Quest Journals
Journal of Software Engineering and Simulation
Volume 8 ~ Issue 6 (2022) pp: 23-42
ISSN(Online) :2321-3795 ISSN (Print):2321-3809
www.questjournals.org

Research Paper

Efficient Security Mechanisms for Multi Access Edge Computing (MEC) for IoT

Bharti Rana[1], Yashwant Singh[1], Ravleen Singh[2]
Central University of Jammu[1], Madhav University[2]
{Corresponding Author: Ravleen Singh}

ABSTRACT
The explosive growth of the Internet of things (IoT) and smart devices in recent years have been drastically encouraging the development of edge computing. To enhance the Quality of service (QoS) with low latency in IoT applications, edge computing acts as a promising paradigm that transfers the data from the cloud to edge nodes. Its remarkable development leads to an ignorance of security threats in edge computing. Security has become an alarming issue in IoT. Many researchers have focused on privacy and security issues in edge computing, but limited work has been done in this field. Therefore, it becomes necessary to maintain an environment that is free from security and privacy breaches to give frequent computing services. This paper aims to provide a comprehensive survey of the communication models in IoT. Next, we discuss the basic concepts of edge computing and its architecture followed by a comparative analysis of the security frameworks in Multi-Access Edge Computing. Then, we have addressed the various security preserving mechanisms on edge and confronted the open issues in multi-access edge computing. Finally, we provide an overview of blockchain and its security benefits on edge followed by some conclusions.

Keywords: *Edge Computing, Security, Communication Models, Cryptography, Blockchain*

***R**eceived 12 June, 2022; **R**evised 24 June, 2022; **A**ccepted 27 June, 2022 © The author(s) 2022.*
P**ublished with open access at **www.questjournals.org

I. INTRODUCTION

IoT is a network that is provided with unique identifiers (UIDs) and can exchange data without human-to-human interaction or human-to-computer interaction. The term IoT was proposed by Kevin Asthon in 1999. He is also known as the "Father of IoT". In other words, IoT describes the fastly developing network of interconnected objects which can transfer data by using embedded sensors. The devices of IoT interact with each other and do a lot of work without the efforts of humans. In this way, IoT saves our time. It is a global network that associates everything to the internet for trading the data through gadgets with concurred conventions by recognizing, finding, observing, and managing things. IoT also refers to a system of interconnected things that can gather data on a cloud and exchange it over a wireless network. IoT is the network of physical things that are enclosed with sensors, software, and other applied technologies for the objective of transferring data with other gadgets over the internet. These gadgets range from normal household things to sophisticated commercial instruments. With more than 7 billion connected IoT devices today, specialists estimated this number will become 22 billion by 2025.

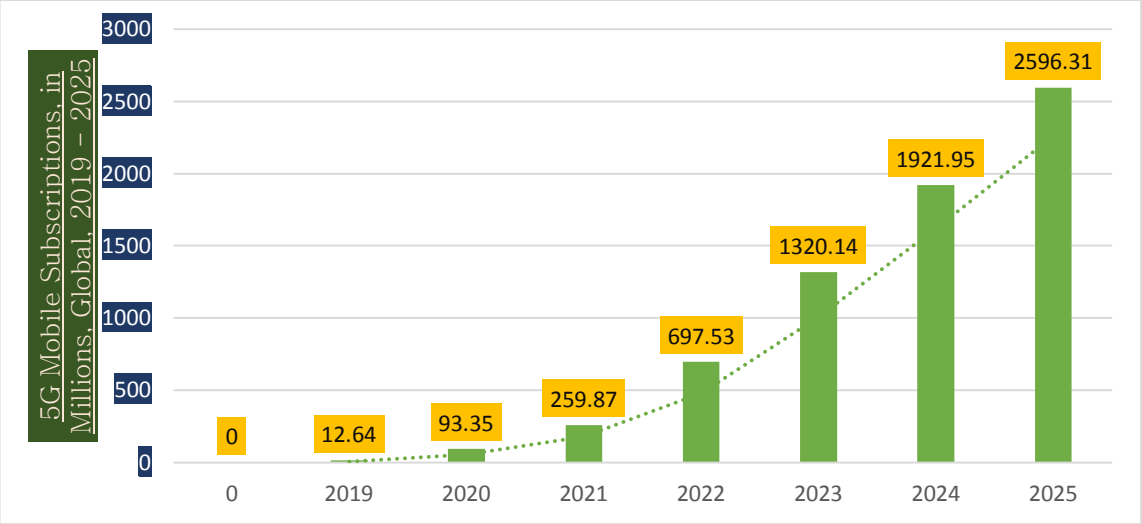

Figure 1: Growth in Mobile Edge Computing Market & Forecasts (2019-2025)[1]

According to the statistical report from the research firm Mordor Intelligence research, it has been estimated that the global edge computing market was USD 93.35 million in 2020. In the coming year, its market value will be USD 2596.31 million by 2025. According to the report, North America is a hub for technological innovations such as 5G. In the future when the new data produced by the market will increase, then we will not be able to satisfy the customer requirements. Then latency will be the critical component for the business. This will lead to radical changes in the business.

MEC is an advanced technology that provides computational resources and backhaul capacity for mobility support, low latency, and location awareness to the end-user and edge of the network. To enhance the efficiency of end-user experience and IoT devices, security in MEC is a key challenge for the formation of the edge paradigm. To overcome the issues related to cloud computing, edge computing was developed. Edge computing enhances the quality of service, reduces latency, and provides high scalability. Edge computing is today's need for IoT. Rather than sending all data collected by IoT sensors directly to the cloud, edge computing processes this data within the network, and only relevant data is sent by reducing latency.

The technologies used by the authors are not so efficient. They lack in terms of privacy and security. As edge computing is not all located within secure datacentre connectivity should be hardened with the use of VPNs and secure tunnels. The edge nodes that have breaches of security can be attacked by an intruder. The intruder will use the edge nodes to enter the whole system. We can use various emerging technologies such as Blockchain, Machine learning, Cryptography, and Artificial intelligence to upgrade traditional encryption techniques to ensure security. Blockchain technology gives a decentred environment by providing a new technique to protect and transfer data securely against any intrusion.

1.1 CONTRIBUTION

Table 1 presents the comparative analysis of our proposed survey with the existing surveys to demonstrate the contribution of the state-of-the-art IoT. The key contributions of the proposed review are as follows:

- Discuss the main IoT elements for efficient communication.
- Provide a comprehensive survey of edge computing and present a holistic overview of related work.
- Identify and examine previous work on MEC challenges.
- We analyzed security approaches on edge in IoT.
- We provide a brief and detailed introduction of blockchain technology with its structure and work.

1.2 ROADMAP

The remainder of the paper is organized as follows. Section 2 provides the literature survey of IoT. Section 3 discusses IoT elements, applications of IoT, and the communication models in IoT. Section 4 outlines the need for edge computing and its architecture followed by the gateway-based edge computing and challenges of multi-access edge computing. Section 5 highlights the securing preserving mechanisms on edge. Section 6 imparts the knowledge about blockchain and its working, and its security benefits on edge and present the types of nodes in the blockchain. Followed by a case study in section 7 we present the findings of the paper and finally, section8 concludes the paper.

II. LITERATURE SURVEY

Yaqiongliu et.al. (2020)[2] proposed a use case that makes use of MEC to attain edge intelligence in the IoT framework. The main aim of this use case is to decrease the transmission rate caused by the interchange of data among the clients and the server. In this use case, the researcher has used five types of neural networks and they are Connected Neural Network (CNN), Convolutional Neural Network (CNN), Recurrent Neural Network (RNN), Long-short term memory (LSTM) neural network, and Gated recurrent unit (GRU) neural network. The researcher proved this by using a MEC server and one cloud server that we can reduce the communication latency. The researcher has also proved that the networks that have maximum efficiency perform best for resolving the problem which explains the strength of smart MEC-enhance proximity detection solutions are GRU neural network and LSTM.

Belal Al.et.al. (2021)[3] provides a comprehensive survey of significant threats, explained the MEC architecture, and point out the functional layers, various kind of threats, and capable security safeguards. The researcher suggested that MEC should execute various layers of security controls to alleviate targeted attacks. A centralized security architecture is required to eliminate the security risk. International Union's Telecommunication (ITU-T) recommends X.805 to give security protection.

Pasika et.al. (2019)[4] analyze the possible threat vectors in the main MEC formation framework that act with the ETSI standards. The author proposed a solution to reduce the identified threat vectors. The author has also given some approaches for example Virtual Machine Introspection (VMI), Trusted Platform Manager (TPM), and Network Slicing (NS) to secure MEC by design.

Peiying et.al. (2020)[5] proposed a strategy to upgrade the security of edge computing by virtualizing edge nodes. Firstly, the author proposed a technique of edge node partition and then virtualizing the edge nodes along with various kinds of things into different virtual networks which are installed in the cloud server and the edge nodes. Secondly, the author proposed a security technique that is based on security level measurement. Finally, by conducting various experiments the author has made a comparison between the existing algorithms to prove the efficiency in upgrading the security of edge computing.

Rongbozhu et.al. (2020)[6] presented the solutions for resource allocation, multimedia processing, as well as novel applications. The researcher aims to throw light on the different aspects of this developing model as well as solutions for the system model, integrity, safety, etc. The author proposed offloading technique to make use of edge devices to process the maximum amount of traffic with minimum power and time.

Jing et.al (2018)[7]proposed a scheme for fiber-wireless access networks and multi-access edge computing which is heterogeneous to attain the multiple application requirements. Various algorithms are developed for example Load balancing multiple routing algorithms (LBMP) and Multipath transmission edge application as an instance of an integrated scheme. Finally, the author conducted various experiments to assess the efficiency of the networking scheme. The performance analysis shows that the multipath based on the LBMP scheme has a shorter delay of 0.1 whereas the standard deviation of the ECMP scheme is 0.3. The results show that the LBMP scheme has better load balancing which can remove network congestion.

