'	Single firm	Selected
Access	read/write permission	restricted	restricted
Identity	anonymous	Known	known
Immutability	Yes	Partial	Partial
Trans. processing speed	Slow	Rapid	Rapid
Permissionless	Yes	No	No
Non-repudiation	Non-refusable	Refusable	Partially Refusable
Transparency	Transparent	Opaque	Partially Transparent
Traceability	Yes	Yes	Partially
Scalability	Poor	Superior	Good
Flexibility	Poor	Superior	Good
Consensus	PoW, PoS, PoX	PBFT, Tendermint, FBFT	Ripple
Examples	Bitcoin, Ethereum	Hyperledger	GemOS

4.5.1. Public Blockchain

Public blockchain also known as permissionless Blockchain [55] because it enables everyone to access a copy of the Ledger and take part in the process of validating new blocks [51]. The public blockchain includes bitcoin, Ethereum, and others in the literature. The specification in this type of blockchain requires that the node generate transactions anonymously, resulting in a decentralized structure.

4.5.2. Private Blockchain

Private blockchain named permissioned, it is used in an organization or enterprise with a subsidiary company where all nodes are known. It is a centralized structure but can use a form of blockchain to validate the transaction.

4.5.3. Consortium Blockchain

It is comparable to a Private one, where the blockchain platform is a permissioned platform that multiple organizations can govern. The features of this technology provide a faster output compared to a public Blockchain (a large number of users). The other features are that we don't have a problem with scalability because here, we have the capability to control nodes. It is also known as the federated blockchain.

Table 3 provide a summary comparison between the types of blockchain, which leads to the following conclusion:

The public blockchain offers a decentralized system with qualities such as immutability, transparency, traceability, and non-repudiation. Furthermore, an anonymous identity with full access to the blockchain is ensured. In addition, the network members require a significant amount of energy and storage to reach a consensus, so there is a high latency in creating a transaction. Therefore, the scalability of the public blockchain is limited. However, in private and consortium Blockchains, the scalability is superior due to the limited numbers of participants in those types. So the consensus is easily gained.

As we will see in a later section on Blockchain technology, the permissionless has a slower speed to create a block that results in high latency in the network while using a good performance and scalable network. On the other hand, the permissioned blockchain represents a slow latency but still has a limit in scalability features because of the number of members of this type of network. So two fields are important to choose which type of blockchain we choose: performance and scalability. With all this description, the permissionless blockchain is more advantageous for industrial applications, and private Blockchains are appropriate for enterprise solutions.

5. Integration of Blockchain and IoT Ecosystem

The principle of the suggested architecture is depicted in Figure 6. The proposed approach combines two technologies to reinforce the security from the physical layer to the application layer. Generally, the basic solution for security starts from the communication to the application layer. A Blockchain layer has been added between the application and network layers, and a PUF Layer has been added just before the Physical one. The Physical Unclonable Function (PUF) is an efficient solution for guaranteeing each device's identity and authentication, like a fingerprint in the Blockchain permit, secures the data exchange between each device in the Internet of Things system. In this way, we can ensure low latency, tractability, immutability, identification, authentication, data integrity and a low cost.

Making the notion more easily, the goal of IoT is to build an intelligent object using the Internet to communicate with each other in a way to collect information or provide services while keeping the security and privacy of information exchanged.

