© Universiti Tun Hussein Onn Malaysia Publisher's Office

JSCDM

Journal of Soft Computing and Data Mining

Journal homepage: http://penerbit.uthm.edu.my/ojs/index.php/jscdm
e-ISSN : 2716-621X

Security Enhancement of IoT and Fog Computing Via Blockchain Applications

Ramadan T. H. Hasan[1*], Siddeeq Y. Ameen[1]

[1]IT Department, Technical College of Informatics Akre,
Duhok Polytechnic University, Duhok, Kurdistan Region, IRAQ

*Corresponding Author

DOI: https://doi.org/10.30880/jscdm.2021.02.02.003
Received 04 June 2021; Accepted 28 June 2021; Available online 15 October 2021

Abstract: Blockchain technology is now becoming highly appealing to the next generation because it is better tailored to the information age. Blockchain technologies can also be used in the Internet of Things (IoT) and fog computing. The development of IoT and Fog Computing technologies in different fields has resulted in a major improvement in distributed networks. Blockchain technology is now becoming highly appealing to the next generation because it is better tailored to the information age. Blockchain technologies can also be used in IoT and fog computing. The blockchain principle necessitates a transparent data storage mechanism for storing and exchanging data and transactions throughout the network. In this paper, first, we explained blockchain, its architecture, and its security. Then we view Blockchain application in IoT security. Then we explained Fog computing, Generic Security Requirements for Fog Computing, and we also discussed Blockchain applications that enhance Fog Computing Security. Finally, we conduct a review of some recent literature on using blockchain applications to improve IoT and fog computing security and compare the methods proposed in the literature.

Keywords: Blockchain, Fog Computing, IoT, blockchain security, decentralization, transaction

1. Introduction

The Internet of Things (IoT) consists of billions of humans, computers, linked electronic objects, and the result of experiences that generate and share both personal and sensitive information. Many modern gadgets employ both big and small sensors and those that you can put on your whole body. At the same time, with the unprecedented rise in the number of IoT's use and variety, it is vulnerable to cyber-attacks [1] "The entire of the Internet of Things" encompasses both sensor networks and machine-to-to-machine (M2M) and machine-to-type systems. Securities concerns that apply to WSN, M2M, and even more specifically, CPS have been factored into these privacy considerations in our sense. If security precautions are not taken, or if they are not appropriate, it is possible that injury will be of greater consequence [1]. Researchers sees that there is great potential for Blockchain-based identity and access protection to provide IoT protection [2].

Fog computing is a dispersed expansion of IoT-oriented cloud-based service computing solutions that increasingly spread cloud processing and storage to the edge network [1]. Each fog node is located near the edge network's IoT devices and offers varying processing, storage, and networking capacities to facilitate the execution of service applications. Fog computing, as a result, uses fog nodes to build cloud resources that are spread across edge domains. As cross-domain data exchange and distributed data use have become an urgent demand, however, fog computing infrastructure still faces the risk of trust-based and centralized control, raising questions regarding data protection and privacy [3]. Data in a single domain cannot be transferred directly between domains and must depend on trusted intermediaries to do so. On the other hand, insider attacks can cause administrators to reveal confidential data, such as healthcare, finance, and so on. A more robust and stable large-scale IoT network is expected to share and process data

Corresponding author: Ramadan.honor@gmail.com autonomously in a trustless environment, and a better system for data protection and privacy will be needed. It is time to think about decentralization for future IoT services computing. It's important to remember that achieving decentralization necessitates distributed consensus to ensure data consistency [2].

Blockchain is an open, interactive public ledger framework that creates a chain of immutable timestamp blocks. Blockchain is no longer a jargon word, and the protocol has been modified for use in a variety of applications. After a mining procedure that is checked by the participating nodes, each block is applied to the ledger. In this collaborative record-keeping and authentication method, blockchain reduces the need for a trustworthy third party [4].

In this paper, we emphasize the important role of blockchain in enhancing the security of the Internet of Things and Fog Computing. First, we explained blockchain, its architecture, and its security. Then we view Blockchain application in IoT security. Then we explained Fog computing, Generic Security Requirements for Fog Computing, and we also discussed Blockchain applications that enhance Fog Computing Security. Finally, we conduct a review of some recent literature on using Blockchain applications to improve IoT and fog computing security and compare the methods proposed in the literature.

Our paper is structured as follows: Section 2 explains the blockchain. Section 3 is a review of Blockchain applications in IoT security. Section 4 reviews Blockchain application enhance Fog Computing security. Section 5 is Assessment of Literature Reviews. Section 6 concludes our paper.

2. Blockchain

Blockchain is a decentralized method to handle authentication and tamper-resistant transactions with integrity through a wide number of users, often known as nodes [5],[6]. According to recent research by [7], blockchain is a kind of distributed ledger technology that gives users trust that information stored, such as certificates, has not been tampered with. Various researches have shown that blockchain can minimize transactional obscurity, unstable states, and cynicism by offering full transaction transparency and the supplementation of homogeneous and validated information for all network participants [8]. Furthermore, Blockchain technology is expected to radically transform markets and societal order by lowering transaction costs and reducing the need for well-known and trustworthy third parties [9],[6]. Furthermore, according to [9], this technology may be used to document transactional information, store medical documents, conclude contractual deals, monitor the flow of items, store person records of credit, track the identification of artworks, and validate payments using the supply chain, among many other procedures and processes. Fig. 1 shows how blockchain works [9].

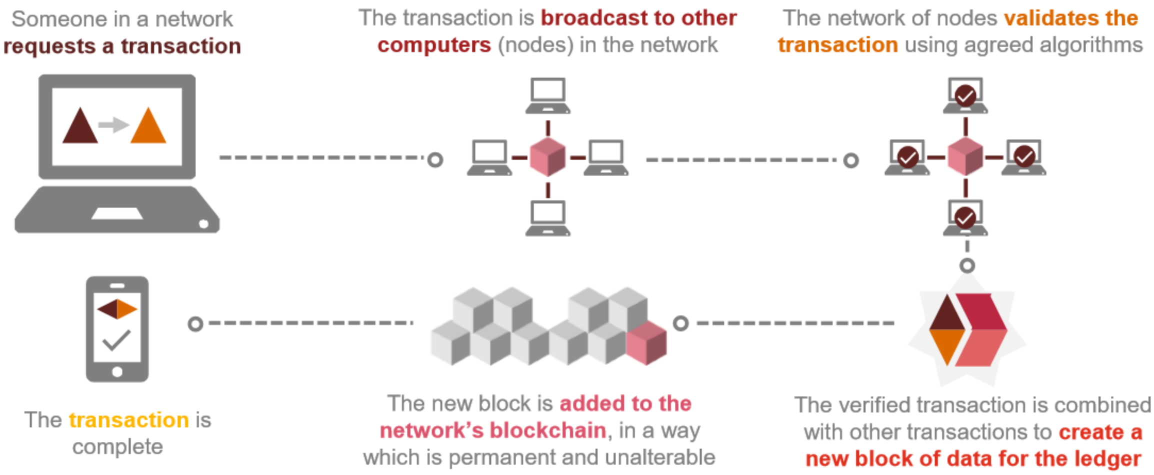

Someone in a network requests a transaction
The transaction is broadcast to other computers (nodes) in the network
The network of nodes validates the transaction using agreed algorithms
The transaction is complete
The new block is added to the network's blockchain, in a way which is permanent and unalterable
The verified transaction is combined with other transactions to create a new block of data for the ledger

Fig. 1- Blockchain works [10].