Vikas Hassija et.al. (2019)[8] presented security-related issues and security threats in IoT applications at different layers. The author has also discussed various technologies to secure IoT by using Blockchain, Fog computing, and Machine learning. The author has also discussed various open challenges that come from the solution itself.

Ghada Arfaoui. et.al (2018)[9] proposed a 5G-security architecture by using the concept of domain and strata which were earlier used in 3G and 4G networks. In this way, the author builds a 5G network. Finally, the author has proposed a use case for the smart city. This use case targets the two features of IoT gadgets. The first is to provide connectivity and the second feature is to investigate software-defined networks in 5G. In this use case, the maximum number of IoT devices are installed to gather information for analysis for automatic control works. For example, various smart electricity meters are to be installed to check the consumption and production. This use case focuses on NFV (Network function virtualization) and SDN (Software-defined network). NFV and SDN technologies give authority to the mechanics to give economical resources for isolating traffic for specific users. The issue in the network connection is the main warning in a mobile network.

Wei Yu et.al (2017)[10] has proposed a structure for the security assessment of IoT networks with edge computing. This paper throws light on the interpretation of networks and has made the comparison in terms of response time, computation capacity, and storage space, and analyzed the benefits of using edge computing to assist IoT. According to the researcher, edge computing transfer data computation to the edge of the network and near the edge nodes. In this way, edge computing decreases the congestion to minimize the bandwidth needs in IoT.

TABLE 1: Comparative analysis of the proposed survey with the state-of-the-art literature in IoT

Author'sName	Year	Domain	Contributions	QoS metrics	Analysis	1	2	3	4	5	6
Belalet.al[3]	2021	Implementation of multiple layers of security control	The author has presented ETSI MEC reference architecture.	Interconnected, Layered, and flexible	The researcher suggested that MEC must execute various layers of security control to alleviate targeted attacks.	×	✓	✓	×	×	✓
Yaqiong et.al[2]	2020	5G in IoT	MEC enhanced proximity detection architecture by using a connected neural network, convolutional neural network (CNN), Recurrent neural network (RNN), Long-short term memory (LSTM) neural network, and Gated recurrent unit (GRU) neural network.	High Bandwidth and Latency	Latency was less than 1ms. Here low latency requirements can be met by MEC architecture.	✓	✓	✓	×	×	✓
Darshan et.al[11]	2020	Security framework for IoT	A distributed security framework is proposed which integrates three technologies namely blockchain, edge-cloud, and SDN.	Less latency, Improve the quality of services	The proposed security framework will accurately and successfully encounter data confidentiality issues given by the method of blockchain, edge-cloud, and SDN paradigm.	×	✓	×	×	✓	×
Showkat et.al[12]	2020	Edge computing	To upgrade the implementation of various technologies AI, and Blockchain for securing edge computing paradigm.	Scalability, energy efficiency, flexibility.	To mitigate the security issues related to edge computing, the implementation of blockchain is necessary.	×	✓	✓	×	✓	✓
Peiying et.al[5]	2020	Network Virtualization	To enhance the security of edge computing a security framework was proposed to upgrade the security framework. The author proposed a security technique by conducting the various observation.	Complex data and security risk	Network virtualization technology is used to mitigate the issues detected by edge computing and the internet of things.	×	✓	×	×	×	✓
Pasika et.al[4]	2019	Vulnerabilities	SDN and NFV	Limited	Techniques for	×	✓	×	×	×	×

		in the edge network	technologies are considered for deploying the data network in MEHs (Mobile edge hosts).	connectivity, Malicious content could penetrate MEH	hindering virtualization-based attacks are Virtual Machine Introspection (VMI) and Trust Platform Manager (TPM).						
Abdur et.al[13]	2019	Smart City	A blockchain-based framework is proposed to secure Spatio-temporal smart contract services for IoT in a smart city.	Security and privacy	The result shows that without the involvement of a central verification authority the framework provides complex Spatio-temporal services worldwide.	×	✓	×	×	✓	×
Abdur et.al[14]	2018	To secure therapy applications	The author proposed a blockchain-based mobile edge computing framework to secure therapeutic data privacy.	Low-latency, security	The results show that without a substantial rise in mean processing time, this framework supports the maximum number of users.	×	✓	×	×	✓	✓
The Proposed Survey	2021	Secure edge computing in IoT	Discuss the challenges and benefits of integrating blockchain with edge computing.	Security		✓	✓	✓	✓	✓	✓

1, IoT Applications; 2,Security; 3, Challenges; 4, Machine learning; 5, Blockchain; 6, Edge computing. Notations: ✓, considered; ×, not considered.

III. INTERNET OF THINGS (IoT)

There are various applications in an IoT network. Sensors, gateways, and cloud networks are the basic elements on which the IoT relies. The different types of elements, models, and applications in IoT are discussed in the subsequent section.

3.1 IoT ELEMENTS

The main elements in an IoT system are sensors, gateways, and the network for the efficient communication of data.

Sensors: A large number of sensors are situated in a broad region in the IoT. These are the vital segments of IoT and give rise to most of the evaluated information in the network. These sensors can give various kinds of information to assist the IoT by monitoring all the things[10]. For end clients, the gadgets can work as human-PC associates to meet the necessities of clients and send them to the IoT. Every sensor and gadget will be interrelated so that they can transfer information and offer extra assistance.

IoT Gateways: The IoT gateways join the network of the sensors and core network to the cloud servers. When the end nodes produce asset needs for IoT operations, they will transmit the information to the cloud servers[10]. The sensors can set up a network to send their created information. It is important to execute information before sending them to the cloud workers.

Cloud/Core Network: Cloud servers will get the information through backhaul networks. The cloud servers have a critical limit with regards to calculation and the ability to assist IoT operations. In this way, the cloud servers can fulfill the asset necessities of various applications. At that point when the information handling is finished the cloud server will convey the outcome to the end clients. The end clients will request the cloud servers to attain the information.

3.2 IoT APPLICATIONS

Security is very crucial in most IoT applications. The IoT applications are developing very quickly and are utilizing in most of the industry. Most of them need more security from the technologies they use. Figure 2 represents the various applications in an IoT network.

- **Smart Home**: Smart home is one of the pioneering applications in the field of IoT. The home where internet-connected IoT devices can monitor and manage the appliances such as heating, cleaning, lightning, and home entertainment system is known as a smart home. A smart home makes the life of people easy and comfortable. A smart home has various functions: household accidents can be prevented by using alarm systems and room heating or cooling can be maintained by using automatic ACs. Security is very essential as we are using costly appliances in the smart home. By using CCTV smart cameras, we can monitor every activity of our home by sitting in any area. Various wireless IoT sensors and actuators in the floors, corners, and walls are deployed in smart homes to improve the quality of life[15]. We can conserve energy by using smart meters in the supply of electricity, water, and gas as people will not be able to indulge to steal the energy. Both physical and cyber attacks[8]takes place in the smart metering system as these are very sensitive. All the electric appliances are linked with smart meters and the data gathered by these appliances can be used for cost and load management.

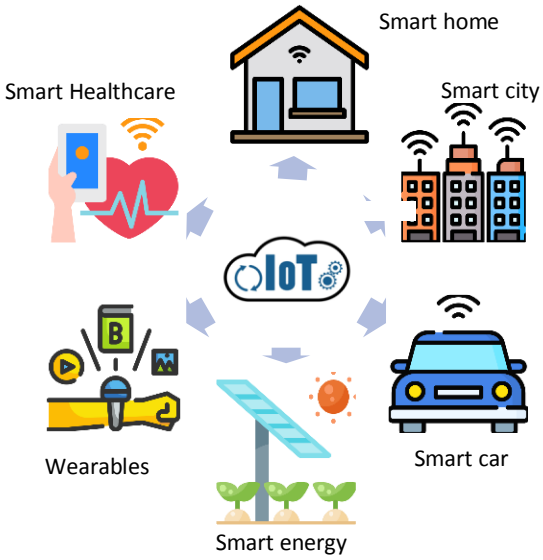

Figure2: Applications of IoT[16]

- **Smart Cities**: Smart cities use modern communication devices to improve the quality of life of the population. In other words, a smart city is a city that uses the latest technology to enhance sustainability and give its citizen a voice. Smart cities have robust IoT connectivity and digitalization. There is a crying need for good governance, especially E-governance and citizen participation in a smart city. The core elements in a smart city are adequate water supply and assured electricity supply for 24 hours. Smart cities make extensive use of emerging IoT devices such as smart traffic lights, smart transport like Metro services, emergency services, and public safety[2]. Modern CCTVs should be installed in every corner of the city to minimize crime.
- **Smart Energy**: The smart grids are advanced grids in ICT that has the potential to generate energy, transportation, and distributed network. A smart grid comprises various elements such as energy-efficient assets, smart equipment, and in-exhaustible energy sources[2]. MEC plays a significant role in promoting smart grid by applying low latency services. Power consumption data can be collected and prepared at the MEC server for instance: Microgrids and smart meters to maintain the workload.
- **Industrial Internet**: The Industrial Internet of things (IIoT) is also termed industry4.0, which is a typical application of IoT in the field of production. IIoT has integrated many automatic and transmission technologies like machine learning and M2M transmission to upgrade connectivity and observation[17]. IIoT furnishes various advantages such as upgrading performance, flexibility, time-saving, and cost-saving to maximize the production by modern machinery.
- **Wearable IoT**: Wearable technology is also called "wearables". It is a type of electronic gadget that can wear as attachments used in clothing, or inserted into a user's body[18]. Numerous things have been manufactured in this field-ranging from a hair pin to footwear and from watches to kitbags. Wearable gadgets are electronic devices worn by customers to capture biometric information related to health or fitness. This technology request the operating system be secured. Low bandwidth is needed to exchange information between

the connected devices. After smartphones, wearables will become the top-selling consumer electronic devices with global availability of more than 929 million devices by the end of 2021.