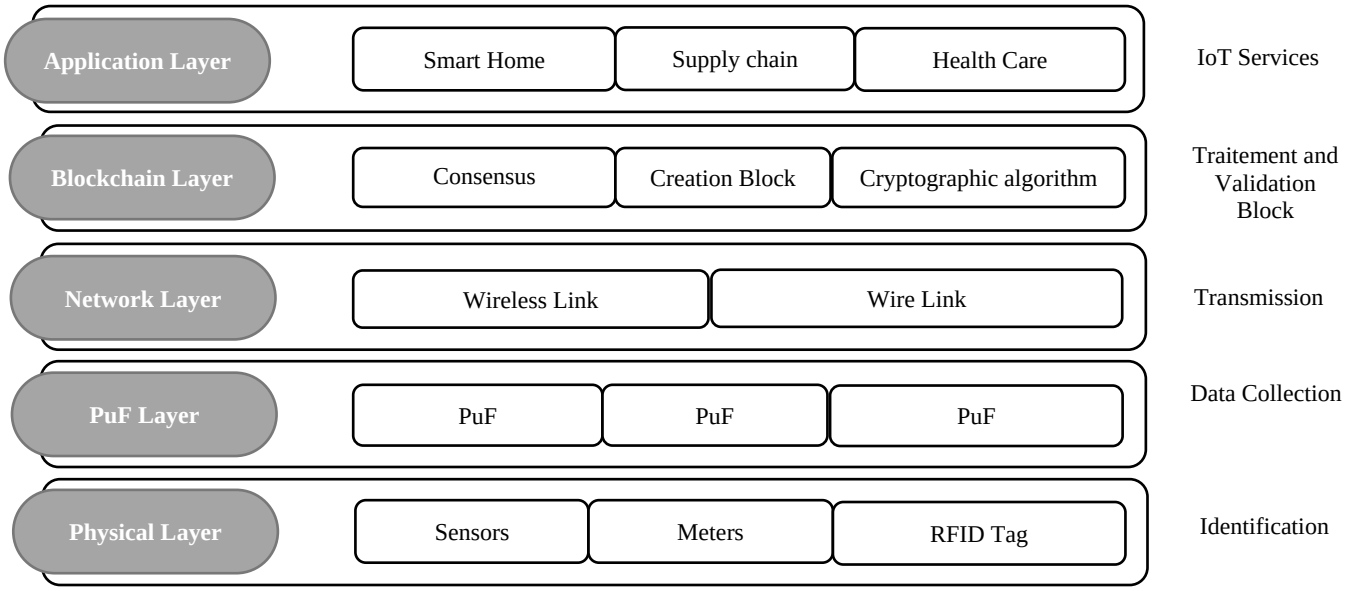

Fig. 6 Architecture IoT with Blockchain Technology

Due to the ubiquitous use of IoT services in all domains, the use of Blockchain technology in the IoT ecosystem represents a huge opportunity to overcome security and privacy matters.

To integrate Blockchain technology into the IoT ecosystem, we proposed to follow the steps below to define some parameters suitable for your IoT:

5.1. Type of Nodes

As we know, the full node can store the entire record of the blockchain and can be a validator and take action by adding a block to the blockchain. Hence, the node must have the sufficient computational power to participate in the validation process. In this case, the communication between objects is direct 'Machine to Machine' without any help such as Vehicle to Vehicle "V2V", payment cases and the implementation of the blockchain in each object. The light node holds a record of the block header from the blockchain. They can use the block header to check a transaction's legitimacy but cannot add a block. In conclusion, devices with limited resources can be used as light nodes. Hence, this kind of object uses a gateway or a fog computation to ensure communication and small computational task.

5.2. Consensus Algorithm

Choosing a suitable consensus algorithm is primordial to integrating blockchain with the IoT in a good way to benefit from all the advantages of this technology. Like proof of work, it needs a huge energy consumption to create and add a block, so it is very difficult to use it in IoT devices. In some studies, they proposed using a light version of PoW [37] while risking network security. The best way to use public blockchain in the IoT ecosystem is to use a voting-based consensus algorithm like Proof of Stake, which appears to be more appropriate with the constraints of IoT devices.

5.3. Smart Contracts

Smart contracts can automatically update each device's framework to overcome software system threats and automatically delegate access control.

For the location of blockchain, several studies provide a variety of scenarios: it may be in the device gateway, the device itself as "the endpoint," or in a hybrid structure utilizing the cloud [37] since it is thought of as a software solution that can be more easily deployed.

In this article, we proposed a global architecture. For that, we consider using the basic architecture with three layers in the first stage and appending to this scheme two layers called:

5.4. Blockchain Layer

Located at the top of the network layer and under the application layer, as shown in figure 6. Our goal is to assure the security of the information exchange in the network while accounting for the heterogeneity of connected devices, allowing them to communicate with one another and managing interoperability. The Blockchain Layer provides peer-to-peer communication and performs the consensus mechanisms to create blocks. It also contains the network of nodes contributing to the chain's validations. Otherwise, the ability to manage the account users related to

the physical equipment or transaction. We can say that the Blockchain layer contains tree functionality:

- Construction data using Merkel tree, cryptography and hash function with the primary goal of creating a block.
- Propagation of data through the network.
- Verification mechanism with consensus algorithm after agreement.