It is crucial to learn how these two systems work together in order to see how blockchain can be used to improve IoT stability. The basic technical concepts of blockchain have been briefly defined. A Blockchain is made up of two distinct but interconnected components[11].

i. Transaction: A transaction is an operation triggered by the user of a public ledger scheme such as the blockchain.

ii. Block in a Blockchain scheme: A block is a list or pool of data that documents the transaction as well as other pertinent information such as the proper order, development timestamp, and so on.

A Blockchain may be classified as either private or public, depending on the nature of the use. In a shared Blockchain, all users usually have read and write control. The monitoring of the generation and financial movement of the Bitcoin cryptocurrency is an indication of a public Blockchain operation. However, depending on the user's position in the protocol, access to certain public blockchain is restricted to either write or read privileges[11]. The aim of a private Blockchain, on the other side, is to keep user information private. Access is confined to a few trustworthy participants or representatives of a particular entity to maintain this. A "consortium Blockchain"[12] is a Blockchain that is operated by a community of individuals. This is particularly true in the case of government entities and their related sister companies or subsidiaries[11].

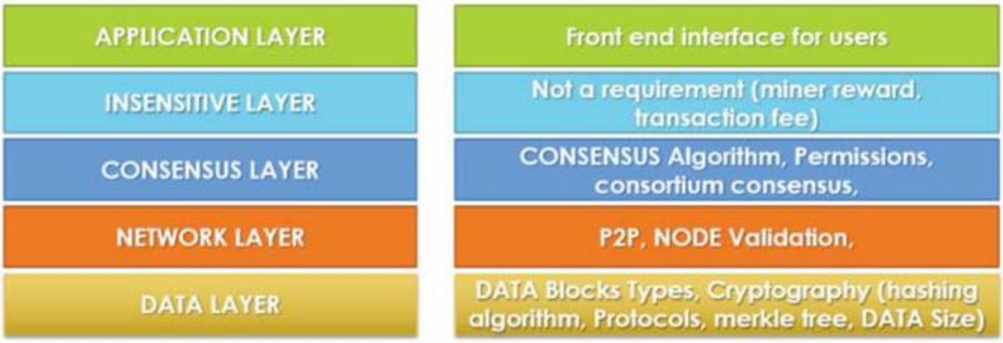
Since the public mostly uses the Blockchain system, the BC is at the forefront of other innovations, especially in terms of protection and accountability. The data stays unaltered since each active node has its own copy of the whole blockchain, i.e., whole blocks of modified documents and transactions. Any unauthorized or unintended modifications would be visible to the public. The data recorded in such publicly accessible blocks are hashed and encrypted (using the private key) to maintain confidentiality and privacy. Since the private key is utilized to encrypt the info, the general public cannot access or understand it [11]. When it comes to Blockchain technology, the two most important characteristics to consider are trust and decentralization[9],[6]. The following sections will discuss trust and decentralization in Blockchain technology, taking into account both of these important characteristics.

i. *Trust*: The decentralized methodology of Blockchain technology conceals the most important feature of Blockchain technology[9]. A proof-of-work protocol protects the network, eliminating the need for a third party to verify and record transactions. This protocol assists Blockchain users in avoiding reliance on third parties for a transaction and asset security[5]. All participants have access to the entire technology code that eliminates the possibility of a backdoor being built into the system. As opposed to the environment of banks, which manage their customers' money and assets, this secure open access allows users to utilize blockchain in a way similar to that of their own banking systems, with control over choices for guaranteeing the safety of their capital [8]. Only a few terminologies (in my opinion) fully mirror the idea of Blockchain technology that consists of shared and public interfaces, shared and public authentication, transactional peer protection, minimal knowledge distribution, cryptographic security, and confidentiality.

ii. *Decentralization*: It is a central characteristic of Blockchain technology. Resistance to censorship and immutability are two of the most critical facets of decentralization[9]. According to research undertaken by [8], one of its unique characteristics is the lack of reliance on a third party to protect and protect an individual's properties or resources. Furthermore, owing to the circularized and transparent features of Blockchain technology, the government or cyber terrorists will be unable to push through the customizable ledger designed for personal usage. The built-in proof-of-work function helps computation in resolving some kind of difficult mathematical task. Furthermore, proof-of-work is a well-known consensus mechanism that is actually being used to reconcile millions of decentralized nodes. As a consequence, there is no chance of discretionary dilution of the money supply, which enhances the certainty of asset protection[6]. A few main terminologies illustrate the essential qualities of decentralization incorporated into Blockchain technology, such as participant pseudonymity [9], the future usefulness of automation, data redundancies, and peer development versatility [13].

2.1 Blockchain Architecture

While there is no systematic or typical Blockchain design, the most straightforward representation is shown in Fig. 2 [14], which has five layers. Data layer for data sort, duration, cryptographic hashing or public key algorithm, and introducing new transaction protocols. The second layer is the network layer for P2P resource sharing networks and the node validation layer, which verifies every node before linking it to the Blockchain network. There is a consensus algorithm on the third layer that verifies every transaction before committing to the blockchain. The fourth layer is optional and is used in the public blockchain, whereas the hyper ledger fabric is used in the private blockchain. Finally, the device layer is where the code is interacted with by the end consumer. For better access control, they may add further layers for added stability, such as a smart touch application after the consensus layer [14].