- **Smart Healthcare**: Health care is very essential to have a longer life span, whether it is in a hospital or a nursing home. By using smart health care, the population of each age group can be cured at the same time. By using various technologies like wearable devices, IoT, and mobile internet, institutions related to healthcare actively manage and intelligently respond to the medical ecosystem. Smart healthcare is a technology that leads to smart diagnostics tools, and better treatment for patients. Smart health care has modern devices such as blood pressure monitors, and dialysis machines. In smart healthcare, patients' medical reports can be seen by doctors by sitting in any corner of the world. It is necessary to secure the patients' personal information from anyone as data is confidential. Smart health cards are also provided by the government to meet the medical facilities for every person who cannot afford the costly treatment.

3.3 IoT: COMMUNICATION MODELS

The main concepts of IoT in edge computing are reviewed and discussed. Following are the three different communication models in IoT.

- **Machine-to-Machine Communication**

This correspondence model addresses different gadgets, that can interface and transfer data among one another without the help of any equipment. These gadgets can interface with each other through different kinds of networks. For instance, figure 3 exhibits a brilliant switch that makes contact with the shrewd light over Bluetooth4.0.

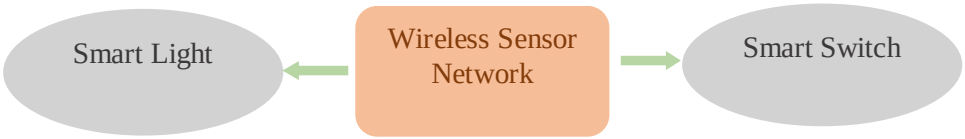

Figure3: Illustration of Machine-to-Machine Communication

This model is generally used in various applications, for example, brilliant home frameworks, smart meters, or programmed control in the electrical framework which interact with one another by sending little information.[10] The main IoT gadgets of this category are shrewd switches, brilliant entryway locks, and smart fire alarms that transfer little information bundles. From the client's point of view, the issue of machine-to-machine communication is the absence of consistency in which various gadgets from different producers utilize various conventions. For instance, the Z-Wave convention gadget cannot interact with the Zigbee convention gadgets. These problems restrict the client's decisions and understandings.

- **Machine-to-cloud communication**

In this correspondence model, IoT gadgets request services from a cloud specialist organization to accumulate information into distributed warehouse according to the computational capacity of the gadgets[10]. This model needs support from previous models like traditional wire cable connections or wi-fi associations which appeared in figure 4. This model also resolves the issue of the previous model. This model is reliant on conventional organization and data transmission. It is important to upgrade the network framework to enhance the efficiency of the model.

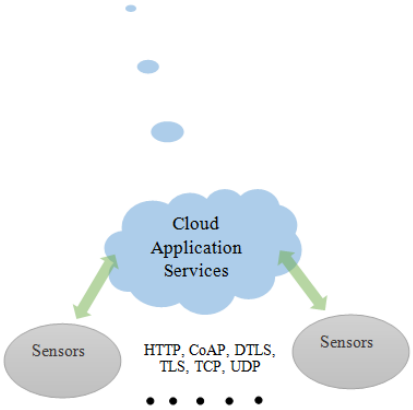

Figure 4: Illustrationof Machine-to-Cloud Communication

- **Machine-to-Gateway Communication**

In this model, the gadget-to-application layer model is referred to as a router. Given below is the formation of Machine-to-Gateway Communication. In the application layer, safeguard plans regarding the program or other services like information or application gateway algorithms move on a gateway to perform as a mediator connection among IoT gadgets and cloud communication functionalities. This upgrades the safeguard plan and adaptability of the IoT organization and transfers a portion of calculated assignment to the application layer. In this way, it lowers the power of IoT gadgets. For example, the brilliant cell phone performs as the gateway, to function some operations for exchanging information with IoT gadgets.

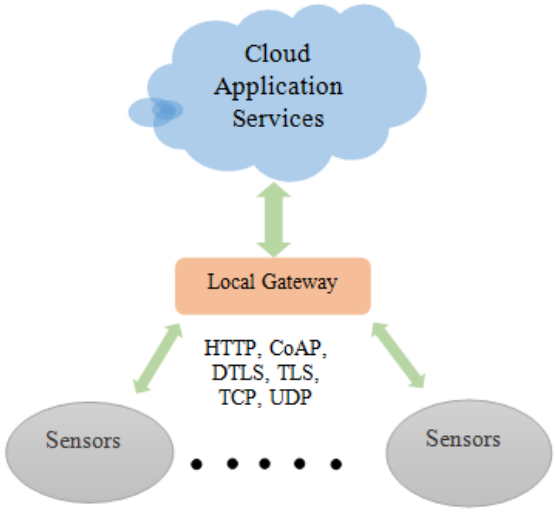

Figure5: Illustration of Machine-to-Gateway Communication

IV. EDGE COMPUTING

Edge computing is a distributed computing paradigm that aims to bring data storage closer to the site to save the bandwidth and upgrade the response[19].To mitigate the limitations[2] associated with cloud computing, Edge computing was developed. Because of the fast expansion in the number of cell phones, ordinary unified cloud computing is trying to fulfill the QoS (quality of service) for certain operations. Edge computing will be the main reason to address this problem with 5G technology. Radio access network (RAN) is the main challenge that is connected with 5G technology. In this network, Mobile edge computing offers ongoing RAN information. By utilizing the continuous RAN data, the network providers will upgrade the Quality of experience for end clients. Consequently, the organization agents can apply RAN by outcast co-executive and rapidly develop the arrangement of modern operations. Also, the computational center points are performing their duties to transfer equivalent safety ideas to ensure the same degree of safety.

4.1 EDGE COMPUTING ARCHITECTURE

In figure 6, the cloud servers are far away from the edge computing servers than the end clients. As compared to the cloud servers, edge computing servers have lower calculation ability to give superior QoS (Quality of Service) and lesser latency to the end clients. Edge computing has mainly three aspects the front-end, close-end, and far-end as demonstrated below.

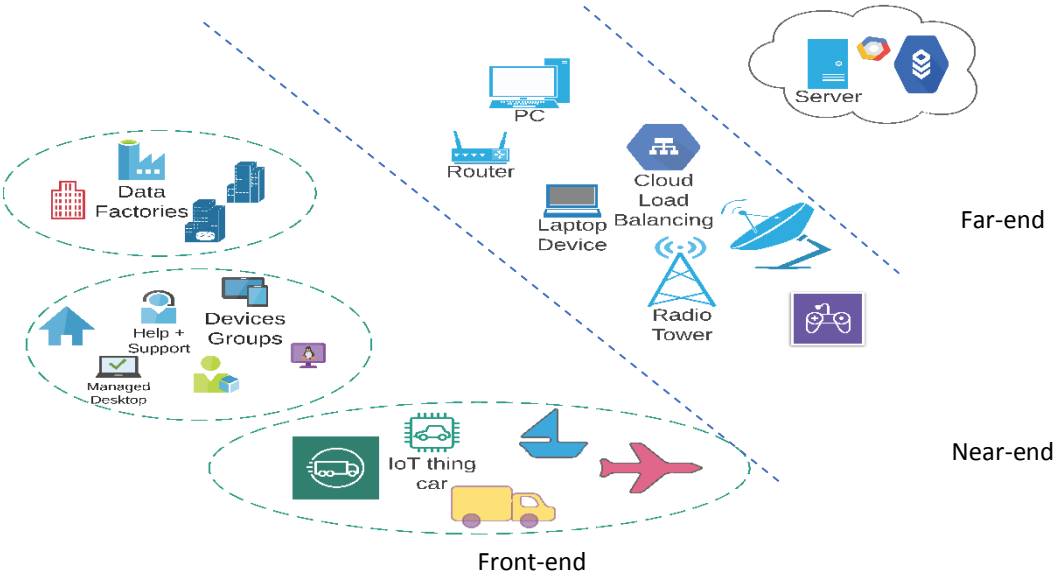

Figure 6: Edge Computing Architecture[10]

Front-end: In edge computing architecture, the end gadgets (e.g., actuators, sensors) are situated at the front end. Edge computing can give immediate assistance to certain applications with calculation ability given by a large number of end gadgets. Because of the restricted limit of the end gadgets, the majority of the necessities can't be fulfilled in the front end. Subsequently in this way, the servers will get the suitable necessities provided by the end gadgets.

Near-end: Most of the traffic flows in the network can be controlled by gateways that are at the near-end. The maximum part of the processed information and capacity will be moved to the near-end in edge computing. Due to this, the end clients can get a superior performance on processed information and capacity with a little expansion in the latency.

Far-end: The communication latency is important in the network when the cloud servers are installed far away from the end gadgets. However, maximum data capacity and computation power are provided by the cloud servers.

4.2 GATEWAY-BASED EDGE COMPUTING

In the course of the most recent decades, the Internet has advanced from a shared system to the internet and the traditional internet has now become the Internet of things. IoT brings an enormous change in the technology perspective by associating a flexible and monstrous assortment of things to the internet. With IoT, individuals and objects can interface at any time with anyone, preferably by using the network. Additional critical headway of the internet will be the Tactile Internet. Tactile Internet is highly used in the case of human-to-machine and machine-to-machine interaction described by super less inertness with more accessibility, authenticity, and safety. IoT framework incited huge popularity for information, and processing assets just as system functionalities oblige the foreseen bunches of interconnected gadgets[17]. Satisfying these outrageous needs will require an adjustment to existing organization frameworks.