In real-world deployments, we have multiple designs due to the many types of devices and use cases discussed previously. The full node can be a cloud server for Internet of thing services or an edge server that provide a sufficient requirement to select useful data, store it in the blockchain and resolve consensus puzzles. As a result, the Blockchain layer is a virtual layer that can be established through existing infrastructure. Therefore, using this design, a device with limited resources may handle this proposition. For example:

- Smart house equipped with devices like “sensors, camera systems” that really can transmit data to an edge server but cannot support blockchain.
- Health Care, such as the remote monitoring of patient data health, in which the device is connected to a server and transmit the information.

Otherwise, the communication can be established Machine to Machine in use cases such as financial transactions and intelligent vehicles. Therefore, the device is powerful and may support the implementation of blockchain. In another scheme, the devices must communicate with an internet of things cloud or server through a gateway. This gateway has the role of collecting and trait the information and transmitting it to the IoT Cloud. In conclusion, our proposed architecture is valid, whatever the organization of devices.

5.5. PuF Layer

It is located between the physical layer and transmission layer. The introduction of the physically unclonable function “PuF” is suggested with the main goal of strengthening the device's security by guarantying the identity and ensuring authentication and unicity of the IoT in the network [61]. This primitive solution provides an unpredictable secret Key [53] that can replace the common secret key-based cryptographic methods and is practically impossible to duplicate. The PuF is a hardware solution containing a random component that makes them unclonable, like a fingerprint.

6. Conclusion and Future Work

This paper provides an overview of the state-of-the-art Internet of things, its architecture and its challenges. We also offer a summary of Blockchain technology in how it may be deployed to increase the security issues of the IoT system, considering different types of devices and proposing a global architecture for its deployment. The proposed solution is an approach that combines two technologies to reinforce the security from the physical layer to the application layer by including Blockchain and PUF layers in the standard architecture. The Physical Unclonable Function is an efficient solution for guaranteeing the identity and authentication of each device, like a fingerprint in the blockchain, which allows secure data exchange between each device in the Internet of Things system. Our future works will address the use of PUFs combined with Blockchain Technology. We are convinced that this proposed approach will contribute to overcoming security issues, establishing a secure data exchange, and guaranteeing the identification and authentication of devices fast, with low cost and low energy consumption in IoT systems.

References

[1] Elham A. Shammar, Ammar T. Zahary, and Asma A. Al-Shargabi, “A Survey of IoT and Blockchain Integration: Security Perspective. *IEEE Access*, vol. 9, pp. 156114–156150, 2021. *Crossref*, https://doi.org/10.1109/ACCESS.2021.3129697

[2] Gyanendra Prasad Joshi, and Sung Won Kim, “Survey, Nomenclature and Comparison of Reader Anti-Collision Protocols in RFID,” *IETE Technical Review*, vol. 25, no. 5, pp. 234-243, 2008.

[3] Hany Fathy et al., “Internet of Things: State-of-the-Art, Challenges, Applications, and Open Issues,” *International Journal of Intelligent Computing Research (IJICR)*, vol. 9, no. 3, pp.928–938, 2018. *Crossref*, http://dx.doi.org/10.20533/ijicr.2042.4655.2018.0112

[4] ITU, The Internet of Things, Technical Report, ITU, 2005.

[5] ITU, Overview of the Internet of Things, Technical Report, ITU, 2012.

[6] Hong-Ning Dai, Zibin Zheng, and Yan Zhang, “Blockchain for Internet of Things: A Survey,” *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8076–8094, 2019. *Crossref*, https://doi.org/10.1109/JIOT.2019.2920987

[7] Smita Dange, and Madhumita Chatterjee, *IoT Botnet: the Largest Threat to the IoT Network*, vol. 1049, pp. 150–170, 2019. *Crossref*, https://doi.org/10.1007/978-981-15-0132-6_10

[8] Jyoti Yadav, and Suman Sangwan, "Dynamic Offloading Framework in Fog Computing," *International Journal of Engineering Trends and Technology*, vol. 70, no. 7, pp. 32-42, 2022. *Crossref*, https://doi.org/10.14445/22315381/IJETT-V70I7P204

[9] Qing Cao et al., “The Liteos Operating System: Towards Unix-Like Abstractions for Wireless Sensor Networks,” *2008 International Conference on Information Processing in Sensor Networks (IPSN 2008)*, pp. 233–244, 2008. *Crossref*, https://doi.org/10.1109/IPSN.2008.54