APPLICATION LAYER	Front end interface for users
INSENSITIVE LAYER	Not a requirement (miner reward, transaction fee)
CONSENSUS LAYER	CONSENSUS Algorithm, Permissions, consortium consensus,
NETWORK LAYER	P2P, NODE Validation,
DATA LAYER	DATA Blocks Types, Cryptography (hashing algorithm, Protocols, merkle tree, DATA Size)

Fig. 2 - Architecture of blockchain security[14]

2.2 Blockchain Security

The following will discuss blockchain integrity, confidentiality, and availability.

i. *The integrity of the blockchain*: The Blockchain is renowned for its data confidentiality and immutability. However, there is a question regarding the data validation protocol, also regarded as 51 percent assaults. It notes that if 51% of linked nodes consent to data validation, the rest do not need to agree. A majority of malicious nodes will tamper with the data utilizing this protocol. This can be strengthened by strengthening the protocols that govern Blockchain validation in compliance with the business method [14].

ii. *Confidentiality of Blockchain*: Any operation on the Decentralized Blockchain is available to the public, so secrecy is a big concern. In Bitcoin, for example, anybody can view all transaction information, including the date and amount; the only thing that remains private is the user's name, which can be deduced from other transaction details. The author proposes two solutions: spinning public keys by using an unseeing permissioned Blockchain. To mislead the sniffer, all users of attaching devises transactions are mixed together, culminating in a loop of transactions that ends in one actual transaction that the sniffer cannot trace. Since it is a permissioned Blockchain and is not available to the internet, privacy is guaranteed [14].

iii. *Availability of Blockchain*: The availability of blockchain is very high. Only a few cases have been reported since the introduction of Bitcoin in 2009. Both nodes would have links to the distributed and up-to-date Blockchain implementations of the ledger. The blockchain operated each node separately. Each node maintains the blockchain independently. If one of the nodes leaves the network, the others will continue to function normally. This is particularly valid in the case of private blockchain. In a decentralized Blockchain, the Blockchain operators are uncertain, and the network's target is undefined, but they may remove and weaken any nodes that impact the network's availability utilizing the validation power [14].

3. Blockchain Application in IoT Security

IoT is a network of connected networks without human intervention, Smart objects, autonomous computers, IoT devices, smartphones, etc. Radio-frequency identification (RFID), Quick Response (QR) codes, sensors, or the use of wireless communication systems may allow for inter-device coordination. Anything from an embedded sensor in a fuel pump to sensors in office buildings that can monitor your position and show your files on the nearest screen is part of the IoT [11].

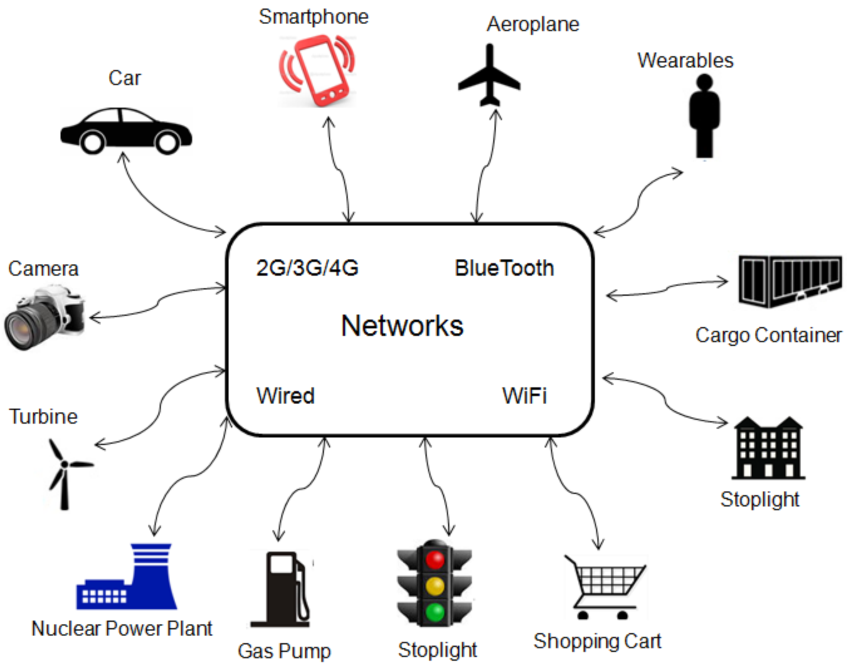


Fig. 3 - Internet of Things[11]

In an IoT world (see Fig. 3), much of the contact is done between Machines (M2M) with no human involvement whatsoever. Establishing confidence between participating machines is an almost unsolvable problem for IoT systems at this time. However, Blockchain implementation may boost stability, scalability, reliability, and privacy. Blockchain is a technology to be deployed to register billions of IoT devices and used to automate and direct transaction processing. That bills itself as "the world's first search engine for internet-connected devices" is, in reality, a search engine named "Shodan”. Using this search engine exposes unsecured Internet of Things, which means it's important to rectify the issue. Absolutely removing the single point of failure in an IoT ecosystem is one of the top strengths of the Blockchain (SPF) [11]. Often, blockchain makes use of both encryption and hashing techniques to store info. This way, blockchain will have stronger protection capabilities in an IoT environment. To carry out these strategies and use cryptographic algorithms, devices mustn't already have sufficient computing capacity. While more investigation will help solve this current shortcoming, further study is needed until in situ power is recommended [11]. The following characteristics make blockchain a powerful weapon in IoT security.

i. *Decentralization*: Data is maintained on different nodes all around the planet in a Blockchain database, eliminating the single point of failure. Until any data is added to the network, it must be approved and verified by all nodes. As a result, no changes are permitted without unanimous consent by all network members. This method is known as peer-to-peer networking, and it is designed to keep malicious actors out of Blockchain transactions. There is no possibility of a man in the center assault, in which hackers intercept data transmitted between a server and a computer since there is no single server [10].

ii. *Public access*: Blockchain is open, which ensures that everyone in the network may use it. The common background of recorded blocks and transactions is visible to all network users, but viewing the content requires a private key. This provides full access to all processes while still keeping data safe. Once data is recorded on a Blockchain, it is difficult to modify it [10].

iii. *Secure data*: Blockchain secures data with sophisticated encryption algorithms, making it more private. This is achieved mainly to ensure that financial transactions are risk-free. Connected Objects can interact with each other using the Internet of Things (IoT) by transmitting and receiving messages the same way transactions do, producing and tracking protected data [10].