Edge computing is empowering another age of revolutions that work near end nodes. Two kinds of functionalities are permitted by edge computing:

• Edge computing decreases the amount of information that must proceed to the subsequent congestion to reduce the latency and lowers the transmission cost

• Edge computing handles unwavering quality very well. It provides uninterruptable services.

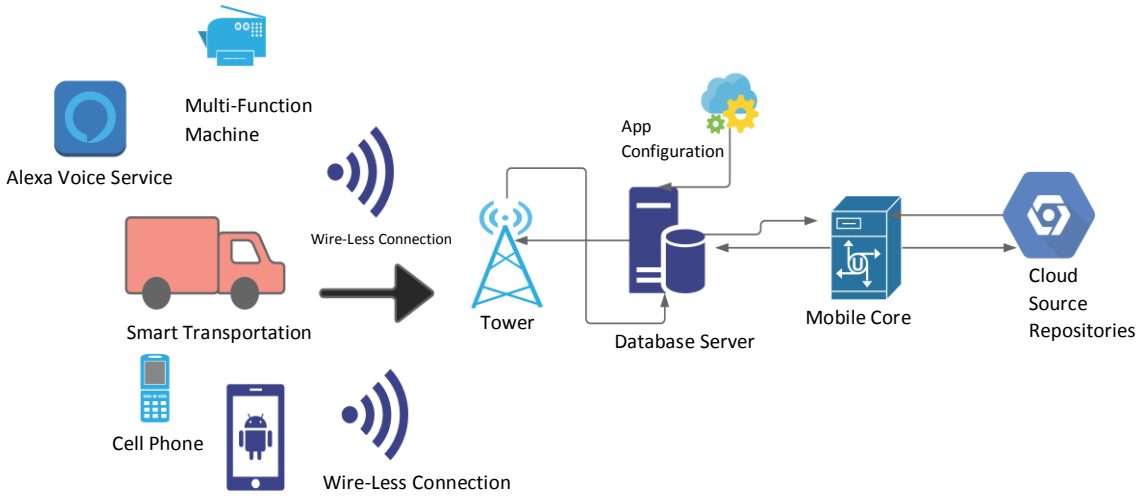

Figure 7: IoT Gateway Framework[17]

Two primary innovative arrangements are required to perform operations on boundary devices in an IoT network: multi-access edge processing (MEC) and fog computing. The traditional design includes processing abilities for boundary switches and end client gadgets. Surely, MEC adds processing capacity in the region of broadcasting stations and recommends an organization to deal with the existent cycle of the executives (LCM) of edge applications. The European Telecommunications Standards Institute (ETSI) is giving particulars to MEC through the MEC Industry Specification Group (ISG)[20]. Later, a few guidelines have been portrayed by ETSI to adopt MEC design, a MEC application model (descriptor), MEC services, MEC coordination, the executive's system, etc. In addition to empowering applications at the edge, MEC also offers different types of open assistance through application programming interfaces (APIs). API gives data to the dynamic clients and cell centre stations, for example, the radio transmitter nature of clients. This permits the establishment of mindful operations. IoT is the main key instance of MEC which is recognized by ETSI.[17]. MEC in IoT enables small IoT gadgets with extra computational capacities through data offloading. Also, IoT exponentially increases MEC services to a wide range of intelligent objects. As demonstrated in Figure 7 MEC proceeded as door hubs that can collect and transfer the little information parcels produced by IoT administration. The three key advantages of IoT in MEC are:

- Minimize the amount of traffic.
- Robustness in-network services.
- Reducing the computational workload.

Table 2 depicted how IoT can leverage MEC technology in various application scenarios. IoT itself is a classic application of MEC where the key value proposition of MEC is exemplified in a variety of application scenarios. These values become evident in the utility factor measured by the end-user experience while using such IoT-related services. Table 2 shows the characteristics of different IoT applications and how each application benefits from MEC-IoT integration.

Table2: MEC and IoT benefits for each application.

Essential Features of MEC in IoT	**Description**	**Smart home**[21],[22]	**Smart city**[2],[23]	**Wearable IoT**[18],[24],[25]	**Smart energy**[17],[2]	**Industrial Internet**[17],[26]

Less Latency	Upgrade maximum volume of data messages with minimum delay	×	✓	✓	✓	×
Increased Bandwidth	Potential to transfer the maximum quantity of data fastly	✓	✓	✓	✓	✓
Low power devices	Reinforcement for fewer power devices that have restricted communication powers.	×	×	✓	✓	✓
Private or regional network	Restrict the transmission and transfer of data to a particular network	✓	✓	✓	✓	✓
Safety	Grant regional safety	×	✓	×	✓	✓
Privacy	Grantregional Privacy	×	✓	✓	✓	✓
Rapid Mobility	Authorize the capacity to proceed within the network or network coverable area	×	✓	✓	✓	✓

4.3MULTIACCESS EDGE COMPUTING CHALLENGES

- **Security for MEC:** Many researchers have focussed on the security issues in edge computing but limited work has been done in this field to provide the solution. The development pace of the security issues cannot fulfill the demand for advanced security challenges to meet the growing demand for the security maintaining mobile services. Most edge devices are asset manageable. Therefore, it is difficult to apply ongoing information security techniques on edge devices. Consequently, it is a big challenge to secure the MEC system[2].
- **Site Selection for MEC server:** In an IoT network, more MEC servers are installed where maximum computational demands are required. Consequently, while installing MEC servers a combined issue of reckoning resource arrangement and selection of the site is required to be resolved by the researchers[27].
- **Edge Intelligence:** Intelligent offloading in IoT is still lacking in edge computing. To save cost, efficient energy, or to acquire quick calculation, conventional offloading generally carries calculated work to the MEC server at the edge. The issue in edge intelligence can be resolved by using advanced AI techniques such as Reinforcement[28] and deep learning[29]. Thus, various parameters are needed to be examined by the researchers to acquire brilliant offloading which is a severe challenge.
- **Mobility Management:** In a real-time application, the mobility management technique cannot be used as VM migration acquire a heavy burden in the backhaul network which leads to a long delay. To mitigate long delays in the network, several delay-sensitive methods need the mobility management method[30]. Hence, this is a challenge for the researcher to give a better real-time method to pace up with the upcoming VM migration technique.
- **Pricing models in Network Function Virtualization:** NFV technology encounters so many challenges. For example, when the resources are used unfairly it bottlenecks the physical framework by the use of resources among many users. Appropriate pricing techniques can be utilized to help users to use the resources smartly.
- **Data Correlation:** A large amount of data would be produced from the edge framework persistently, where some of the data is tactful and put under strong safety but some of the data is not so tactful and revealed in front of the public without any safety in an edge-computing system. Consequently, invisible connections occur within the data that are not genuine. However, by utilizing these relationships and exploiting numerous models an intruder can reckon the data and even tamper[31].
- **Privacy in MEC:** Data privacy is a crucial challenge as a large quantity of clients' personal information gathered from edge nodes is imparted to the MEC or MCC servers.[2] There is a need to pay attention among clients to use both privacy protection and other activities like data privacy (e.g, restoring, examining, penetrating). Nowadays, location information is becoming a crucial challenge. The privacy of location can be secured by engaging cache proxies to accumulate the information regarding location rather than dispatching the actual location to location-based services.

5. SECURITY PRESERVING MECHANISMS ON EDGE

The various security preserving mechanisms on edge are blockchain, cryptography, machine learning, and artificial intelligence.

- **BLOCKCHAIN:** Blockchain is a method in which a record of transactions is made in a way that makes it impossible to hack the system. It is a digital ledger of transactions that is categorized in the whole computer system on the blockchain.[32] Various security issues are already existing in an IoT network. Blockchain is a suitable technique to address the security issues in IoT. Blockchain technology brings radical change by tracking and keeping a record of every document. All the devices that are linked with the application must have authentication in the blockchain network. After registration, the devices can give the best performances according to their characteristics. In the same way, clients need to authenticate in the blockchain network. Consequently, in the network client examine and observes the distinct objects.

- **CRYPTOGRAPHY:** Cryptography is a method of securing the information by using codes to provide information to the intended user who processes and understands it. In this way, this method prevents the information from an unintended user. Before transmitting the data to the cloud servers this method encrypts the context of the data. This method experiences excessive overhead and needs essential key management. To operate the data without disclosing the information Homomorphic encryption (HE) can entrust the task to the third parties[33]. HE technique produces a key pair that is based on numerical problems that are not able to give the solution by computers. There are two types of keys one is a public key and the other is a private key. Data will be sent to the mediator by the public key, then the mediator will do all the processes on the encrypted data and give feedback which can only be decrypted by the private key. In the whole process, the information is confidential. RSA algorithm and the ECC algorithm are the common homomorphic encryption algorithms.

- **MACHINE LEARNING(ML):** Machine learning is a subfield of artificial intelligence that makes the machine automatically learn from past experiences[34] without being programmed. The main aim of the machine learning technique is to enhance its efficiency and to provide the particular security policies to implement in the data plane. The main goal of the ML technique is to alleviate a variety of attacks by defining access control policies or by labeling the network traffic. For example, a Neural network can be used to find network intrusion, K-NN, and DoS attacks in malware detection. Machine learning is used when humans are unable to use their experiences, for example, speech recognition, robotics, etc. Machine learning is also used in various smart systems, for example, Google is using machine learning to find out the threats against mobile applications and endpoints operating on Android. Similarly, Amazon has introduced a Macie service[34] which uses machine learning to allocate information that is stored in the cloud. Machine learning is classified into three groups namely supervised, unsupervised, and reinforcement learning[35].
  - **Supervised Learning:** It is a type of machine learning technique in which training is given to models by using labeled data. In this type of learning, there is a need to find the mathematical function for the models to map the input variable(X) and the output variable(Y).