[10] P. Levis, "TinyOS: An Operating System for Sensor Networks," *Ambient Intelligence*, pp. 115–148, 2005.
[11] Aswini N, Nagashree R. N, and Vibha Raob, "Near Field Communication," *International Journal of Wireless and Microwave Technology*, vol. 2, pp. 20–30, 2014. *Crossref*, https://doi.org/10.5815/ijwmt.2014.02.03
[12] Daqiang Zhang et al., " Real-Time Locating Systems Using Active RFID for Internet of Things," *IEEE Systems Journal*, vol. 10, no. 3, pp. 1226–1235, 2016.
[13] A. Whitmore, A. Agarwal, and L. Da Xu, "The Internet of Things a Surveyof Topics and Trends," *Information Systems Frontiers*, vol. 17, pp. 261–274, 2015.
[14] P. Mcdermott-Wells, "What is Bluetooth?," *IEEE Potentials*, vol. 23, pp. 33–35, 2004.
[15] Shyamala G et al., "Home Automation Security Using Blockchain," *SSRG International Journal of Computer Science and Engineering*, vol. 7, no. 7, pp. 63-68, 2020. *Crossref*, https://doi.org/10.14445/23488387/IJCSE-V7I7P111
[16] Garth V. Crosby, and Farzam Vafa, "Wireless Sensor Networks and LTE-A Network Convergence," *38th Annual IEEE Conference on Local Computer Networks*, pp. 731–734, 2013. *Crossref*, https://doi.org/10.1109/LCN.2013.6761322
[17] Nick Lewis, Business Logic Attack. [Online]. Avilable: https://www.techtarget.com/whatis/definition/business-logic-attack
[18] Leyla Bilge, and Tudor Dumitras, " Before We Knew It: an Empirical Study of Zero-Day Attacks in the Real World," *CCS '12 Proceedings of the 2012 ACM Conference on Computer and Communications Security*, CCS '12, pp. 833 – 844, 2012. *Crossref*, https://doi.org/10.1145/2382196.2382284
[19] Ratinder Kaur, and Maninder Pal Singh, "A Survey on Zero-Day Polymor-Phic Worm Detection Techniques," *IEEE Communications Surveys and Tutorials*, vol. 16, no. 3, pp. 1520–1549, 2014. *Crossref*, https://doi.org/10.1109/SURV.2014.022714.00160
[20] Shashank Gupta, and B. B. Gupta, "Cross-Site Scripting (XSS) Attacks and Defense Mechanisms: Classification and State-of-the-Art," *International Journal of System Assurance Engineering and Management*, vol. 8, no. 1, pp. 512–530, 2017. *Crossref*, https://doi.org/10.1007/s13198-015-0376-0
[21] Qazi Mamoon Ashraf, and Mohamed Hadi Habaebi, "Autonomic Schemes for Threat Mitigation in Internet of Things," *Journal of Network and Computer Applications*, vol. 49, no. C, pp.112–127, 2015. *Crossref*, https://doi.org/10.1016/j.jnca.2014.11.011
[22] Raymond Canzanese, Moshe Kam, and Spiros Mancoridis, "Toward an Automatic, Online Behavioral Malware Classification System," *2013 IEEE 7th International Conference on Self-Adaptive and Self-Organizing Systems*, pp.111–120, 2013. *Crossref*, https://doi.org/10.1109/SASO.2013.8
[23] P. Saxena, and V. Tiwari, "Network Security Attacks and Defence," *Journal of Computer and Information Technology*, vol. 9, no. 50–54, 2018.
[24] Mauro Conti, Nicola Dragoni, and Viktor Lesyk, "A Survey of Man in theMiddle Attacks," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, pp. 2027– 2051, 2016. *Crossref*, https://doi.org/10.1109/COMST.2016.2548426
[25] Mary K. Pratt, Cyber-Attack. [Online]. Available: https://www.techtarget.com/searchsecurity/definition/cyber-attack
[26] Ameya Sanzgiri, and Dipankar Dasgupta, "Classification of Insider Threat Detection Techniques," *Proceedings of the 11th Annual Cyber and Information Security Research Conference*, CISRC '16, Association for Computing Machinery, New York, NY,USA, 2016.
[27] Jason R.C. Nurse, "Smart Insiders: Exploring the Threat From Insiders Using the Internet-of-Things," *2015 International Workshop on Secure Internet of Things (SIOT)*, pp. 5–14, 2015. *Crossref*, https://doi.org/10.1109/SIOT.2015.10
[28] Hui Suo et al., "Security in the Internet of Things: A Review," *2012 International Conference on Computer Science and Electronics Engineering*, vol. 3, pp. 648–651, 2012. *Crossref*, https://doi.org/10.1109/ICCSEE.2012.373
[29] Denis Kozlov, Jari Veijalainen, and Yasir Ali, "Security and Privacy Threats in IoT Architectures," *BODYNETS*, pp. 256-262, 2012.
[30] Xu Xiaohui, "Study on Security Problems and Key Technologies of the Internet of Things," *2013 International Conference on Computational and Information Sciences*, pp. 407–410, 2013. *Crossref*, https://doi.org/10.1109/ICCIS.2013.114
[31] M. Vivekananda Bharathi, "Node Capture Attack in Wireless Sensor Network: A Survey," *2012 IEEE International Conference on Computational Intelligence and Computing Research*, pp.1–3, 2012. *Crossref*, https://doi.org/10.1109/ICCIC.2012.6510237
[32] Deepak Puthal et al., "Threats to Networking Cloud and Edge Datacenters in the Internet of Things," *IEEE Cloud Computing*, vol. 3, no. 3, pp. 64–71, 2016. *Crossref*, https://doi.org/10.1109/MCC.2016.63
[33] David Brumley, and Dan Boneh, "Remote Timing Attacks are Practical," *Computer Networks*, vol. 48, no. 5, pp. 701–716, 2005. *Crossref*, https://doi.org/10.1016/j.comnet.2005.01.010
[34] M. Selvavathi, and S.Edwin Raja, "Anticipation of Vulnerable Attacks in Vanet Using Blockchain Technique," *SSRG International Journal of Computer Science and Engineering*, vol. 8, no. 1, pp. 19-23, 2021. *Crossref*, https://doi.org/10.14445/23488387/IJCSE-V8I1P104
[35] Ibrahim Mashal et al., "Choices for Interaction with Things on Internet and Underlying Issues," *Ad Hoc Networks*, vol. 28, pp. 68–90, 2015. *Crossref*, https://doi.org/10.1016/j.adhoc.2014.12.006