The following are some of the most popular usage cases for Blockchain-based implementations in the Internet of Things.

i. *Supply chain*: The main challenge in supply chain IoT is ensuring accountability. The Blockchain-based approach will provide data-sharing users with visibility, optimization, petitioning, and proper access control. The performance of supply chain management can be improved by the integrity, affordability, and durability of real-time data access [15].

ii. *Vehicular IoT*: The automobile industry is one of the most advantageous implementations of Blockchain-based IoT technologies since it allows for real-time data access and transaction execution between large car firms, suppliers, partners, service providers, insurance, lending agencies, regulators, and consumers. Blockchain incorporation enables on-the-go actions, utilities, and payments. To aid in the production of a single automobile, Toyota, for example, has launched an initiative to monitor vehicle parts as they travel around the world through factories and suppliers [15].

iii. *Smart Grid and Energy Management:* The use of Blockchain and IoT in the energy sector has resulted in a significant improvement in the reliability of smart grids and energy distribution and the tracking and management of resource distribution. For example, surplus electricity from a roof-top solar panel may be distributed to those consumers who use it, with record and payment, without compromising protection or privacy. Likewise, Blockchain-based mesh networks with IoT devices may be used to track electricity grids for fault tolerance and to resolve any issues that arise [15] quickly.

iv. *Healthcare*: One of the uses of the Blockchain-based Internet of Things is the data storage and tracking of patient records at home or remotely. The data of patients' is safeguarded by having it stored in a distributed ledger, with defined rules of access. Blockchain technology is utilized in all manner of diverse areas of the pharmaceutical supply chain, from factories to sales [15].

v. *Other applications*: Besides these listed uses, the efficient introduction of Blockchain-based IoT will also prove enhanced control and protection of IoT nodes and assured privacy as data moves from the network. Often, it enables participants to gain and maintain ownership over information and resources. Because the blockchain was created to support cryptocurrencies, it can be used for encrypted transactions, thus keeping the information anonymous [15].

4. Blockchain Application Enhance Fog Computing Security

Fog Computing is gaining popularity as a complementary computing model to Cloud Computing for resource-constrained computing nodes' computing, storage, and network needs. Smartphones, laptops, the IoT, and wireless sensors and actuators are only a few instances of electronic systems with minimal capital [13],[16]. These devices have minimal computational capacity, memory, and network connectivity across wireless media. Given their restricted capacities, such machines are changing computing from an industry phenomenon to a widespread phenomenon. This segment addresses the shortcomings of Cloud Computing in meeting the needs of resource-constrained applications and the Fog's specific characteristics in comparison to the cloud [6],[13].

4.1 Generic Security Requirements for Fog Computing

The generic security requirements for fog computing include:

i. *Authentication*: In a distributed or networked system, it is the prime operation. The entire point of authentication is to make sure and confirm who an individual is. An end consumer can be a computer, or a service, or both. It is a basic process since it only lets approved users into the network. Many of the methods used for identifying users in the cloud are: keys, PINs, DNA, or both. When thinking about issues related to Fog Computing, for instance, low resource density, low Fog node mobility, and high network accessibility should be accounted for [13].

ii. *Secured communication*: Assumption of privacy gives rise to certain possible attacks like leakage, spoofing, eavesdropping and. Hence, all Cloud and Fog implementations have to provide a protected channel over an unsecured medium. Two distinct modes of interactions are noticed in Fog networks: Next, an edge system binds to a fog node. The details of this correspondence may be kept hidden using symmetric encryption. Fog networks can face certain resource limitations when using a shared key infrastructure. The connectivity between fog nodes is subject to a second problem: offering end-to-end protection and accessibility while allowing for several hops is difficult [13].

iii. *Availability*: One of the most important criteria shared by both domains is that the Fog services provided be accessible 24 hours a day, seven days a week. To deprive legitimate users of requested facilities, malicious users use tactics such as overwhelming the network with unauthorized packets or rerouting network traffic to incorrect destinations. In the Health and IIS realms, easily identifying and defending against certain risks will save lives [13].

iv. *Privacy*: To offer customized services, the majority of Fog applications monitor personal details. Following are a few points. For instance, technologies like ITS and urban monitoring map citizens' personal movement trends. Second, in the case of smart grids, grid managers map and control electricity consumption trends. Finally, intelligent healthcare networks maintain records of patients' personal and medical details. When service providers utilize such confidential personal details for monetary benefit or strategic advantage without the permission of service consumers, their privacy is jeopardized. It's challenging to construct a fog layer that prevents sensitive details from unintended use [13].

v. *Trust management*: In network-centric structures, trust is a two-way path. By delivering prompt and secure answers, service providers will win the loyalty of their customers. Additionally, service consumers must show that they are legal and non-malicious users of service providers. A sequence of connections between service providers and consumers builds bidirectional confidence. In the case of cloud-based service companies, some of the approaches employed include quantifying service provider reputations, customer opinions, and service level agreements. The transient design of fog nodes, in which a fog node exits and rejoins the network on a regular basis, and the mobility of edge devices are two considerations to remember when designing a confidence management scheme at the fog layer [13].

Having specified generic requirements, blockchain-based methods can be used to include solutions for general protection criteria in fog computing, as addressed in the following sub-sections.

4.2 Authentication based on Blockchain

There are two types of authentications in a networked device, such as a cloud or fog world. There are two forms of authentication: centralized and decentralized. OAuth 2.0, for example, is a centralized authentication protocol [16]. In these kinds of protocols, a centralized authentication server verifies the credentials submitted by a receiver and, after successfully validating the client, authorizes access to the requested resources from a third party. The vast majority of cloud service providers use this form of authentication. The security mechanisms of Google, Facebook, and Twitter act as authentication repositories, with the user id and password on these pages acting as the client's credentials. The privacy of clients is often violated by such centralized validation repositories, which have a single point of failure. Decentralized security protocols address the limitations of a centralized scheme. Web of Trust (WoT) and Very Good Privacy (PGP) are two instances of decentralized protocols. Blockchain technology is a Blockchain that allows for the development of decentralized apps. As a consequence, it is simpler to incorporate decentralized authentication services. Fog networks use blockchain systems in a number of applications [13].

In the first implementation method, fog nodes use a smart contract running on the fog nodes to authenticate a client or edge computer. The smart contract stores a mapping of edge devices and active customers, as well as their passwords [16]. After receiving an authorization order, the smart contract running on any of the Fog nodes would validate the requested credentials. The system utilizes distributed ledgers to store certificate data and accepted device mapping in the second tier of Blockchain-based authentication protocols. In credential records, asymmetric key cryptography or digital signatures are often used. Any fog node running a Blockchain event, known as miners, can authenticate a request to access the requested service. In the third Blockchain-based version, edge nodes form a cluster known as bubbles of trust. Edge devices can send and receive messages within the trust bubbles. A master node manages each confidence bubble. A submission to send or receive is a transaction to be recorded in the blockchain. The master node, like a verification authority, validates a send/receive order. The Blockchain-based authentication schemes have been tested on a variety of protection issues and have been shown to be immune to denial-of-service attacks. Furthermore, unlike clustered protocols, these protocols are modular [13].

4.3 Secured Communication based on Blockchain

Fog/Cloud networks that utilize Blockchain technologies for verification often use the same technology for encrypted communication [16]. Blockchain technology uses cryptographic algorithms to connect nodes and store data in distributed ledgers. Protection is needed for two types of communication: (i) communication from an edge device to a fog node and (ii) communication from one fog node to another fog node. Blockchain is usually implemented as a fog service that operates on fog nodes. A public address is used to safeguard communication among edge devices and fog nodes. In the case of Ethereum, an edge node is identified by a 20-byte address. This address can be used to create an SSL session between an edge computer and a fog node. For all connections between fog nodes, asymmetric-key cryptography is used by default. Man-in-the-middle and replay attacks have been shown to be vulnerable to Blockchain networks that utilize secure contact. As a consequence, data security, data confidentiality, and communication justice are all ensured [13].