Y=F(X)

Assume that we have a picture of different kinds of vegetables. Now, there is a need to classify the vegetables accordingly. So, to classify the picture of vegetables we will provide both the input and output data, which means we have to instruct the model by recognizing the shape, color, size, and taste of each vegetable. When the instructions are concluded, we will attempt the model by giving a new basket of vegetables. In this way, the model will recognize the vegetable and give the output with the help of an algorithm.

  - **Unsupervised Learning:** In Unsupervised learning, data need not be labeled. It tries to find hidden correlations on its own. With the help of an appropriate algorithm, the model can train itself and only input data is given to the model. It is less accurate as compared to supervised learning. For example, Unsupervised learning was used by NASA for the formation of clusters of celestial bodies which were based on the identical characteristics of objects.[36]
  - **Reinforcement Learning:** It is used in many software and machine to monitor the result of its output and compute its value function[35]. It uses a try and error strategy which is distinct from the above two types. In reinforcement learning, particular results are not defined and the user acquires knowledge from the feedback[34]. For example, Autonomous parking.
- **ARTIFICIAL INTELLIGENCE:** AI is a technology that makes a computer system behave and copy the human thinking power. It does not need any prior program. On the other hand, these systems use algorithms that perform their job with their intelligence. It is used to solve complex problems. Artificial Intelligence provides a solution for various IoT security threats[37]. The conventional solutions lack in terms of processing capability and have low real-time execution and less efficiency. Nowadays, AI methods provide new solutions to the problem such as DDoS attacks are becoming a global problem. On a cyber platform, it is one of the most powerful weapons that use multiple servers and internet connections to intrude on the targeted resource.

Whenever a website is not working or crashing it means it has been attacked by an intruder. To solve this problem artificial intelligence approach is used. Different attackers can intrude in the different systems at the same time in different positions. Therefore various AI-based detection methods namely the K-nearest neighbor (K-NN) algorithm, fuzzy logic, and SVM (Support Vector Machine) are used[38].

6. BLOCKCHAIN: SECURITY BENEFITS ON EDGE

Blockchain is a distributed, open, decentralized paradigm that can be used to keep a catalog of data records[33]. The various security benefits of the blockchain are depicted in Figure 8.

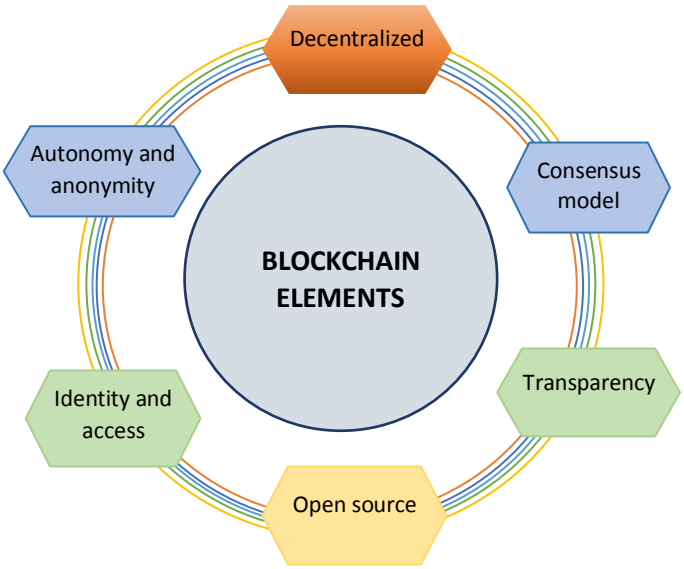

Figure8: Security benefits on Edge using Blockchain.

- **Decentralization:** In Blockchain technology, there is no requirement to control each transaction of blockchain by a centralized trusted authority[12]. Blockchain technology is more secure due to the absence of centralized management in it. In the blockchain, the information of transactions is validated, saved, and upgraded. To secure the nodes in the blockchain network, consensus protocols are used so that data cannot be lost.
- **Open Source:** Blockchain technology is itself an open-source[12] platform that can be launched to frame their applications and attain suitable outcomes without getting consent from any central management. For example, Bitcoin Cash, Dash, Ethereum, Litecoin, etc are powerful open-source platforms made by community members. Users can use new technologies in open-source applications.
- **Anonymization:** Anonymization techniques are used for preserving the identities of a group of people by erasing a few of their key features such as ID number, and user's name[33]. The relevant data is essential and will not be destroyed during the exchange of information as the lost information has a direct relationship with a particular identity. That is why Bitcoin is regarded as pseudo-anonymous which means a user may be linked to a public address but not with an actual name or address.
- **Transparency:** Data registered on the blockchain network give users a chance to go through the previous data of all transactions and update the data after getting verified by all the nodes and consequently can be verified.
- **Consensus Model:** Due to the presence of consensus protocol in the blockchain, every transaction in the blockchain is fully safe and valid. The consensus protocol is also known as the central part of the blockchain network. This model permits all the data to be followed by a single authority. The consensus model protects against malicious attacks.
- **Identity and access:** In blockchain technology every user keeps their digital identity information on identity wallets through identity management[39]. If a device is sanctioned then identity credentials are valid. The main criteria associated with blockchain identity and accessibility are:

➢ Public: In a public blockchain, there is no need for permission, anybody can make new blocks.
➢ Private: In a private blockchain, only authorized users can take part and add to the blockchain. It is a restricted network where permission is required to join.
➢ Consortium: Only authorized users can verify, view, and take entry in the blockchain. It is handled by authorized nodes.

TABLE3: Comparison of different types of blockchain networks.

FEATURES	PUBLIC BLOCKCHAIN	PRIVATE BLOCKCHAIN	CONSORTIUM BLOCKCHAIN
Consensus Operation	Permissionless	Permissioned	Permissioned
Security	Prone to malicious attack	Trusted	Trusted
Energy Efficiency	High	Low	Low
Transaction approval time	Relatively longer compared to private and consortium	Remains lower than one second	Comparatively faster than Public Blockchain
Complexity	More	Less	Less
Type of Network	Decentralized	Centralized	Partial
Entity identity	Anonymous	Known Identities	Known Identities
Immutability	Impossible to tamper	Could be tamper	Could be tamper
Speed	Low	Fast	Fast
Access	Anyone	Single group	Multiple groups

6.1 TYPES OF BLOCKCHAIN NODES

Generally, there are two kinds of nodes in a blockchain network. The hierarchy of blockchain nodes is demonstrated in Figure 7.

1) Full node
2) Lightweight node

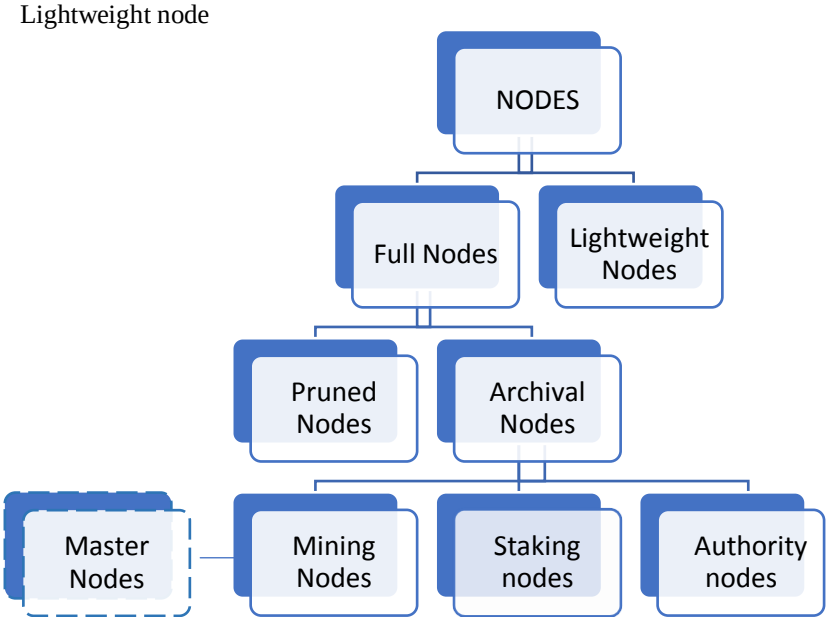

Figure 9: Hierarchy of Blockchain Nodes.

- Full node: The functional node which plays the server node is known as the full node. This node can maintain a copy of all the transactions which are performed in the blockchain. It can verify, receive and dismiss the transaction[40]. It also decides the future policy.
- Pruned node: It is a type of full node[41]. In the beginning, pruned nodes retain the information of the blocks but when these nodes arrived at the intended limit, they remove the previous ones and keep only the header of blocks.
- Archival node: Archival node give a complete record of everything happening on a blockchain. This node is efficient concerning space utilization. They act as a server that hosts all blockchain. These nodes can easily add blocks that can be verified.
- Miner node: Mining nodes are also known as miners. All the transactions can be added by these nodes to a blockchain.
- Staking node: This node creates new blocks in the blockchain which are to be rewarded. The Proof of work algorithm determines which node will be honored. In staking, there is no need for costly equipment. Everybody can have a crypto wallet online that can be downloaded with a device like Raspberry pi.
- Authority node: Networks that make use of selected algorithms, in general, are known as authority nodes. The main function of this node is to generate and validate blocks but at the same time, they exchange information with clients on the network[41].
- Master node: The main purpose of the master node is to keep a record of the transaction and validate them. Similar to miners in a proof of work[42] master node try to give the solution to the issue by acting as full

nodes and the workers are awarded. The first virtual currency to consider the master node model was Dash, a fork of Bitcoin.