[36] Miao Yun, and Bu Yuxin, "Research on the Architecture and Key Technology of Internet of Things (IoT) Applied on Smart Grid," *2010 International Conference on Advances in Energy Engineering*, pp. 69–72, 2010. *Crossref*, https://doi.org/10.1109/ICAEE.2010.5557611

[37] Ali Dorri et al., "Blockchain for IoT Security and Privacy: the Case Study of a SmartHome," *2017 IEEE International Conference on Pervasive Computingand Communications Workshops (Percom Workshops)*, pp. 618–623, 2017. *Crossref*, https://doi.org/10.1109/PERCOMW.2017.7917634

[38] Rafiullah Khan et al., "Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges," *2012 10th International Conference on Frontiersof Information Technology*, pp. 257–260, 2012. *Crossref*, https://doi.org/10.1109/FIT.2012.53

[39] Gokulahari.U et al., "Decentralized Application," *SSRG International Journal of Computer Science and Engineering*, vol. 7, no. 7, pp. 45-50, 2020. *Crossref*, https://doi.org/10.14445/23488387/IJCSE-V7I7P108

[40] Ibrahim Mashal et al., "Choices for Interaction with Things on Internet and Underlying Issues," *Ad Hoc Networks*, vol. 28, pp. 68–90, 2015. *Crossref*, https://doi.org/10.1016/j.adhoc.2014.12.006

[41] Jun Zhou et al., "Security and Privacy for Cloud-Based IoT: Challenges," *IEEE Communications Magazine*, vol. 55, no. 1, pp. 26–33, 2017. *Crossref*, https://doi.org/10.1109/MCOM.2017.1600363CM

[42] Rodrigo Roman, Jianying Zhou, and Javier Lopez, "On the Featuresand Challenges of Security and Privacy in Distributed Internet of Things," *Computer Networks*, vol. 57, no. 10, pp. 2266–2279, 2013. *Crossref*, https://doi.org/10.1016/j.comnet.2012.12.018

[43] Shiho Kim, and Ganesha Chandra Deka, *Advanced Applications of Blockchain Technology*, Springer, 2020.

[44] Mahdi H. Miraz, *Blockchain of Things (BCOT): The Fusion of Blockchain and IoT Technologies*, Springer, pp. 141–159, 2020.

