JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

LEVERAGING THE PRINCIPALS OF BLOCKCHAIN FOR SECURE IoT BASED DEVICES.

[1]Amos K. Kibet, [2]Rosanna A. Esquivel, [3] James A. Esquivel

[1]Angeles University Foundation, [2]Angeles University Foundation, [3]Angeles University Foundation
[1]Graduate School,
[1]Angeles University Foundation, Angeles City, Pampanga, Philippines

Abstract: In this day and age, Internet use is growing, which has led to development of the Internet of Things (IoT), IoT facilitates the communication, computation and coordination of machines and objects. IoT is classified in two types, first is "inside of IoT" and second is "outside of IoT". Inside of IoT is considered as protocols. Outside IoT is consider as sensor, actuators and other physically components. In inside of IoT, there are protocol stack which have different layers example Application layer, Transport layer, Internet layer and Physical/Link layer. IoT's layers role is to ensure open and effective communication and transaction between two objects and use of different applications to build a continuous bond between them. One of the major concerns on today IoT is to enhance its security, when privacy of network's users is increased, the reliability of system increases correspondingly. IoT faces many security and privacy issues due to less computation power, heterogeneity, and limited resources available with its devices. Data is transferred among these devices with little or no human interaction. Data Confidentiality and Integrity are very critical parameters and can be achieved by securely sharing information in IoT scenarios. There is a need to mitigate these new threats and vulnerabilities and ensure Confidentiality, Integrity and availability. This paper is going to introduce blockchain of things with the aim of mitigating all possible vulnerabilities and threats associated in IoT Devices by increasing management of these IoT devices.

Index Terms **- IoT; Security; CIA; Cryptography; Blockchain, Hash, public key, private key; Things.**

I. INTRODUCTION

In today's integrated and connected world, most on-line activities deal in business networks supported cloud computing infrastructure for broad networking deployments. These networks are typically attached through dedicated interfaces, which are expandability and security to design, to provide the highest possible degree of flexibility, scalability, and all interconnected entities. Technologies have changed the way we live, particularly in our data driven society. This is partly due to advances in semiconductor and communication technologies, which allow a multitude of devices to be connected over a network, providing us with ways to connect and communicate between machines and people, e.g., machine-to-machine (Lee, 2018). Such a trend is also commonly referred to as the Internet-of-Everything, comprising the Internetof-Things (IoT), Internet-of-Medical-Things (IoMT), Internet-of-Battlefield-Things (IoBT), Internet-of-Vehicles (IoV), and so on. Given the occurrence of such devices in our society (e.g., in smart cities, smart grids and smart healthcare systems), Internet-of-things consists of sophisticated sensors, actuators and chips embedded in the physical things that are around us by making them smarter than ever. These things are connected together and exchange huge data between them and with other digital components without any human intervention.

The main concern of IoT is security and privacy. When modern new interesting applications and verticals such as the Internet-of-Things (IoT) get higher, it is essential to look back once more and try to address the security issue entirely in a radical way. Some researchers focused only on reviews on some of the challenges related to implementing security mechanisms in the IoT nodes and supporting networks. However, they did not mention all vulnerabilities according to the model layers of IoT eco-structure. In response to this problem, our study proposes to deeply investigate all of the vulnerabilities of all the layers and how blockchain and IoT gateway can secure these IoT devices. We also consider which IoT applications are best suited, at the practical level, to implement blockchain-based security mechanisms.

The summary of key contributions of this article is as follows:

1) Detailed literature review of non- Blockchain and Blockchain-based trust and security techniques for IoT.
2) An outline of the main contributions and limitations of these techniques is also provided.

3) Blockchain solutions to the current issues and challenges of making IoT systems secure and trusted.

4) Compare and contrast non-Blockchain and Blockchain-based security techniques to highlight the significance of Blockchain in ensuring IoT security and trust.

The rest of this paper is organized as follows: First part discusses more on related literature and the gaps; second part describes the vulnerabilities and additional security issues associated to the layers of IoT. Third part presents the basic elements of blockchain and the solutions. Finally, last part concludes the paper with recommendations.

II. Theoretical background

This section provides a brief introduction to IoT applications and architecture. Further, we will learn about security trust management in IoT and its parameters. Later in this section, we will explore Blockchain technology to understand its working principles.

2.1 IoT applications

IoT applications are huge in number and increasing day by day (See Fig. 1). From common consumers to large industries, IoT is making its positions strong among them. IoT smart and connected world includes, Smart Home, Smart Grids, Smart Health Care System and Smart Accessories, etc. are