- Lightweight node: Lightweight nodes are the simple payment verification code (SPV)[43]. These nodes interact with the blockchain to give the required information. Without the verification of the transaction, these nodes store all the transactions. Consequently, the size of a full node is always greater than the lightweight nodes.

6.2 BLOCKCHAIN: STRUCTURE AND WORKING

A blockchain is a set of blocks that builds a ledger which is used to secure the data by using cryptography[44]. Each block is associated with a cryptographic hash function. The main feature of this technology is that it keeps an eye on all the changes in the block so that no data in the block will be modified retroactively[45]. By doing this, without the interruption of any mediator like banks or government this technology is a very protected method for exchanging money or properties. In this way, once the data is recorded in the blockchain it cannot be changed or updated.

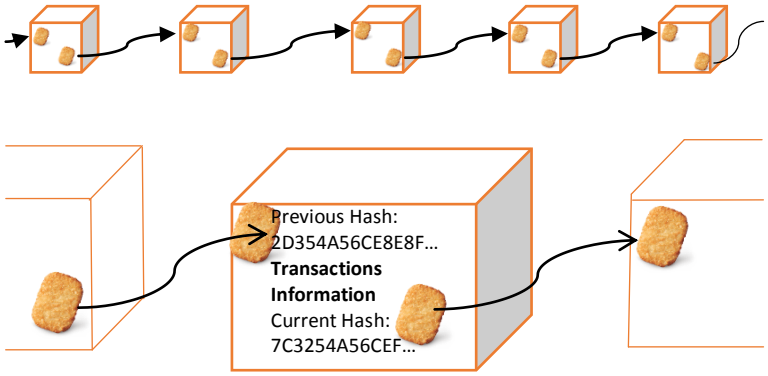

Figure10: Basic Structure of Blockchain

In figure 10, the foundation of the blockchain is known as Genesis Block. Each newly generated block is then attached to the previous block in the chain. Therefore, each block is attached to the foundation block. A hash is also in each block apart from the information. The hash could be viewed as a unique finger impression that extraordinarily recognized each block and its contents as appeared in figure 11. Consequently, any kind of variation in the block will provide a variation in the related hash[46]. Hash provides a fundamental assurance for the security of blockchain and plays an indispensable role in the blockchain method. Each block has its hash and the main is shown in figure 11. This strategy makes the blockchain one of the innovative and safe alternatives in the business. Suppose when a block is attacked by an intruder to change its data which is stored in the block, then the hash of the actual block will change, but the hash in the following block will not change. This shows that all the following blocks in the chain are invalid.

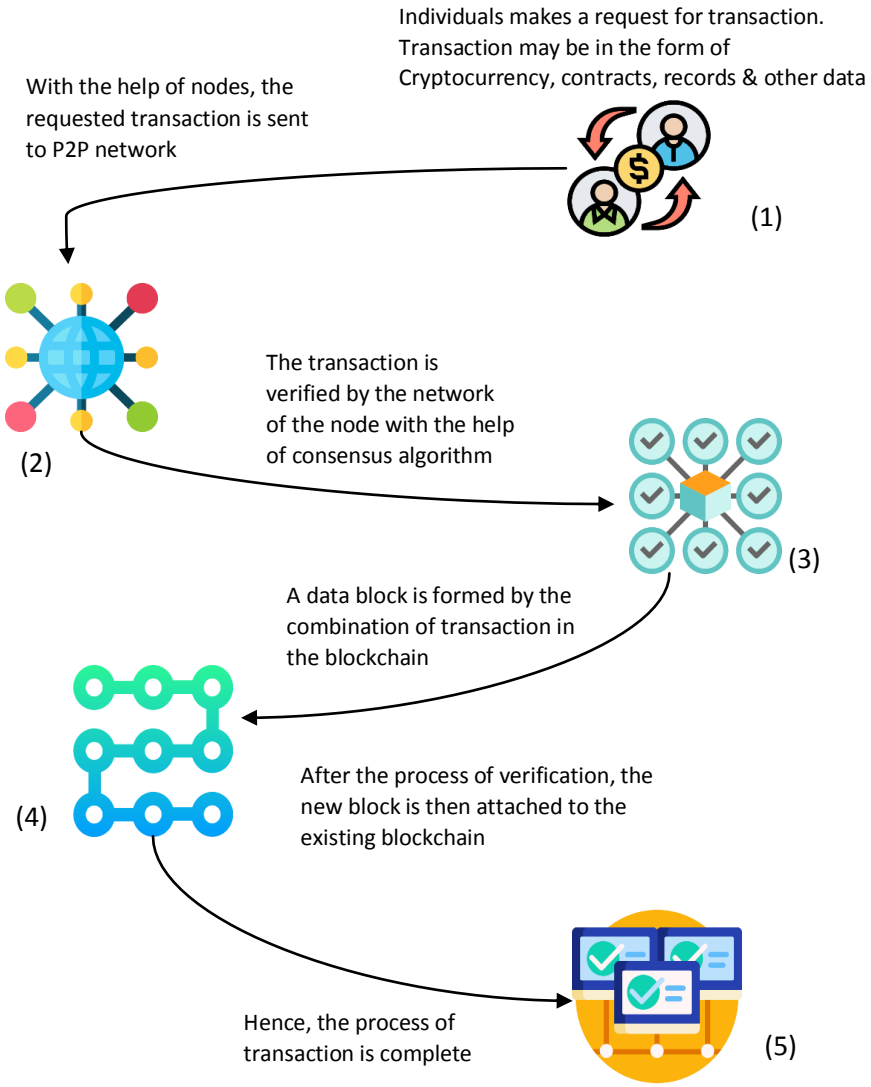

Figure11: Working of Blockchain

The procedure of the transaction begins with a request by the user. Then, in the network, the transaction is transmitted. After that, with the help of hashes, the verification process begins. After the completion of the verification process, the new block is then attached to the existing blockchain which makes it unalterable. The utilization of hashes makes the blockchain method secure. But the intruders can alter the data in a block with the help of powerful computers and then all the hashes of the succeeding blocks are computed. To solve this problem, various consensus algorithms have been introduced[47]. The affirmation time relies upon the transaction volumes, size of the block, and the algorithm that has been utilized. Algorithms with distinct features have been created and used in business. The main consensus algorithms are[48]:

- **Proof of Work (PoW):** The term "Proof of work" was coined by Markus Jakobson and Ari Juels in 1999. The PoW is used to choose a miner for the upcoming blocks. The miners use a hash function (i.e. mathematical functions) to solve the mathematical puzzle without errors. If the miner creates a new block accurately it will join with the blockchain and gets rewarded[12]. The most popular cryptocurrency using this PoWapplication is bitcoin.
- **Proof of stake (PoS):** This algorithm is energy-efficient and provides distributed consensus in a blockchain[49]. In PoS, a new block is selected by the combination of random selection. Users have investigated that this algorithm is not so risky as it reduces the opportunity for an intruder to hack the system.
- **Practical Byzantine Fault Tolerance(PBFT):** This consensus algorithm was coined by Barbara Liskov and Miguel Castro in the '90s [50]. The main aim of this algorithm is to provide the solution to the issues which are already associated with Byzantine Fault Tolerance. It is energy efficient as this algorithm does not require difficult mathematical computation as in the case of PoW. There are two types of nodes that are used in this algorithm one is the primary node which is called as leader node and the other is the secondary which is

called a backup node. If the primary node fails, then any node in the system can shift the primary node by converting from secondary to primary.

- **Proof of Authority (PoA):** This type of algorithm can be visualized as an embedded pattern that gives a rapid consensus process. By the use of this algorithm only verified users which have their accounts approved can request a new transaction in the block.
- **Proof of Burn(PoB):** With PoB, rather than spending coins on any valuable devices, validators burn[49] their coins by transferring them to an invalid address. After this, users fabricate new blocks and receive the reward. When the participating nodes invest at the beginning with the permission of PoB and build their shows on the blockchain to become authenticated validators. In this way, PoB provides less energy consumption[50] as compared to PoW.
- **Proof of Elapsed time (PoET):** PoET is a consensus algorithm that selects new blocks on the chain. The node which has a minimal expiry is chosen as the leader[51] by connecting every node for a random amount of time. The blocks which are generated are transmitted to the network. If a similar type of node is chosen as a leader it is authorized to search the intruder in the system. Due to the random allocation of time PoET provides the solution for the energy consumption issue in PoW.

7. CASE STUDY: VEGETABLES SUPPLIER SUPPLY CHAIN USING BLOCKCHAIN

Since organizations need explicit methodologies in running supply chains that's why the supply chain in the organization is hard. Thus, it is very challenging to evaluate the quantity of the ordered products[52]. Although, Blockchain can remove this obstacle. In this case study, vegetable provider organizations have new customer organizations that consistently purchase raw vegetables for resale. Customers who need to buy vegetables request by sending messages, e-mail, or book orders online. When the vegetable provider organization gets a request from the customer, these organizations will make a receipt as proof that the order has been confirmed by the organization. At last, the requesting customer will get a payment receipt along with their order.