4.4 Availability based on Blockchain

A Blockchain-based system's database and computing components are public ledgers and smart contracts. The Blockchain network contains several copies of these components. Consensus protocols keep the global state of storage and computations constant. Blockchain-based fog services are immune to single-point loss due to these intrinsic architecture properties. As a consequence, they are fault-tolerant, resulting in less downtime. Another way to stop fog systems from working is to use denial of service assaults. To protect itself against such an assault, a Blockchain-based framework may use hierarchical structures. One such process can be found in. At the system stage, Blockchain miners secure edge devices from malicious users running malware on them. Since all miners must first accept and check access to edge computers. At the network stage, blockchain is responsible for validating each contact coming from edge devices and from fog nodes. A Blockchain-based framework may also dynamically build confidence bubbles to restrict send/receive actions with a community of trustworthy edge nodes or isolate a malicious device [16],[13].

4.5 Privacy based on Blockchain

Developers of cloud/fog systems that use the client-server paradigm for interaction have a small range of primitives (e.g., storing sensitive details in an encrypted format) to preserve the privacy of the personal information exchanged by their customers. Unlike this, blockchain, which is a peer-to-peer framework, offers a variety of mechanisms to secure sensitive data privacy [13].

4.6 Trust Management based on Blockchain

Calculating confidence is a daunting job. The Blockchain platform has a number of tools for dealing with it. Any Blockchain-based approaches to computing faith in decentralized networks are accessible. The subjectivity of the problem creates the first computational problems. Trust is a very subjective concept. Confidence is calculated either for an agent or for the delivered results, or both to deal with subjectivity. E.g., in a vehicular ad-hoc network, the trustworthiness of a car or a received letter, such as a warning regarding a road accident, must be established, as must the trustworthiness of both the message and the sender [13]. The Blockchain-based anonymous reputation scheme, which computes the trustworthiness of a sender and the received message, is defined in Reference [17]. A message's trustworthiness and its author are calculated using historical experiences and indirect views from other participating nodes. The second computational difficulty results from the assumption that confidence fluctuates over time. Reference [18] proposes a Blockchain-based approach to solve this issue. In the case of wireless sensor networks, the method measures a node's trustworthiness. A node's credibility is determined by how it reacts to an incident. Any case has a prestige element attached to it. The credibility element is a steadily diminishing mechanism to keep it meaningful over time. Blockchain immutability allows allocating a credibility attribute to nodes dependent on their past connections. The third computational task is to build a confidence model that is versatile in the sense that it can be generalized to a number of domains. Reference [16] discussed this problem, which proposes a Blockchain-based approach for measuring confidence by defining various attributes. These qualities are reputation, meaning, setting, priorities, desires, social interactions, desire, and assessment timelines. The method also shows the model's applicability in the Social Internet of Vehicles domain. It goes on to say that emerging technologies like blockchain and fog computing are suitable for providing scalable solutions for managing trust in a dynamic environment like the Internet of Things [13].

5. Assessment of Literature Reviews

Blockchain technologies are the most widely known techniques among a large number of researchers. So, it contains various features which support numerous requirements in diverse fields of life. Blockchain technology is considered an extremely elastic system that can be used in various fields. Most of them are that it is a critical technology that can compensate for security flaws in environments where they exist. Because of its decentralized architecture and peer-to-peer characteristics, Blockchain technology is well-known and highly regarded. We review some recent literature concerning Blockchain application in IoT and fog computing security enhancement.

Dabbaghjamanesh et al. [19], by using a Blockchain-enabled Internet of Things (IoT) approach, they propose a novel system for improving the safety and security of power trading in networked microgrids. Using Blockchain-enabled IoT technology in network MGs power trading would potentially result in a number of significant benefits, such as reduced infrastructure risks, financial fraud protection, and lower operational costs.

Du et al. [3] introduced a high-performance and stable Blockchain architecture with the architecture of a three-dimensional ledger to allow the Internet of Things to be accessible (or allow them to accept the use of blockchain). To deal with the variety and scalability of IoT networks, he initially devised a three-dimensional architecture with innovative data structures. They then propose the Three-Dimensional Greedy Heaviest-Observed Sub-Tree (3D-GHOST) agreement approach for Spacechain to boost the security and performance of a network. In addition, they do a more thorough security analysis and robust verification to see the outcome of Spacechain.

Cui et al. [20] proposed architecture for the IoT data processing and a supply chain focused on blockchain and smart contracts to deal with the two major challenges: data management and useful cross-tracing for related objects. Experimental studies demonstrate that the device works well with internal data losses under reasonable limits.

Rashid and Pajooh [21] did a good job putting the systems for the personal security of the Internet of Things and authorization on a Blockchain. The model integrates Hyper-ledger Fabric, which is an open-source framework of blockchain, on top of it. The local authentication and authorization system allows IoT devices to coordinate with greater security and intelligence at the lower levels as the global model explores improved integration.

Al-Madani and Gaikwad [22] proposed a service-centric networking paradigm for secure IoT info built on Blockchain (SCN). SCN uses service names rather than IPv4 addresses, which helps users talk to each other quickly and data flows reliably and securely.

Asare et al. [23] introduced a Blockchain-based nodal authentication method for protecting the privacy of data passing across IoT nodes. In their work, they used the GOST algorithm as part of our strategy. Finally, they were able to accomplish nodal authentication and data verification. This means an attacker can't impersonate a node in the communication chain of the connected nodes. Data secrecy became achieved in the nodes during contact.

Gupta et al. [24] focus on how Blockchain technologies can be used to guarantee the confidentiality of data sent and retrieved from nodes in an IoT network. They suggest a resource-constrained Blockchain consensus model. On top of the Blockchain platform, they also suggest a model for IoT stability.

Xie et al. [25] suggested a decentralized encryption system of Blockchain-based vehicular IoT in 5G-VANETs with SDN. Both active nodes in the vehicular scheme, inclusive RSUs, OBUs, and gNBs, are part of a P2P network that maintains the blockchain. The cars give each other real-time road condition texts, and the blockchain tracks all of the messages as well as the message origins. The source message's accountability is confirmed by using the Blockchain immutable function. In this application, they also provide a real-time video report service.

Li et al. [26] suggested FICA, a carpooling scheme that promotes conditional anonymity, utilizing assisted Blockchain for Vehicle Fog Computing, one-to-many matching, destination matching, and data auditability are all possible. The proposed scheme is secure against a threat paradigm under which the cloud service and RSUs are semi-honest, and users can submit false positions.