[45] Hamed Haddadpajouh et al., "A Survey on Internet of Things Security: Requirements, Challenges, and Solutions," *Internet of Things*, vol. 14, 2021. *Crossref*, https://doi.org/10.1016/j.iot.2019.100129

[46] Md. Ashraf Uddin et al., "An Efficient Selective Miner Consensus Protocol in Blockchain Oriented IoT Smart Monitoring," *2019 IEEE International Conferenceon Industrial Technology (ICIT)*, pp. 1135–1142, 2019. *Crossref*, https://doi.org/10.1109/ICIT.2019.8754936

[47] Binance Academy, Delegated Proof of Stake Explained, 2021. [Online]. Available: https://academy.binance.com/en/articles/delegated-proof-of-stake- explained

[48] Beongjun Choi et al., "Scalable Network-Coded PBFT Consensus Algorithm," *2019 IEEE International Symposium on Information Theory (ISIT)*, pp. 857–861,2019.

[49] Konstantinos Christidis, and Michael Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292-2303, 2016. *Crossref*, https://doi.org/10.1109/ACCESS.2016.2566339

[50] Muhammad Nasir Mumtaz Bhutta et al., "A Survey on Blockchain Technology: Evolution, Architecture and Security," *IEEE Access*, vol. 9, pp. 61048–61073, 2021. *Crossref*, https://doi.org/10.1109/ACCESS.2021.3072849

[51] Muhammad Salek Ali et al., "Applications of Blockchains in the Internet of Things: A Comprehensive Survey," *IEEE Communications Surveys and Tutorials*, vol. 21, no. 2, pp. 1676–1717, 2019. *Crossref*, https://doi.org/10.1109/COMST.2018.2886932

[52] Sandeep Kumar, Abhay Kumar, and Vanita Verma, "A Survey Paper on Blockchain Technology, Challenges and Opportunities," *International Journal of Computer Trends and Technology*, vol. 67, no. 4, pp. 16-20, 2019. *Crossref*, https://doi.org/10.1109/COMST.2018.2886932

[53] Alexandra Balan et al., "A Puf-Based Cryptographic Security Solution for IoT Systems on Chip," *EURASIP Journal on Wireless Communications and Networking*, 2020. *Crossref*, https://doi.org/10.1186/s13638-020-01839-6

[54] E. Sweetline Priya, R. Priya, and R. Surendiran, "Implementation of Trust-Based Blood Donation and Transfusion System Using Blockchain Technology," *International Journal of Engineering Trends and Technology*, vol. 70, no. 8, pp. 104-117, 2022. *Crossref*, https://doi.org/10.14445/22315381/IJETT-V70I8P210

[55] Beena G Pillai, and Dayanandlal N, "Blockchain-Based Asymmetric Searchable Encryption: A Comprehensive Survey," *International Journal of Engineering Trends and Technology*, vol. 70, no. 7, pp. 355-365, 2022. *Crossref*, https://doi.org/10.14445/22315381/IJETT-V70I7P237

[56] Maha M. Althobaiti, "Blockchain Adoption Opportunities in Healthcare Sector," *International Journal of Engineering Trends and Technology*, vol. 68, no. 10, pp. 117-120, 2020. *Crossref*, https://doi.org/10.14445/22315381/IJETT-V68I10P220

[57] Aparna Kumari et al., "Fog Data Analytics: A Taxonomy and Process Model," *Journal of Network and Computer Applications*, vol. 128, pp. 90–104, 2019. *Crossref*, https://doi.org/10.1016/j.jnca.2018.12.013

[58] E. Ferro, and F. Potorti, "Bluetooth and Wi-Fi Wireless Protocols: A Surveyand a Comparison," *IEEE Wireless Communications*, vol. 12, no. 1, pp. 12–26, 2005. *Crossref*, https://doi.org/10.1109/MWC.2005.1404569

[59] Muhammad Burhan et al., "IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey," *Sensors*, vol. 18, no. 9, 2018. *Crossref*, https://doi.org/10.3390/s18092796

[60] Fatma Alshohoumi et al., “Systematic Review of Existing IoT Architectures Security and Privacy Issues and Concerns,” *International Journal ofAdvanced Computer Science and Applications*, vol.10, no. 7, 2019. *Crossref*, https://dx.doi.org/10.14569/IJACSA.2019.0100733

[61] Muhammad Aman, Kee Chua, and Biplab Sikdar, “Position Paper:Physical Unclonable Functions for IoT Security,” pp. 10–13, 2016. *Crossref*, https://doi.org/10.1145/2899007.2899013