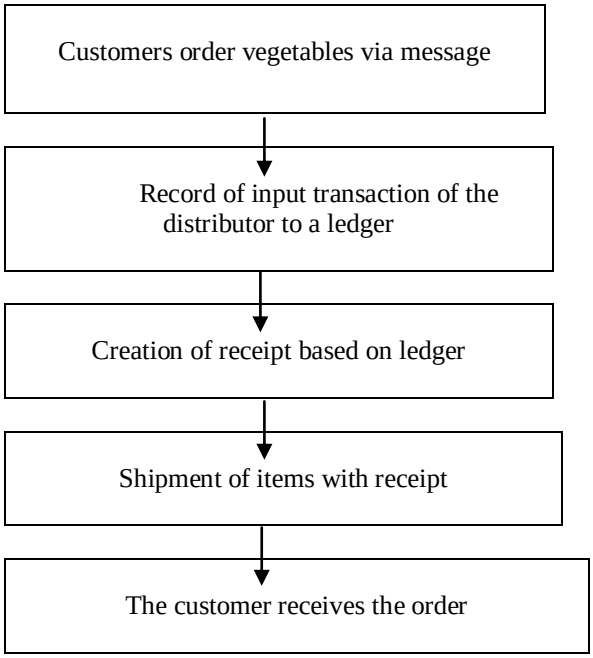

Figure 12: Steps of requesting services in the vegetable supply chain.

The procedure generally delays that can rise the possibility of late shipment of the order to the customer. But few customers never accept the late delivery of products. Except for the late delivery of the products, variation in demand of order is a critical problem. If the items in the order are incomplete then the distributor must add surplus items and send the customer to complete the order.

A blockchain network is made for the vegetable requesting organizations to mitigate the issues of speed of transaction recording and validate the ledger of the vegetable provider organization. The blockchain itself records the information to mitigate the issues when the exchange of information and the ability of the blockchain in circulating records and making the ledger irreversible is very beneficial to solving the problems regarding information stored in the ledger.

Hyperledger Fabric is a framework that divides the implementation of the transaction from the requesting transaction[53]. It includes two steps: Implementation of order and validates the order. With the use of Hyperledger Fabric, a blockchain network for the vegetable distributed organization is framed which contains nine orders, one distributed company, and nine customer companies, everyone has two associators, nine channels, everyone comprises of two provider associators and two companions one customer administrator, for Kafka brokers[52] and three zookeepers for crash fault-tolerant consensus. Kafka is mainly a fault-tolerant and commits log. In the blockchain network, there may be many Kafka nodes correlated with the zookeeper group.

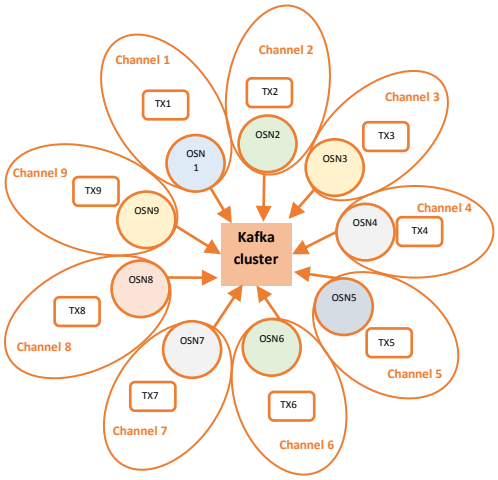

Figure 13: Blockchain Plan for a vegetable provider organization

The reason for making a particular nine-channel for each customer association is to enhance security on the grounds. The peers who are enrolled in the channel can interact with exchanges so that data transactions are frequently completed where costs are concerned upon will be framed into a block is just possessed by peers on the channel.

8. CONCLUSION

Edge computing plays a pivotal role to remove the flaws related to cloud computing. Security and privacy are crucial challenges influencing its acknowledgment. In this article, we have presented a survey of edge computing in IoT and specifically throw light on the security benefits of edge computing in blockchain including the working of blockchain to enhance the implementation of different technologies such as cryptography, machine learning, and artificial intelligence. Furthermore, security preserving mechanisms on edge are explored in detail to provide security. At last, a blockchain-based case study for vegetable provider organizations is discussed to showcase the actualization of its work. In addition, various challenges in MEC are addressed in this article. In the future, we will explore more in-depth to offer security solutions on edge using the blockchain model.

REFERENCES

[1]. "Edge Computing Market | Growth, Trends, Forecasts (2021 - 2026)." https://www.mordorintelligence.com/industry-reports/edge-computing-market-industry (accessed May 30, 2021).

[2]. Y. Liu, M. Peng, G. Shou, Y. Chen, and S. Chen, "Toward Edge Intelligence: Multiaccess Edge Computing for 5G and Internet of Things," *IEEE Internet Things J.*, vol. 7, no. 8, pp. 6722–6747, 2020, doi: 10.1109/JIOT.2020.3004500.

[3]. B. Ali, M. A. Gregory, and S. Li, "Multi-Access Edge Computing Architecture, Data Security and Privacy: A Review," *IEEE Access*, vol. 9, 2021, doi: 10.1109/ACCESS.2021.3053233.

[4]. P. Ranaweera, A. D. Jurcut, and M. Liyanage, "Realizing Multi-Access Edge Computing Feasibility: Security Perspective," *2019 IEEE Conf. Stand. Commun. Networking, CSCN 2019*, pp. 1–7, 2019, doi: 10.1109/CSCN.2019.8931357.

[5]. P. Zhang, C. Jiang, X. Pang, and Y. Qian, "STEC-IoT: A Security Tactic by Virtualizing Edge Computing on IoT," *IEEE Internet Things J.*, vol. 8, no. 4, pp. 2459–2467, 2020, doi: 10.1109/jiot.2020.3017742.

[6]. R. Zhu, L. Liu, H. Song, and M. Ma, "Multi-access edge computing enabled internet of things: advances and novel applications," *Neural Comput. Appl.*, vol. 32, no. 19, pp. 15313–15316, 2020, doi: 10.1007/s00521-020-05267-x.

[7]. J. Liu, G. Shou, Y. Liu, Y. Hu, and Z. Guo, "Performance Evaluation of Integrated Multi-Access Edge Computing and Fiber-Wireless Access Networks," *IEEE Access*, vol. 6, pp. 30269–30279, 2018, doi: 10.1109/ACCESS.2018.2833619.

[8]. V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures," *IEEE Access*, vol. 7, pp. 82721–82743, 2019, doi: 10.1109/ACCESS.2019.2924045.

[9]. G. Arfaoui *et al.*, "A Security Architecture for 5G Networks," *IEEE Access*, vol. 6, pp. 22466–22479, 2018, doi: 10.1109/ACCESS.2018.2827419.

[10]. W. Yu *et al.*, "A Survey on the Edge Computing for the Internet of Things," *IEEE Access*, vol. 6, no. c, pp. 6900–6919, 2017, doi: 10.1109/ACCESS.2017.2778504.

[11]. D. V. Medhane, A. K. Sangaiah, M. S. Hossain, G. Muhammad, and J. Wang, "Blockchain-Enabled Distributed Security Framework for Next-Generation IoT: An Edge Cloud and Software-Defined Network-Integrated Approach," *IEEE Internet Things J.*, vol. 7, no. 7, pp. 6143–6149, 2020, doi: 10.1109/JIOT.2020.2977196.

[12]. S. A. Bhat, I. B. Sofi, and C. Y. Chi, "Edge computing and its convergence with blockchain in 5g and beyond: Security, challenges, and opportunities," *IEEE Access*, vol. 8, pp. 205340–205373, 2020, doi: 10.1109/ACCESS.2020.3037108.

[13]. M. A. Rahman, M. M. Rashid, M. Shamim Hossain, E. Hassanain, M. F. Alhamid, and M. Guizani, "Blockchain and IoT-Based Cognitive Edge Framework for Sharing Economy Services in a Smart City," *IEEE Access*, vol. 7, pp. 18611–18621, 2019, doi: 10.1109/ACCESS.2019.2896065.

[14]. M. A. Rahman *et al.*, "Blockchain-Based Mobile Edge Computing Framework for Secure Therapy Applications," *IEEE Access*, vol. 6, pp. 72469–72478, 2018, doi: 10.1109/ACCESS.2018.2881246.

[15]. X. Wang, Y. Han, V. C. M. Leung, D. Niyato, X. Yan, and X. Chen, "Convergence of Edge Computing and Deep Learning: A Comprehensive Survey," *IEEE Commun. Surv. Tutorials*, vol. 22, no. 2, pp. 869–904, 2020, doi: 10.1109/COMST.2020.2970550.

[16]. R. Hassan, F. Qamar, M. K. Hasan, A. Hafizah, M. Aman, and A. S. Ahmed, "SS symmetry Internet of Things and Its Applications :," pp. 1–29, 2020.

[17]. P. Porambage, J. Okwuibe, M. Liyanage, M. Ylianttila, and T. Taleb, "Survey on Multi-Access Edge Computing for Internet of Things Realization," *IEEE Commun. Surv. Tutorials*, vol. 20, no. 4, pp. 2961–2991, 2018, doi: 10.1109/COMST.2018.2849509.

[18]. F. Javed, M. K. Afzal, M. Sharif, and B. S. Kim, "Internet of Things (IoT) operating systems support, networking technologies, applications, and challenges: A comparative review," *IEEE Commun. Surv. Tutorials*, vol. 20, no. 3, pp. 2062–2100, 2018, doi: 10.1109/COMST.2018.2817685.

[19]. K. Cao, Y. Liu, G. Meng, and Q. Sun, "An Overview on Edge Computing Research," *IEEE Access*, vol. 8, pp. 85714–85728, 2020, doi: 10.1109/ACCESS.2020.2991734.

[20]. A. Ksentini and P. A. Frangoudis, "On Extending ETSI MEC to Support LoRa for Efficient IoT Application Deployment at the Edge," *IEEE Commun. Stand. Mag.*, vol. 4, no. 2, pp. 57–63, 2020, doi: 10.1109/MCOMSTD.001.1900051.