Debe et al. [27] introduced the framework configuration, implementation specifics and demonstrated the overall suggested solution's right functionality. In addition, we analyze the smart contract code's efficiency, expense, and protection to demonstrate its efficacy and robustness in the face of major security concerns.

Zhu and Badr [28] present a hybrid Internet of Things architecture that is used to ensure security in a trustless IoT setting, using fog computing. By combining our fog computing infrastructure with Blockchain-based social networks, users would be able to securely manage smart artifacts by providing tamper-proof digital identities in a trustless environment and introducing a new class of authentication and authorization protocols for the IoT.

Mountain et al. [17] for Fog computing with fault-tolerant and the Internet of Things are areas where they have proposed a modern management system using blockchain as a part of theme architecture. Blockchain offers security and control for Internet of Things nodes. To achieve establish trust and keep our transactions safe, each person in the network must be authenticated in the blockchain. They also plan to incorporate an attribute into the blockchain so that only permitted individuals may interact with the IoT devices. In addition, they suggest creating a protected link between IoT devices and the users. They also propose to provide an attribute in the blockchain so that only approved individuals are able to communicate with the IoT, which is enforced by the contract. They look to correct both the accountability and attribute encryption at the same time.

Simpson et al. [29] suggest a system for ensuring that patients' healthcare information is accessible through many healthcare institutions. The Blockchain ledger enables the usage of timestamps in records to validate and archive existing patient health details in a consolidated data cloud.

Lei et al. [30] suggest Group chain, a new scalable distributed Blockchain of a two-chain layout ideal for Internet of Things and fog computing services computing. After that, they designed a Group chain prototype and performed tests on it. The findings of the experiments reveal that the Group chain optimizes confirmation latency and transaction throughput, all of that is discussed in Bitcoin.

Mudhar et al. [31] suggest a Blockchain-based mechanism to safe access for user authentication to fog-enabled Internet of Thing devices. The Ethereum Smart Contract is included in the planned system. They used Remix-IDE to create a smart contract and checked its functionality on two test networks: Rinkeby Test and Test RPC (Ganache) Network. On the ChainSecurity analyzing tool, they have looked at the security flaws in our smart contract.

Chen et al. [32] propose the architecture for the creation of a management framework of stable distributed data for fog computing in large-scale Internet of Things applications, coupled with a Blockchain-based data management platform implementation that addresses main issues, how to incorporate information protection and fog-computing storage management into the vast Internet of Things application and improve rational interoperability of connected stuff.

5.1 Blockchain application in IoT

Table 1 shows a comparison of IoT blockchain application studies.

Table 1 - Comparison table of IoT blockchain application studies

No.	Ref	Year	Proposed schema	Result	Advantage
1	[19]	2019	suggests an Internet of Things solution to providing an efficient privacy and management system for microgrids (MGs)	as suggested, the approach may yield greater protection, anonymity, and less susceptibility to fraud within the network	Reducing the risk of the scheme, controlling fraudulent activities, reduce operating expenses
2	[3]	2020	create a stable and high-performance three-dimensional Blockchain for IoT	Prove that Spacechain is more secure and more preferment than both NKC and GHOST.	Specifically, in terms of defense, the chain has proved capable of resisting both single and DoS (denial of service) attacks
3	[20]	2019	Uses IoT as a tool for managing real-world data on a Blockchain	Placements for jobs that scale well in the face of computer and communication errors but work well to protect against unauthorized access	it achieves fine-grained and safe data storage for IoT devices while validating data provenance and authenticity by the introduction of the Blockchain framework
4	[21]	2019	IoT networks may use blockchain as a multi-layered authentication system	The suggested model would deal with real application-specific issues by implementing the blockchain through a multi-layered IoT network	Hyperledgerio is an open access Blockchain proposal to prove the framework.
5	[22]	2020	Provides a framework for IoT data security built on service-centric network structure (SCN).	A centralized network is less vulnerable to a third party being able to sabotage because it does not require a service provider compared to the classical model's strengths. There is the concern that the data on IoT could be violated	decentralized user records, p2p system, which stores user information on the user’s device
6	[23]		Proposed a Blockchain-based solution to IoT security by using nodal authentication	successfully finished the task of securing the link at the nodal point of origin, obtained the data was deemed authenticated and validated as correct at the nodal points	An attacker cannot make a false link in the entire chain of the network. The data was preserved in the individual nodes during the correspondence
7	[24]	2019	Create a new protection paradigm for IoT developed by using a Blockchain distributed ledger	To secure the network from DDoS and local attackers, devices, an authentication and session tracking service that records and correlates all sessions and node security in the IoT should be applied.	

8	[25]	2019	A Blockchain-based security architecture assists Vehicle-based security	The simulation results suggest that it is possible to classify malicious vehicles with appropriate overhead for large networks accurately.	The specification guarantees a safe and reliable vehicle-Internet of Things (VitIoIoIoT) environment with consumer privacy guaranteed.

Work in [19] focuses on the energy management of networked MGs; confronted with concerns in terms of privacy and security. According to [3] Blockchain deployment on IoT is an efficient solution to resolve conventional security problems. But there are two main disadvantages of the present approaches. Since the blockchain itself is prone to assaults, including selfish mining, twin expenditure, and distributed denial of service assaults, smart IoT devices are likewise susceptible after blockchain systems have successfully invaded hackers. The work of [20] views the unique properties of the resources restriction, short-term communication, and IoT self-structure requirements for huge information processing and storage. This resulted in a series of innovative challenges to safety and privacy. Research in [21] explored the probable use of IoT security issues blockchain technology under 5G cellular systems because of centralized IoT security and performance, which is challenging when it comes to the coordination of external computing resources. In the future generation of wireless media, there is a gap in the deployment of scalable, secure, and secure systems. According to [22], the main issue of IoT security is Distributed Denial of Service (DDOS), which prevents users from accessing the server since the attacker has run a vast number of server requests. According to [23], as an ongoing exponential expansion in IoT engagement occurs, there is an increase in the number of nodes for data transmission, leading to a rise in cyber-attacks inside IoT, which constitutes a serious danger to these linked nodes. Work in [24] concentrated on the security, integrity, and accessibility of data that is transferred and received through IoT network nodes because IoT nodes are resource-restricted. In [25], it investigates the safety and privacy challenges in the SDN-enabled 5G-VANET transport system and vehicle IoT ecosystem, where realistic and trustworthy security systems are required to administer a trust.

5.2 Blockchain Application in Fog Computing

Table 2 shows a comparison table of blockchain application studies in fog computing.