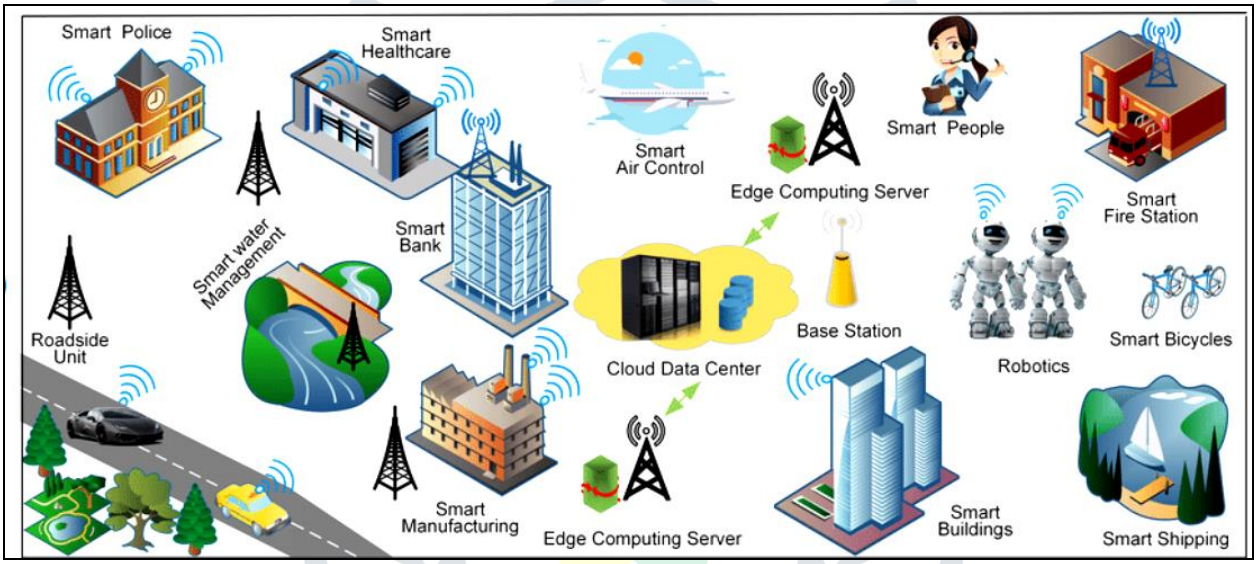

Figure 1: Application of IoT

IoT- based application include:

Smart Transportation: Vehicle tracking systems, smart toll systems, vehicle-to-vehicle communication systems (IoV) (Sharma and Kaushik, 2019), smart accident monitoring, smart parking systems, etc. are just a few of the solutions that the Internet of Things (IoT) may provide in the transportation sector. In terms of safety, management, efficiency, and effectiveness, smart transportation systems outperform conventional systems by a wide margin (Muthuramalingam et al., 2019).

Smart Power Grid: Combining a communication network with traditional electricity grids creates smart grids. In a power grid, the purpose of this communication network is to process and examine data gathered from transmission lines, substations, and consumers. When it comes to monitoring energy generation and consumption, transmission lines, electrical towers, and other relevant equipment, the sensing and real-time communication capabilities of IoT make a power grid smarter (Ghasempour, 2019).

Smart Appliances: Smart appliances are IoT-based services that interact directly with customers. Smart home appliances including smart fans, smart TVs, smart lights, smart refrigerators, smartwatches, glasses, and many more are steadily becoming a part of everyday life. Popular smart speech assistants include Siri, Alexa, and Google Assistant. Smart Cities and Homes: IoT enables smart infrastructure, such as smart lighting, smart parking, smart trash management, smart air quality management systems, damage indications, energy consumption monitoring, real-time fire alerts, etc., to make a city or a home smart (Alaa et al., 2017).

Smart Environment Monitoring Systems: Smart Environment Monitoring Systems: The Internet of Things (IoT) is widely utilized in environmental sensing and monitoring, such as temperature Real-time measurements of temperature, air quality, humidity, air pressure, soil quality, etc. Data is processed and analyzed in IoT-based systems before being transmitted to distant sites (Abraham et al., 2017).

Smart Safety Accessories: This IoT application offers clever methods for protecting various aspects of people's social and professional lives. Security and monitoring are provided through CCTV cameras, smart locks, smart biometric identification systems, position tracking, etc. for homes, roadways, and industries (Gnoni et al., 2020). Military IoT applications include human wearable biometric sensors, smart border surveillance systems, and surveillance robots.

Smart Healthcare System: This IoT application offers clever methods for protecting various aspects of people's social and professional lives. Security and monitoring are provided through CCTV cameras, smart locks, smart biometric identification systems, position tracking, etc. for homes, roadways, and industries (Gnoni et al., 2020). Military IoT applications include human wearable biometric sensors, smart border surveillance systems, and surveillance robots.

Smart Industries: IoT is used more in industries than in other disciplines. The Internet of Things (IoT) is enabling this industry with smart sensors, smart control systems, smart power management, statistical analysis, autonomous industrial big data robots for performing various jobs, etc (Boyes et al., 2018).

Smart Agriculture: By connecting them to the internet, IoT makes basic farming operations intelligent. IoT devices in smart farming collect information on water dam levels, meteorological conditions, and soil moisture. IoT in agriculture can simplify monitoring and increase crop quality and yield without sacrificing cost (Muangprathub et al., 2019).

2.2 OSI model and IoT

Usually, the internet networks adopt the Open Systems Interconnection (OSI) model, which is a standard ISO model for the internet. The OSI model architectures the internet into seven layers - physical, data link, network, transport, session, presentation and application - though the actual implementation of OSI model is done through TCP-IP model, which simplifies the seven-layer OSI model to four-layer internet protocol suite. In TCP-IP model (realistic implementation of OSI Model), the physical and data link layers are merged to form physical and network access layer and the session, presentation and application layers of OSI model are merged to a single application layer (Khachane, 2016).