[21]. S. Wang, X. Zhang, Y. Zhang, L. Wang, J. Yang, and W. Wang, "A Survey on Mobile Edge Networks: Convergence of Computing, Caching and Communications," *IEEE Access*, vol. 5, no. c, pp. 6757–6779, 2017, doi: 10.1109/ACCESS.2017.2685434.

[22]. B. K. Mohanta, D. Jena, U. Satapathy, and S. Patnaik, "Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology," *Internet of Things*, vol. 11, p. 100227, 2020, doi: 10.1016/j.iot.2020.100227.

[23]. S. Kumar, P. Tiwari, and M. Zymbler, "Internet of Things is a revolutionary approach for future technology enhancement: a review," *J. Big Data*, vol. 6, no. 1, 2019, doi: 10.1186/s40537-019-0268-2.

[24]. J. Pan and J. McElhannon, "Future Edge Cloud and Edge Computing for Internet of Things Applications," *IEEE Internet Things J.*, vol. 5, no. 1, pp. 439–449, 2018, doi: 10.1109/JIOT.2017.2767608.

[25]. F. John Dian, R. Vahidnia, and A. Rahmati, "Wearables and the Internet of Things (IoT), Applications, Opportunities, and Challenges: A Survey," *IEEE Access*, vol. 8, pp. 69200–69211, 2020, doi: 10.1109/ACCESS.2020.2986329.

[26]. H. Boyes, B. Hallaq, J. Cunningham, and T. Watson, "The industrial internet of things (IIoT): An analysis framework," *Comput. Ind.*, vol. 101, no. April, pp. 1–12, 2018, doi: 10.1016/j.compind.2018.04.015.

[27]. Y. Mao, C. You, J. Zhang, K. Huang, and K. B. Letaief, "A survey on mobile edge computing: The communication perspective," *arXiv*, vol. 19, no. 4, pp. 2322–2358, 2017.

[28]. Y. Keneshloo, T. Shi, N. Ramakrishnan, and C. K. Reddy, "Deep Reinforcement Learning for Sequence-to-Sequence Models," *IEEE Trans. Neural Networks Learn. Syst.*, vol. 31, no. 7, pp. 2469–2489, 2020, doi: 10.1109/TNNLS.2019.2929141.

[29]. Q. Mao, F. Hu, and Q. Hao, "Deep learning for intelligent wireless networks: A comprehensive survey," *IEEE Commun. Surv. Tutorials*, vol. 20, no. 4, pp. 2595–2621, 2018, doi: 10.1109/COMST.2018.2846401.

[30]. P. Mach and Z. Becvar, "Mobile Edge Computing: A Survey on Architecture and Computation Offloading," *IEEE Commun. Surv. Tutorials*, vol. 19, no. 3, pp. 1628–1656, 2017, doi: 10.1109/COMST.2017.2682318.

[31]. Y. Xiao, Y. Jia, C. Liu, X. Cheng, J. Yu, and W. Lv, "Edge Computing Security: State of the Art and Challenges," *Proc. IEEE*, vol. 107, no. 8, 2019, doi: 10.1109/JPROC.2019.2918437.

[32]. B. K. Mohanta, D. Jena, S. Ramasubbareddy, M. Daneshmand, and A. H. Gandomi, "Addressing Security and Privacy Issues of IoT Using Blockchain Technology," *IEEE Internet Things J.*, vol. 8, no. 2, pp. 881–888, 2021, doi: 10.1109/JIOT.2020.3008906.

[33]. Z. Xu, W. Liu, J. Huang, C. Yang, J. Lu, and H. Tan, "Artificial Intelligence for Securing IoT Services in Edge Computing: A Survey," *Secur. Commun. Networks*, vol. 2020, 2020, doi: 10.1155/2020/8872586.

[34]. F. Hussain, R. Hussain, S. A. Hassan, and E. Hossain, "Machine Learning in IoT Security: Current Solutions and Future Challenges," *IEEE Commun. Surv. Tutorials*, vol. 22, no. 3, pp. 1686–1721, 2020, doi: 10.1109/COMST.2020.2986444.

[35]. M. Bagaa, T. Taleb, J. B. Bernabe, and A. Skarmeta, "A Machine Learning Security Framework for Iot Systems," *IEEE Access*, vol. 8, pp. 114066–114077, 2020, doi: 10.1109/ACCESS.2020.2996214.

[36]. B. Rana, Y. Singh, and P. K. Singh, "A systematic survey on internet of things: Energy efficiency and interoperability perspective," *Trans. Emerg. Telecommun. Technol.*, no. October, pp. 1–41, 2020, doi: 10.1002/ett.4166.

[37]. H. Wu, H. Han, X. Wang, and S. Sun, "Research on Artificial Intelligence Enhancing Internet of Things Security: A Survey," *IEEE Access*, vol. 8, pp. 153826–153848, 2020, doi: 10.1109/ACCESS.2020.3018170.

[38]. B. A. Khalaf, S. A. Mostafa, A. Mustapha, M. A. Mohammed, and W. M. Abduallah, "Comprehensive review of artificial intelligence and statistical approaches in distributed denial of service attack and defense methods," *IEEE Access*, vol. 7, pp. 51691–51713, 2019, doi: 10.1109/ACCESS.2019.2908998.

[39]. S. Singh, A. S. M. Sanwar Hosen, and B. Yoon, "Blockchain Security Attacks, Challenges, and Solutions for the Future Distributed IoT Network," *IEEE Access*, vol. 9, pp. 13938–13959, 2021, doi: 10.1109/ACCESS.2021.3051602.

[40]. BitcoinCore, "Running A Full Node - Bitcoin," *2020*. [Online]. Available: https://bitcoin.org/en/full-node# minimum-requirements.

[41]. M. N. M. Bhutta *et al.*, "A Survey on Blockchain Technology: Evolution, Architecture and Security," *IEEE Access*, vol. 9, pp. 1–1, 2021, doi: 10.1109/access.2021.3072849.

[42]. "Master Node," *SpringerReference*. 2011, doi: 10.1007/springerreference_18544.

[43]. John Evans, "J. Evans. (Jan. 10, 2019). Blockchain Nodes: An in Depth Guide. Nodes.com. Accessed: Mar. 13, 2019. [Online]. Available: https: //nodes.com - Google Search." https://www.google.com/search?q=J.+Evans.+(Jan.+10%2C+2019).+Blockchain+Nodes%3A+An+in+Depth+Guide.+Nodes.com.+Accessed%3A+Mar.+13%2C+2019.+%5BOnline%5D.+Available%3A+https%3A+%2F%2Fnodes.com&rlz=1C1CHBF_enIN905IN909&oq=J.+Evans.+(Jan.+10%2C+2019).+Blockchain+Nodes%3A+An+in+Depth+Guide.+Nodes.com.+Accessed%3A+Mar.+13%2C+2019.+%5BOnline%5D.+Available%3A+https%3A+%2F%2Fnodes.com&aqs=chrome..69i57j69i59.1988j0j15&sourceid=chrome&ie=UTF-8 (accessed May 30, 2021).

[44]. K. Zhu, Z. Chen, W. Yan, and L. Zhang, "Security attacks in named data networking of things and a blockchain solution," *IEEE*

Internet Things J., vol. 6, no. 3, pp. 4733–4741, 2019, doi: 10.1109/JIOT.2018.2877647.

[45]. A. S. Musleh, G. Yao, and S. M. Muyeen, "Blockchain Applications in Smart Grid-Review and Frameworks," *IEEE Access*, vol. 7, pp. 86746–86757, 2019, doi: 10.1109/ACCESS.2019.2920682.

[46]. R. Beck, "Beyond Bitcoin: The Rise of Blockchain World," *Computer (Long. Beach. Calif).*, vol. 51, no. 2, pp. 54–58, 2018, doi: 10.1109/MC.2018.1451660.

[47]. J. Moubarak, E. Filiol, and M. Chamoun, "On blockchain security and relevant attacks," *2018 IEEE Middle East North Africa Commun. Conf. MENACOMM 2018*, pp. 1–6, 2018, doi: 10.1109/MENACOMM.2018.8371010.

[48]. M. N. Luke, S. J. Lee, Z. Pekarek, and A. Dimitrova, "Blockchain in Electricity: a Critical Review of Progress to Date," *NERA Econ. Consult. eurelectric*, p. 36, 2018, [Online]. Available: http://www.energie-nachrichten.info/file/01 Energie-Nachrichten News/2018-05/80503_Eurelectric_1_blockchain_eurelectric-h-DE808259.pdf.

[49]. K. Salah, M. H. U. Rehman, N. Nizamuddin, and A. Al-Fuqaha, "Blockchain for AI: Review and open research challenges," *IEEE Access*, vol. 7, pp. 10127–10149, 2019, doi: 10.1109/ACCESS.2018.2890507.

[50]. M. A. Ferrag, L. Shu, X. Yang, A. Derhab, and L. Maglaras, "Security and Privacy for Green IoT-Based Agriculture: Review, Blockchain Solutions, and Challenges," *IEEE Access*, vol. 8, pp. 32031–32053, 2020, doi: 10.1109/ACCESS.2020.2973178.

[51]. L. Chen, L. Xu, N. Shah, Z. Gao, Y. Lu, and W. Shi, "On security analysis of proof-of-elapsed-time (PoET)," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 10616 LNCS, no. May 2019, pp. 282–297, 2017, doi: 10.1007/978-3-319-69084-1_19.

[52]. H. Yusuf, I. Surjandari, and A. M. M. Rus, "Multiple channel with crash fault tolerant consensus blockchain network: A case study of vegetables supplier supply chain," *2019 16th Int. Conf. Serv. Syst. Serv. Manag. ICSSSM 2019*, pp. 1–4, 2019, doi: 10.1109/ICSSSM.2019.8887678.

[53]. "Hyperledger.pdf." .