Table 2 - Comparison table of blockchain application studies in Fog Computing

No.	Ref	Year	Proposed schema	Result	Advantage
1	[28]	2018	Introduce a fog computing infrastructure to make it safe in the trustless Internet of Things To leverage our fog computing. We use social networks that utilize Blockchain technologies	The fog computing security framework outlines security measures for the IoT based on the inclusion of unusual characteristics of the IoT	Using zero-knowledge evidence, giving privacy protection to the blockchain identification ledger
2	[26]	2018	FICA, a conditional privacy-friendly carpooling approach using vehicular fog computing, was implemented using blockchain-aided matching, one-to-many matching, and auditable transportation.	Except in a world where the cloud server and issued RSUs are all equal, this scheme is vulnerable if users can upload fake positions.	Used a range query approach to accomplish get-off location matching. He also implemented a private blockchain further into the carpooling system, maintaining a verifiable ledger of carpooling records and ensuring data integrity.
3	[29]	2019	Proposes an adoption framework prove data integrity in decentralized healthcare environments using a tiger hunt paradigm to use a hash function.	A method for ensuring healthcare data is readily accessible at all medical facilities	Offers a safe and standard method of transferring medical information between different healthcare facilities

4	[17]	2020	Invent a modern access management system for the Internet of Things (and add error tolerance to it).	This suggested authentication strategy achieves security objectives while also protecting against eavesdropping and DDoS attacks and maintaining resiliency against various types of DoS.	Its creative approach resolves the issues of storing information, executing transactions, and carrying out functions in an open network, while still securing the network
5	[27]	2020	Suggest an incentivized program that uses blockchain and contracts to undo every transaction	Ethereum has the total expense of operating smart contracts by one-third.	It keeps everyone in the game: The proposal would guarantee that all nodes are equally and legitimately bidding against each other.
6	[30]	2020	Propose Group chain, a new modular shared Blockchain with a two-chain framework for IoT applications fog computing.	Show the Group chain optimizes transaction throughput and confirmation latency, as claimed in Bitcoin.	Group chain retains Bitcoin's encryption properties while also strengthening protection against threats like double spending and greedy mining.
7	[31]	2020	An effective method for user authentication for IoT devices equipped with fog is proposed.	The suggested system allows the use of Ethereum's Smart Contracts.	The scheme is resistant to replay and eavesdropping threats.
8	[32]	2020	Is concerned with the creation of a stable distributed data processing framework for fog computing in large-scale IoT applications.	Display that the device works well in fog computing to empower data provenance and openness and effectively protect against unauthorized access, scales well with the loss of contact and computing efficiency while staying within a reasonable range	Fog computing in large-scale IoT applications needs a stable distributed data processing infrastructure.

Work in [28] mentioned that although cloud computing is seen as the panacea for processing and analyzing IoT data, there are disadvantages in many other respects, such as latency, bandwidth, and mobility, when data from connected devices are sent to the cloud. The fog computer paradigm extends the cloud and refers to a geographically dispersed IoT network computing paradigm. Fog computing still has a long way to go, particularly in terms of security with unusual IoT features, such as scalability, heterogeneity, mobility, and restricted resources. According to [26], fog computing delivers low latency for local data processing, but it also raises worries about security and privacy, as the private information of users (e.g., identity, location) may be revealed when this information is exchanged. While before transmission, they may be encrypted, it makes it a challenge for users to match and bad users to publish phony sites. In addition, carpooling records should be provided to ensure trustworthy data auditing. Reference [29] when there is a connection, data from dew systems should be synced with cloud data. The cloud server should validate the dew system data to guarantee that the data is complete.

According to [17] Fog computing is designed to improve service quality, data access, networking, processing, and storage. However, even when various cloud solutions are suggested, security and privacy challenges exist. In fact, because of its unique characteristics such as mobility, geo-distribution, heterogeneity, and others, fog computing introduces new challenges to security and privacy. According to [27], a distant cloud server query leads to needless overhead communication and longer response latency. The recent introduction of fog computing to deliver low-latency local data processing creates additional security and privacy issues since sensitive user information (such as identity, location) might potentially be divulged when exchanged during a carpool. While before transmission, they are encrypt able, it enables users to match a difficult challenge and bad users to submit bogus locations. According to [30], the combination of blockchain with Fog Computing offers a natural solution for decentralization, and fog computing may thus be used to overcome certain shortcomings, such as security and privacy. But scalability is one of the fundamental issues of the integration of blockchain with fog computing. According to [31], IoT devices from WSN to RFIDs can detect, actuate and share data but have limited memory, storage, and computing capacity as resource-restricted devices. IoT devices are thus unable to protect themselves against different risks to security and privacy. Current cloud-IoT designs are centralized; therefore, people are not regulated and managed by trusted third parties. According to [32], several fog nodes on a network edge suffer external attacks that lead to severe safety concerns stemming from the confidence relation vulnerability as the attributes of the fog computing system are not considered. In summary, IoT and fog computing have facilitates data acquisition and processing [33], [34] and blockchain intends to solve the challenges of communication security of this domain [35].

6. Conclusions

Blockchain technology is considered an extremely elastic system that can be used in various fields. Most of them are that it is a critical technology that can compensate for security flaws in environments where they exist. Because of its decentralized architecture and peer-to-peer characteristics, Blockchain technology is well-known and highly regarded. Blockchain is a new Internet of Things infrastructure that stores transactions between IoT nodes using a shared, distributed, transparent, and real-time ledger. In fog computing, Blockchain-based applications are solutions for verification, encrypted connectivity, compatibility, anonymity, and confidence management, enhancing the security of Fog Computing. In this paper, first, we explained blockchain, its architecture, and its security. Then we view Blockchain application in IoT security. Then we explained Fog computing, Generic Security Requirements for Fog Computing, and we also discussed Blockchain applications that enhance Fog Computing Security. Finally, we conduct a review of some recent literature on using Blockchain applications to improve IoT and fog computing security and compare the methods proposed in the literature.

Acknowledgement

The author would like to acknowledge the IT Department, Technical College of Informatics Akre, Duhok Polytechnic University, Duhok, Kurdistan Region, Iraq.

References

[1] Singh, S., Hosen, A.S. and Yoon. B. (2021). Blockchain security attacks, challenges, and solutions for the future distributed IoT network. IEEE Access, p. 13938-13959

[2] Ataşen, K., and Üstünel. H. (2019). Designing a Secure IoT Network by using blockchain. in 2019 3rd International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMS). IEEE

[3] Du, M., Wang, K., Liu, Y., Qian, K., Sun, Y., Xu, W., Guo, S. (2020). Spacechain: a three-dimensional blockchain architecture for IoT security. IEEE Wireless Communications. 27(3): p. 38-45

[4] Roy, S., Ashaduzzaman, M., Hassan, M. and Chowdhury, A. R. (2018). Blockchain for IoT Security and Management: Current Prospects, Challenges and Future Directions, 5th International Conference on Networking, Systems and Security (NSysS), pp. 1-9

[5] Glaser, F. (2017). Pervasive decentralization of digital infrastructures: a framework for blockchain-enabled system and use case analysis. in Proceedings of the 50th Hawaii international conference on system sciences.