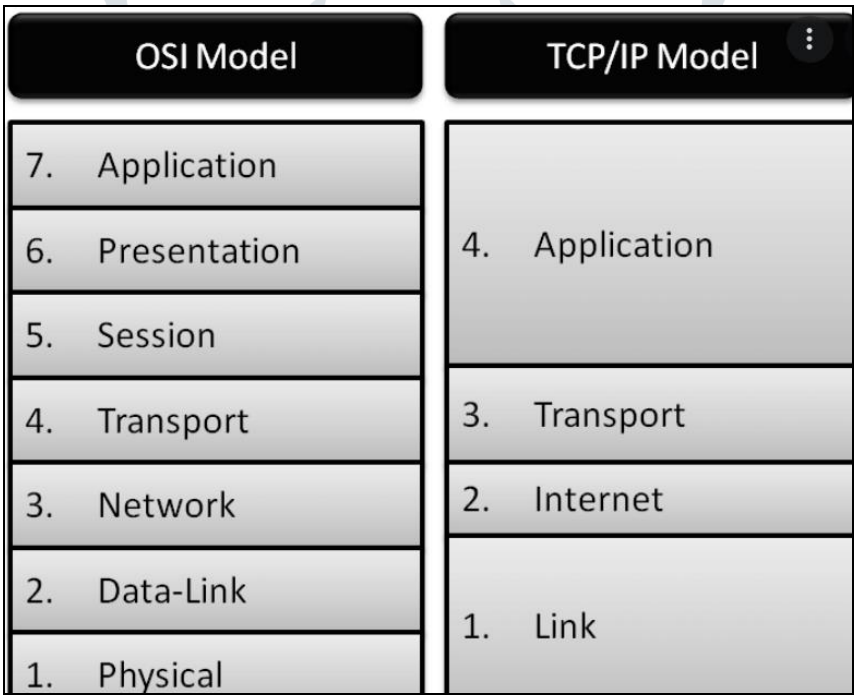

Figure 2: OSI and TCP/IP Model

The application layer (Layers 5, 6, and 7 in OSI) covers application-level messaging. HTTP/S is an example of an application layer protocol that is widely adopted across the internet. Although the TCP/IP and OSI models provide useful abstractions for discussing networking protocols, and the specific technologies that implement each protocol, in practice, some protocols do not fit neatly into these layered models. For example, the transport layer security (TLS) protocol that implements encryption to ensure privacy and data integrity of network traffic can be considered to operate across OSI layers 4, 5, and 6.

TCP/IP model	IoT protocols
Application	HTTPS, XMPP, CoAP, MQTT, AMQP
Transport	UDP, TCP
Internet	IPv6, 6LoWPAN, RPL
Network access & physical	IEEE 802.15.4 Wifi (802.11 a/b/g/n) Ethernet (802.3) GSM, CDMA, LTE

Figure 3: TCP/IP Model and IoT protocols

2.3 Architecture of IoT

Most of the researchers like (Khan et al., 2012) and (Jabraeil Jamali et al., 2020) defined a three-layered architecture of IoT. These layers are the Perception layer, Network layer, and Applica-tion layer (see Fig. 2).

Most of the researchers like (Khan et al., 2012) and (Jabraeil Jamali et al., 2020) defined a three-layered architecture of IoT. These layers are the Perception layer, Network layer, and Applica- tion layer (see Fig. 2).

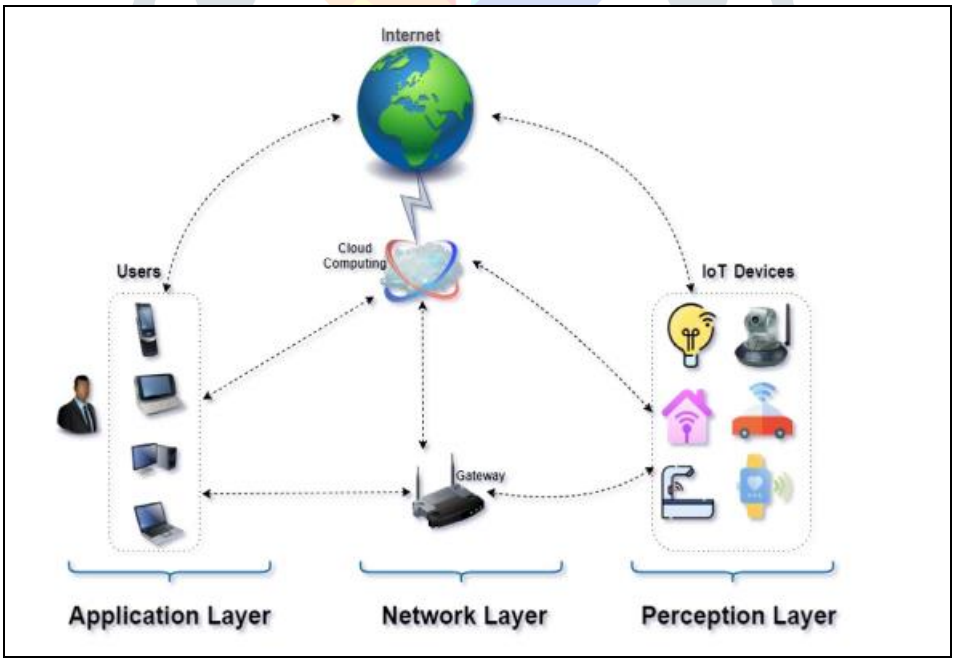

Figure 4: three-layered architecture of IoT

The perception layer is a component of physical or intelligent computing devices like sensors, RFID, bar codes, etc. that gather real data for processing. The acquired analog data from restricted devices is digitalized in this layer. Additionally, it recognizes changes in the sensing environment's physical conditions that take place in real-time. Some common attacks on this layer include eavesdropping, reply attacks, and timing assaults.

The second layer, known as ***the network layer***, is in charge of joining physical devices to other physical devices or the network. This layer transfers information obtained from physical devices, such as sensors and cameras, to the perception layer. Due to its

sensitivity and the difficulty in transferring genuine and temper-proof data at this layer, this layer has the highest risk of attacks. ZigBee (ZigBee, 0000), WiFi, Z-Wave (Z-Wave Mesh Network Protocol Specification, xxxx), 6LowPAN (Gomez et al., 2012), and other protocols are examples of those that work with this layer. At this layer, popular attacks include Man in the Middle, Storage, and Denial of Service (DoS).

The third and uppermost layer of the IoT is ***the application layer***. Users and IoT services are interfaced through this layer. The term "deployed IoT applications" is used here. This layer includes protocols like the Hyper Text Transfer Protocol (HTTP), the Constrained Application Protocol (CoAP) (RFC 7252, xxxx), the Mes-sage Queue Telemetry Transport (MQTT), and others. The gateway transmits data obtained from physical devices, such as sensors, cameras, etc., to the application layer. Data from the Perception layer can be delivered to users either directly through the gate or online.

2.4. Security aspects and trust management in IoT

Security is the number 1 issue for IoT developers, according to the 2017 IoT developer poll conducted by the Eclipse IoT Working Group. It is more challenging to handle security and trust in the IoT due to factors including heterogeneity, restricted resource availability, such as storage and computing power, location, and a huge scale of constrained devices. In the IoT environment, trust management is essential for addressing people's worries about their privacy and data integrity (Frustaci et al., 2018). In this section we will discuss some significant IoT security and trust issues.

a) Security Aspects:

Transforma Insights research estimates that by 2030, there will be 24.1 billion active Internet of Things devices. Some of these Internet of Things (IoT) devices, such as wired or wireless sensors, cameras, or other restricted devices, are placed in places where it is easy for unscrupulous means to access them. These gadgets could also be entirely replaced. For illustration, a sensor in It is simple to tamper with and create fake data in fields used to monitor temperature and humidity. This kind of bodily because all devices are connected to the IoT system, reaching certain devices leaves others open to attacks. This problem has an impact on both manufacturers and consumers. Manufacturers can address it by creating devices with a tight covering and secured interface. By placing devices in places that are difficult to reach or see, users can promote more confidence and security.

Cyber Attacks and Vulnerabilities in IoT:

General architecture of IoT has three layers that are susceptible to different vulnerabilities and attacks. ***Phishing*** attacks use fake emails and messages to obtain sensitive data from smart devices and users, including their individual identities, credit card information, etc. ***Malicious Code Injection*** Attack is applied when malicious code is injected into smart devices using an application layer to compromise them. In ***Sniffing*** Attack, attackers use sniffer applications to monitor and capture network traffic packets. ***Denial of Service*** Attack is accomplished by sending a large number of fake service requests to the server to make it unavailable to the actual users. In ***Man in Middle*** Attack, information from data packets is captured while it is being transferred over the network. ***Spoofing*** Attack is easy to launch where a node hides its original identity and claims as another legitimate node using a faked identity. ***Node Capturing*** Attack is used on physical devices of IoT by tampering nodes in terms of communication links, fake data input, etc. Using a botnet attack, a ***distributed denial of*** service (DDoS) attack is conducted. A bot-net is a collection of infected nodes connected to an IoT network that is under the control of hackers. ***Mirai*** Attack is launched by taking advantage of unsecured IoT devices. It scans IoT devices for any open Telnet port and then tries to log in using some common default passwords. ***Eavesdropping*** Attack is applied where data is transmitted over an unsecured network like in an RFID system.

b) Trust Management in IoT:

Trust Management is the process in which unwanted or malicious nodes are identified and removed from the communication process. Trust is probably the most important factor required for a successful communication system like IoT. Trust among nodes makes it easy to share information without the worry of the integrity of data. Over IoT systems, trust ensure privacy, integrity, reliability of users. The five important parameters in data trust are ***authentication, authorization/access control, Integrity, Inter-operability or Adaptability, and privacy***. These are security goals to make a secure and trusted IoT system.

Trust is very complicated to manage because this depends on many direct measurable and non-measurable factors. According to (Fortino et al., 2020) he defines types of trust. The first is **behavior trust**, which states that a device is trustworthy if it behaves as expected, even if this expected behavior is not fixed and changes over time. The second is **Reputation** in which the reputation of a node is expected behavior that is based on collective information from other nodes. This collective infor- mation can be based on nodes' observation or nodes' past behavior within a specific environment and time. The third one is **Honesty** which is an important factor in the trust evaluation.

A good model doesn't recommend assuming that nodes would be honest without evaluation. A recommender will be known as an honest node if information received from any node is the same as it was expected within a given environment and time. To develop a good model of trust management we need a smart technique to find out honest nodes. IoT networks can use a variety of trust management systems with a variety of algorithms and features depending on the situation. Because of the network's heterogeneity, creating a trust management system is not an easy task. Due to their restricted resources, nodes can either support this system or cannot. Trust management systems are susceptible to a wide range of assaults despite the existence of several security solutions and protocols. Trust-related attacks should also be researched in order to better comprehend trust-related

problems and obstacles. Despite numerous security solutions and protocols, trust management systems are vulnerable to a variety of attacks. To understand, trust-related issues and challenges more precisely, trust-related atacks should also be studied.

This will surely help in enhancing the security of the system. Some trust-related attacks (Djedjig et al., 2018) on IoT are listed here. ***Self-promotion attacks***: In these types of attacks, any malicious node manipulates a reputation of its own by suggesting good rec- ommendations for itself. It is usually performed with trust management systems with a positive feedback mechanism in calculating trust. Systems with weak integrity and authentication features are more vulnerable.

Selective behavior attack: In this type of attack, a malicious node behaves well from most of its neighbors' points of view, and behaves badly from the point of view of the rest of the nodes. In this way, the average recommendation value will remain positive, while it can damage some other nodes.

Sybil attack and newcomer attack: If there is a weak authentication and access control mechanism in an IoT system, any malicious node can create, emulate or impersonate different nodes in the network, and thus it can change the recommendation values and promote itself as a respected node. These attacks allow a malicious node to hide its bad reputation by creating a new identity.

III. REVIEW OF RELATED LITERATURE

This chapter presents the related literature and studies after the thorough and in-depth search done by the researchers in relation to IoT security.

These recent years, a loT of studies are leading to address the various security challenges closely related to IoT such as key management issues, confidentiality, integrity, privacy, policy enforcements among many other challenges (Minoli & Occhiogrosso, 2018). The team at Carnegie Mellon University was aware of the cross- device dependencies early, and proposed a set of new security policies for detecting anomaly behavior of interdependence. However, these policies will be more complicated and impractical with the increasing number of devices.

To discover and address the potential vulnerabilities for more kinds of IoT devices, researchers attempted to use static or dynamic analysis of the firmware and source running on these devices. (Zaddach et al. 2018) put forward a framework to support dynamic security analysis for a variety of embedded systems' firmware. It could not simulate all action of the real devices and need to forward action from the emulator to the device. Thus, it is unsuitable for largescale firmware analysis. (Chen et al. 2016 presented a framework for largescale automated firmware dynamic analysis, but it is only applicable to the Linuxbased system.