[6] Beck, R., C. Müller-Bloch, and J.L. King (2018). Governance in the blockchain economy: A framework and research agenda. Journal of the Association for Information System. 19(10): p. 1

[7] Mohanta, B.K., et al. (2020). Addressing security and privacy issues of IoT using blockchain technology. IEEE Internet of Things Journal. 8(2): p. 881-888

[8] Nærland, K., et al. (2017). Blockchain to Rule the Waves-Nascent Design Principles for Reducing Risk and Uncertainty in Decentralized Environments. in ICIS

[9] Ali, O., et al., (2021) A comparative study: blockchain technology utilization benefits, challenges and functionalities. IEEE Access, p. 12730-12749

[10] Miraz, M.H. and D.C. Donald. (2018). Application of blockchain in booking and registration systems of securities exchanges. in 2018 International Conference on Computing, Electronics & Communications Engineering (iCCECE). IEEE

[11] Miraz, M.H. and Ali, M. (2020). Integration of Blockchain and IoT: An Enhanced Security Perspective. Annals of Emerging Technologies in Computing (AETiC), p. 2516-0281

[12] Cho, S. and Lee. S. (2019). Survey on the Application of BlockChain to IoT. in 2019 International Conference on Electronics, Information, and Communication (ICEIC). IEEE

[13] Kiwelekar, A.W., et al. (2021). Blockchain-Based Security Services for Fog Computing, in Fog/Edge Computing for Security, Privacy, and Applications, Springer. p. 271-290

[14] Al-Abbasi, L. and El-Medany, W. (2019). Blockchain security architecture: A review technology platform, security strength and weakness

[15] Muzammal, S.M. and Murugesan, R.K. (2018). A Study on Leveraging Blockchain Technology for IoT Security Enhancement. Fourth International Conference on Advances in Computing, Communication & Automation (ICACCA). IEEE

[16] Zheng, X., et al. (2018). Fog Computing: Concept, Applications and Future. in 2018 International Conference on Cloud Computing, Big Data and Blockchain (ICCBB). IEEE

[17] Mounnan, O., et al. (2020). Privacy-Aware and authentication based on Blockchain with Fault Tolerance for IoT enabled Fog Computing, Fifth International Conference on Fog and Mobile Edge Computing (FMEC). IEEE

[18] Tang, W., et al. (2018). A blockchain-based offloading approach in fog computing environment. in 2018 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Ubiquitous Computing & Communications, Big Data & Cloud Computing, Social Computing & Networking, Sustainable Computing & Communications (ISPA/IUCC/BDCloud/SocialCom/SustainCom). IEEE

[19] Dabbaghjamanesh, M., et al. Networked microgrid security and privacy enhancement by the blockchain-enabled Internet of Things approach. in 2019 IEEE Green Technologies Conference (GreenTech). 2019. IEEE

[20] Cui, H., et al. (2019). IoT data management and lineage traceability: A blockchain-based solution. in 2019 IEEE/CIC International Conference on Communications Workshops in China (ICCC Workshops). IEEE

[21] Rashid, M. and Pajooh. H.H. (2019). A security framework for IoT authentication and authorization based on blockchain technology. in 2019 18th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/13th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE). 2019. IEEE

[22] Al-madani, A.M. and A.T. Gaikwad. (2020) IoT Data Security Via Blockchain Technology and Service-Centric Networking. in 2020 International Conference on Inventive Computation Technologies (ICICT). IEEE

[23] Asare, B.T., Quist–Aphetsi, K. and Nana. L. (2019). Nodal authentication of IoT data using blockchain. in 2019 international conference on computing, computational modelling and applications (ICC). IEEE

[24] Gupta, Y., et al. (2018). The applicability of blockchain in the Internet of Things. in 2018 10th International Conference on Communication Systems & Networks (COMSNETS). IEEE

[25] Xie, L., et al. (2019). Blockchain-based secure and trustworthy Internet of Things in SDN-enabled 5G-VANETs. IEEE Access, p. 56656-56666

[26] Li, M., Zhu, L. and Lin, X. (2018). Efficient and privacy-preserving carpooling using blockchain-assisted vehicular fog computing. IEEE Internet of Things Journal. 6(3): p. 4573-4584

[27] Debe, M., et al., (2020). Blockchain-Based Decentralized Reverse Bidding in Fog Computing. IEEE Access, p. 81686-81697

[28] Zhu, X. and Badr. Y. (2018). Fog computing security architecture for the internet of things using blockchain-based social networks. 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

[29] Simpson, G. and Quist-Aphetsi. K. (2019). A Centralized Data Validation Approach for Distributed Healthcare Systems in Dew-Fog Computing Environment Using Blockchain. in 2019 International Conference on Cyber Security and Internet of Things (ICSIoT). IEEE

[30] Lei, K., et al., (2020). Group chain: Towards a scalable public blockchain in fog computing of IoT services computing. IEEE Transactions on Services Computing, 13(2): p. 252-262

[31] Mudhar, J.K., Kalra, S. and Malhotra. J. (2020). An Efficient Blockchain-Based Authentication Scheme to Secure Fog Enabled IoT Devices. in 2020 Indo–Taiwan 2nd International Conference on Computing, Analytics and Networks (Indo-Taiwan ICAN). IEEE

[32] Chen, Z., et al. (2020). Secure Distributed Data Management for Fog Computing in Large-Scale IoT Application: A Blockchain-Based Solution. in 2020 IEEE International Conference on Communications Workshops (ICC Workshops). IEEE

[33] Abdulkareem, K. H., Mohammed, M. A., Gunasekaran, S. S., Al-Mhiqani, M. N., Mutlag, A. A., Mostafa, S. A., ... & Ibrahim, D. A. (2019). A review of fog computing and machine learning: concepts, applications, challenges, and open issues. IEEE Access, 7, 153123-153140

[34] Mutlag, A. A., Khanapi Abd Ghani, M., Mohammed, M. A., Maashi, M. S., Mohd, O., Mostafa, S. A., ... & de la Torre Díez, I. (2020). MAFC: Multi-agent fog computing model for healthcare critical tasks management. Sensors, 20(7), 1853

[35] Monrat, A. A., Schelén, O., & Andersson, K. (2019). A survey of blockchain from the perspectives of applications, challenges, and opportunities. *IEEE Access*, *7*, 117134-117151