The full firmware dynamic analysis simulation framework for RealTime Operating System (RTOS) and bare-metal system is nearly blank. As the DDoS attack by IoT botnets increased, many researchers tried to mitigate IoT botnets related cyber risks by using the source code for the Mirai. Researchers have designed a tactic that could use the same compromise vector as the Mirai botnet to catalog vulnerable IoT devices, and detect potential poor security practices early. While there are still no effective and universal precautions for botnet virus, (Zhang et al. 2017) first considered the device and environment constraints of IoT network, then designed a lightweight algorithm to distinguish malicious requests from legitimate ones in an IoT network. But their assumption was too simple, hackers would not send requests with the same content, but usually simulate users' request with different reasonable content. Moreover, the current DDoS intrusion detection methods only apply in certain scenarios like smart grid (Sathish, 2018).

We must point out that IoT's challenges take a new dimension which is far from being easy to overcome with traditional solutions. In addition, we must emphasize that most security approaches rely to centralized architectures, making their applications in IoT much more complicated regarding the large number of objects. So, distributed approaches are required to deal with security issues in IoT. Other researchers have dealt with IoT security issues and reviewed solutions according to each security service. In contrast, the authors investigated confidentiality, access control, trust management and privacy solutions in IoT. On the other hand, (Ouaddah et al. 2017) reviewed access control solutions, while Stergiou et al. (2016) gave a classification of key management solutions in IoT. A survey of IoT and cloud computing with an emphasis on the security issues of different technologies was presented. The security and privacy requirements for the IoT applications such as personal and home, government and utilities, and enterprise and industry were analyzed by (Ouaddah et al. 2017) while (Alcaraz et al. 2013) and Ghaeini and Tippenhauer (2016) analyzed the security requirements of industrial sensor network-based remote substations in the context of IoT. In those researches, the authors focused particularly on classical based cryptographic approaches without discussing the new relevant techniques which could potentially bring huge values in terms of security and privacy when everything is interconnected. Intrusion detection in IoT is another important research field which has received a high interest of

researchers. Some surveys have discussed intrusion detection systems (IDS) in wireless sensor networks and Internet - of - Things and have provided analysis and comparison of the main existing IDSs (Butun et. al., 2014).

The main common line between the existing surveys is that most of them focus on cryptographic solutions which belong to centralized approaches. However, recently, many emergent technologies (ex. blockchains, SDN) are being adopted by industries as promising solutions to fix security and privacy issues in IoT that have not been addressed in all existing papers. Security subject is one of the hot research problems in IoT and has attracted a lot of researchers not only from academic and industry but also from standardization organizations. To date, there have been a lot of proposals aiming to address the security problems in IoT.

The use of Blockchain technology in the IoT domain to facilitate the sharing of services and resources and automate in a secure manner several time-consuming workflows is studied in (Kshetri, N. 2017). The authors concluded that the Blockchain-IoT combination is powerful and can pave the way for novel business models and distributed applications. Moreover, a related literature and work designed for Blockchain use in IoT was studied by (Christidis, K. and Devetsikiotis, M. 2016) and proposed a private Blockchain infrastructure for Smart homes. They focus on security issues with respect to confidentiality, integrity and availability, while simulation results indicate that the overheads imposed by the use of such technology remain at low levels. Additionally, (Conoscenti et. al. 2016) discusses the security enhancements with the use of Blockchain in IoT. The role of Blockchain is examined through four challenges, namely: costs and capacity constraints, architecture, unavailability of services and susceptibility to manipulation. They conclude that with the decentralized and consensus-driven structures of Blockchain, more secure IoT ecosystems can be provided as the network size increases. IT companies have also shown a great interest in applying Blockchain architectures in IoT ecosystems.

Targeting an economy of things, ADEPT focuses on Distributed Transaction Processing and Applications, Robust Security and Privacy by Design and Default. There are also other companies and startups that focus on transaction integrity, trust and security in the IoT domain. Almost all relevant research works utilize the Blockchain technology as a data storage management solution, taking advantage of the underlying infrastructure that provides decentralization, resilience, trust, security, scalability, autonomy and integrity. Most of the above-mentioned researches used Private Blockchain systems which use private network and confidential transactions; wherein IoT devices are communicating with each other daily, meaning they are public.

As discussed by (Paszu 2018), a denial-of-service attack (DOS) is any type of attack on a networking structure to disable a server from servicing its clients. Attacks range from sending millions of requests to a server in an attempt to slow it down, flooding a server with large packets of invalid data, to sending requests with an invalid or spoofed IP address. Denial-of-service attacks (DOS) is a constant danger to web sites. DOS has received increased attention as it can lead to a severe loss of revenue if a site is taken offline for a substantial amount of time. This work proposes use-case for the security of IoT smart devices with a token based access control and management model with the use of public and permission-less network (Ethereum Blockchain) that provides an access control mechanism realized within a Blockchain infrastructure.

IV. THE PROMISE OF BLOCKCHAIN

Due to the continuous development of crypto currencies, the potential of the blockchain has gradually been discovered and has gained considerable attention in recent years. The blockchain technology, which is also known as distributed secure ledger technology, is a time-series data block that is interconnected to form a chain structure embedded with cryptography and the distributed ledgers. Blockchain technology uses blockchain data structures to validate and store data; distributed consistent algorithms to generate and update data; encryption to ensure data transfer and access security; and automated scripting code to form a new distributed infrastructure and computing paradigm associated with smart contract (Swan, 2015).

The technological innovation of blockchain includes the concept of blockchain technology and also the structure of an ecological blockchain system (Nguyen, 2016). Blockchain is now not limited to tokens used in crypto- currencies but also has potential for IoT industry, governance, security and privacy, healthcare, cloud computing, big data and smart cities transportation system (Lu, 2017). Blockchain technology is not a single technical subject, but an integration of encryption, theoretical physics, communication networks and other techniques (Crosby, et al., 2016).

The blockchain architecture is divided into six layers which is shown in Fig. 1: the data layer, the network layer, the consensus layer, the contract layer, the service layer, and the application layer. The data layer and the network layer are considered as lower level that create, validate and store data. The upper level is at the top of the architecture, including the service and application platform (Zheng et al., 2017). The consensus and contract layers are the middleman between the lower and the upper level. The consensus layer consists mainly of Proof of Work (PoW), Proof of Stake (PoS), Delegated proof of Stake (DpoS) and Proof of Byzantine Fault Tolerance (PBFT). The contract layer involves an intelligent contract, a consensus directive and an incentive mechanism.

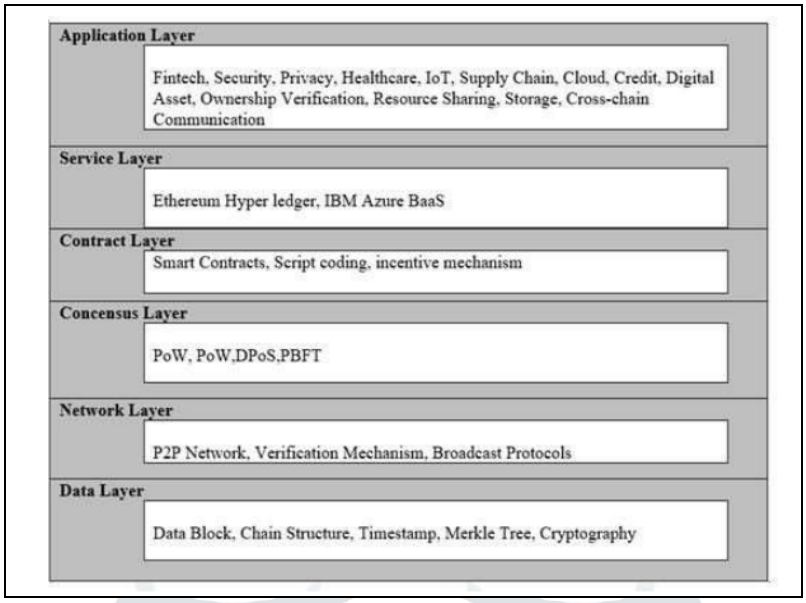

Figure 5: Blockchain structure

4.1 Principle and Types of Blockchain

Decentralization

Blockchain technology does not rely on involvement by third parties or hardware, nor does it have any central control. All blockchain regular users can partake in the authentication of their data. As discussed previously, blockchain technology forms a network through a P2P protocol. Unlike the centralized network, nodes in a P2P network have the same network power, and there is no centralized server (Crosby et al., 2016).

Openness and Transparency

Blockchain technology is an open source, data is open to everyone. Anyone can query blockchain data and develop applications through a common interface. Blockchain data resources and management belong to all nodes joining the blockchain system, while entities outside the blockchain system are blocked. As a distributed general ledger technology, all data records and operations within the system are transparent to all nodes in the network. The blockchain ensures high transparency of data information through a combination of asymmetric encryption and hash encryption. The procedures, rules, and access methods of the blockchain network are public (Zheng et al., 2017).

Independence

The blockchain is maintained by its own system node, and its data proof mechanism is implemented by the computer through a protocol without manual intervention (Dinh et al., 2017).

Unforgeable

Each node added to the blockchain is distributed to record blockchain data, which guarantees irreversible modification of the data. Once the data information is verified and added into the blockchain, it will not be tampered.

4.2. Applications of Blockchain and smart contract for trusted IoT

At present, Blockchain is gaining immense popularity due to its wide application domains. It is not just limited to cryptocurrencies like Bitcoin and Ethereum. Blockchain has proved that it has a vast number of applications for the IoT. The decentralized nature of Blockchain makes it possible to solve many security and trust-related issues in front of the proper functioning of the IoT. Particularly, Smart Contracts of Blockchain can provide many functions related to IoT like authentication and authorization of IoT devices, security of information flowing over IoT networks, maintaining agreement between different users of IoT, etc. Some important applications of Blockchain and Smart Contract for trusted IoT are as follows.

Blockchain for Internet of Vehicles (IoV): Blockchain has the potential to solve many trust and security issues associated with connected vehicles over the internet. A successful reliable system is required which can ensure basic trust and security parameters like identity management of vehicles, the integrity of reputation and communication channels, automation of the system, etc.

Blockchain for Industrial Internet of Things (IIoT): Integration of smart IoT devices into industries enables it in monitoring every

single activity with minimum human interactions. But to make more reliable IIoT in terms of privacy, transparency, trust, and access control to sensors data, we can integrate Blockchain with it (Rathee et al., 2021), (Latif et al., 2021).

Blockchain for Authentication and Access Control in IoT: Before transferring data, verification of valid data input and access control of data output is a more important task. Fortunately, Blockchain and smart contracts can also help in tackling this problem. Blockchain-based solutions(B et al., 2018) and (Yavari et al., 2020) can successfully perform authentication and access control over IoT networks.

Blockchain for Trusted Firmware Updates in IoT: As in IoT systems, each device is connected, there are strong possibilities of interruption in the updating process of devices, and code execution flow can be manipulated also. Moreover, the limited capabilities of IoT devices create obstacles in pushing out proper firmware updates. Scalability is another issue because it is not simply possible for thousands of end devices to update them manually. Most firmware update mechanisms use asymmetric cryptography systems which require complex and high processing power. As Blockchain is distributed in nature, it can solve the problem of the center point of failure (Pillai et al., 2019). Further, Blockchain uses smart contracts and consensus algorithms which ensure the integrity of software updates (Yohan and Lo, 2019).

4.3. Security vulnerabilities in Blockchain and smart contracts

This section highlights some important security vulnerabilities of Blockchain and Smart Contracts. Certainly, Blockchain and its ancillary technologies, such as Smart Contracts, offer a high level of security. But, as with every technology, Blockchain, and Smart Contracts have their own set of restrictions and vulnerabilities. There can be multiple vulnerabilities in the codes of smart contracts.

Our main focus is on Smart Contract security vulnerabilities, but we also discussed some Blockchain- related issues as well.

Majority Attack or 51% Attack: This attack is related to consensus-based Blockchains. During the process of Proof of Work, miners compete with all others to find a nonce value that is required to solve a given mathematical puzzle. Miner with the highest computation power wins the race and gets reward and broadcast mined block to others to update their local Blockchain. But, if anyhow, a miner gets more than 50% of total computation power, it could get control of the complete Blockchain. It can mod- ify transactions, control permissions, etc. This attack can lead to many other cryptocurrency-related attacks like Double Spending attacks, Self-Mining Attacks.

Eclipse Attack: This type of attack is implemented over the victim's incoming and outgoing connections to present a moderated view of Blockchain. This attack can be performed using some attacking techniques like botnet.

Border Gateway Protocol Attack: This attack is used to infect routing information over the Blockchain network. The main purpose of this attack is to create a delay of information propagating over the network. As a result, there is a knowledge gap among the other miners, and they fall behind in the mining process.

Re-entrancy in Smart Contracts: This is an important vulnerability that needs to be considered. In a Smart Contract, whenever a function has an external untrusted function call, there are strong chances of this attack. If this happens, an attacker needs only to exploit that external function which can steal some amount before completion of the initial function. The main example of this type of attack is DAO which stands for Decentralized Autonomous Organization.

Transaction Order Dependency in Smart Contracts: Miners usually choose a different sequence for transactions from the one in which they arrive. As a result, smart contracts which depend on the current state of storage variables faced a problem of transaction order. A transaction is picked based on the amount of Gas associated with it. So, a malicious transaction can be picked before a genuine one based on the amount of Gas.

Lack of Exception Handling in Solidity: Exception can occur at any time and lack of proper exception handling for some operations of smart contracts in a solidity programming language makes it vulnerable to some attacks. For example, a ''SEND" operation in Solidity doesn't have an exception handler if a failure occurred. It sends Boolean values only that may be sufficient for the sender. tx. origin Authorization: It is a type of phishing attack in which the identity of the initiator of a chain of transactions is spoofed. The tx. origin which used for managing the identity of transaction origin must be protected with extra care to prevent this type of attack.

Unknown Smart contract Call: Usually, transactions occurred when smart contracts call other smart contracts and it is also possible that addresses of caller and callee smart contracts are pro- vided by users. This creates an authentication vulnerability and a malicious user can authenticate a malicious smart contract.

Timestamp Dependency: Some applications required proper timing to proper functioning. But any miner with sufficient computation power can affect the output in his/her favor by manipulating time for few seconds. This type of vulnerability is severe in only some specific situations where a fraction of a second matters a lot.

V. METHODOLOGIES

IoT trust issues and their solution by Blockchain Current IoT challenges, such as heterogeneity, poor interoperability, low-powered constrained devices, a lack of a good update system, and so on, make it extremely difficult to perform trusted and

smooth operations on it. In this section, first, we highlight some major issues (See Figure below) that are being faced by trusted IoT, then we will try to find some possible solutions to these issues and challenges.

Summary of Blockchain Solutions of Security Issues and Challenges of IoT.

IoT Security Issues & Challenges	Blockchain Solutions
Authentication	Asymmetric Cryptography used in Blockchain in a distributed way and each entity in the Blockchain system has a Unique hash id, which is available openly to all the nodes. So it creates trust among the nodes in the network.
Identity Management	Distributed Ledger and Immutability of Blockchain can be used
Authorization/ Access Control	Smart contracts in Blockchain like Ethereum Blockchain
Integrity of Data	All the Blockchain nodes have the same data and can verify from using previous data.
Interoperability	Blockchain functions in a distributed and automated manner, so all dependency of interoperability is based on it
Privacy	Private Blockchain and Smart contracts can be used for privacy

Table 1: Security issues and challenges of IoT.

5.1 Trust in authentication

Authentication is not a new idea for identifying undisputed devices. It bounds each device with a unique digital identity with the help of cryptography. Symmetric-cryptosystem-based proto- cols, asymmetric-cryptosystem-based protocols, and hybrid proto-cols, these three types of Authentication protocols are defined (Ferrag et al., 2017). In IoT environments, mutual communication is required, so authentication is used on both sides to authenticate nodes.Multifactor authentication and lightweight authentication protocols are very necessary for IoT scenario because IoT is a com-plex network where different type of constrained devices works together. Almost all authentication protocols are based on public- key cryptography which is not much secure. Despite the availabil- ity of various authentication methods, a variety of protocols, and the limited resources of IoT devices make authentication extremely difficult. Some common authentication methods like X.509 certifi- cates, Hardware Security Module (HSM), Trusted Platform Module (TPM) and Symmetric Keys can be used. However, every method has its advantages, choosing the right kind of authentication mech- anism is very crucial for maintaining trusted communication among IoT devices. Potential Solution: By adding some required security features at the manufacturing level, we can deal with the limited resources of IoT. The use of authenticated servers is not possible always due tothe vast number of devices. To decide the best authentication model, we have to consider several factors like available hardware resources, connectivity, energy resources, and security require- ments. Devices with fewer security requirements and limited resources can use the Symmetric Key model because keys are hard- coded on devices. HSM can be used when we need to secure hardware-based storage of any device and it provides the safest form of storage. When we need to store keys in tamper-proof hard- ware using asymmetric authentication, we can use TPM. X.509 is the most secure model of digital identity which uses a chain of trust. When we require management of security, X.509 provides many vendor options. However, these models are not completely secure and can be bypassed or broken. Blockchain, on the other hand, can provide the ultimate solution because it is nearly impos- sible to forger information in it. Private Blockchain can be used as an isolated network of IoT which can protect it from the outside world. A protocol given in (Lau et al., 2018) named Authenticated Devices Configuration Protocol (ADCP) successfully implemented Blockchain for authentication in IoT

5.2. Trust in identity management

Identity in digital platforms works in the same manner as nor- mal paper-based identities. Different actors working on informa-tion systems must be identified. Particularly for systems such as IoT, where the number of devices and users is enormous, the requirement for a robust and trusted identity management system is growing. An identity management system must create verifiable identities because if it is not verifiable, it cannot be used for iden- tification whether it is authentic. Isolated, Federated and Central-ized are the three types of traditional identity management systems(Rathee and Singh, 2021) that are used for digital identity management. Identity Owner, Identity Issuer, and Identity Verifier are the three main actors in identity management systems. Although a digital identity can speed up processes and reduce the number of required actors, most traditional identity manage-ment systems like (Vossaert et al., 2013) store identity data on a centralized server, making it vulnerable to many security attacks.

5.3 Potential Solution: Blockchain security features can be used for building a secure and trusted identity management system. Block- chain can overcome many limitations from traditional identity management systems (Rathee and Singh, 2021). Blockchain- based identity management systems use a unique identifier called Decentralized identifiers or DID for the verification of digital identities (Liu et al., 2018). A DID must be non- reassignable, resolvable, cryptographically verifiable, decentral- ized, and independent providers. In a Blockchain-based system, the identity Issuer attaches DID to credentials and this DID is stored on Blockchain also. Here, Blockchain acts as an identity ver- ifier by providing the same information to everyone with actual data access restrictions. So, in a Blockchain-based system, valida- tion of a credential depends on the identity Verifier's assessment of the reliability of the identity Issuer. Some popular Blockchain- based identity management systems are uPort, Sovrin, and ShoCard. These protocols are open source and work in a fully automated manner (Haddouti, 2020).

5.4. Trust in integrity of data

Integrity of data ensures that data is modified by those who are authorized to do so. Vulnerabilities in IoT data integrity not only prevent it to operate correctly but also expose it as a compromised platform for attackers. To maintain data integrity, several crypto- graphic methods are used like Secure Hash Algorithm(SHA), Advanced Encryption Standards (AES), RSA, etc. which are based on some typical mathematical calculations. However, performing such heavy calculations may not be possible for resource- constrained IoT devices. Moreover, the IoT nodes are not always active and during this time, attackers can manipulate data. Authen- tication and read-write protections can be the solution but may not possible in all IoT scenarios. Operating system-level security which is known as multilevel security (MLS) and hardware-level security such as Trusted Platform Module (use cryptography) are also pos- sible. Still, these techniques cannot be widely used due to IoT sys- tems architectures (Musonda, 2019). Some protocols like (Aman et al., 2018) and (Bhattacharjee et al., 2018) are used to maintain integrity in IoT systems, however, these techniques were intended for specific attacks only. Potential Solution: The main features of Blockchain such as decentralization, distributed ledger, and immutability can be used for maintaining data integrity over IoT systems. Data over Block- chain is immutable because committed transactions cannot be updated or deleted. Limited resource availability of IoT devices can be overcome by integrating Blockchain partially or fully on cloud computing (Liu et al., 2017). Distributed ledger using private Blockchain can be integrated into IoT to ensure data integrity (Hang and Kim, 2019).

5.5 Trust in Authorization/Access control

The authorization mechanism controls the access to the ser- vices available in the IoT. It is very challenging to bind specific services to certain devices but it is very compulsory to maintain trust. In an IoT scenario data access, queries are executed in real-time, unlike traditional database management systems. Execution of queries and streaming of data occurs in IoT, so a strong mechanism of access control must be used. A scheme in which a single key is given to each user or node and other required keys are controlled by a given algorithm is described in (A hierarchical access control scheme for perceptual layer of IoT. It can reduce processing and storage costs because the number of required keys to be exchange is limited. Furthermore, mostly authorization or access control models use a mechanism in which decisions of access control are taken based on local data available on the device itself. Although decisions based on local data make authorization models flexible, it is very hard to trust these policies decided by devices. Authorization Server (AS) can be used for authorization in place of depending on local devices, but it does not provide much security and availability. OAuth 2.0, JSON Web Token, CBOR (Concise Binary Object Representation), Web Token (CWT), etc. are some famous and secure frameworks which use token passing mechanism for authorization. However, these frameworks require users to be online and use the internet for communication which is always an open surface for attackers. Potential Solution: Combining authorization frameworks like OAuth 2.0 with blockchain can solve most of the problems and provides many benefits. Immutability of records and decentralization nature of Blockchain makes trusted communication between the user and AS. For example, models proposed in (Siris et al., 2020) and (Siris et al., 2019) are the combination of OAuth 2.0and Block- chain and addressed mostly issues and challenges of authorization and access control. Using Blockchain abolish the requirement form user to be online which results in decreasing the surface attacks. Access control policies can become immutable and transparent due to distributed and smart contract mechanism nature of Block- chain. It can work as indisputable proof of the agreement between user and service provider in IoT because Blockchain uses an immu- table chain of hashes of records.

5.6 Trust in interoperability

Although interoperability is a great characteristic of IoT, it cre- ates security and trust challenges in front of the research community. Diversity in IoT demands interoperability to function it but this diversity and heterogeneous environment originate many security issues. This interoperability can have many different stances like heterogeneous devices, networks, platforms, and protocols. Most of the present solutions of interoperability are based on network devices like gateways. But these gateways have limited capabilities to provide a stable solution. Currently, to enable any new standard of interoperability, the involvement of vendors, developers, and service providers is a must. This involvement makes it very difficult to fasten the development in this direction. Another issue is with security solutions used by IoT devices. Most devices use third-party software which cannot be used with all other devices due to their limited capabilities. Potential Solution: An automated system is needed to resolve the issue of involvement of different entities in standardizing new frameworks and Blockchain can be a perfect solution. Blockchain functions in a distributed and automated manner, so all depen- dency of interoperability will be based on it. Models given in (Liu et al., 2020) proves that integration of Blockchain in IoT can solve many interoperability issues. Collaborative Proof of Work (Co-PoW), S2GHOST, and Tornadoare three models defined in this paper

5.7 Trust in privacy

Data privacy is one of the biggest challenges of any information system and IoT is not an exception. Any application area of IoT such that smart homes, smart healthcare systems, and smart vehicular systems, the privacy of information flowing over it needs to be pre- served. For instance, a patient enrolled in an IoT-based smart health care system may not want others to know about her medi- cal condition. Similarly, a vehicle linked to smart vehicular systems may wish to keep its current location private. It the

architecture of IoT that increases the privacy risk because after collecting data by IoT devices, it needs to be analyzed and pre-processed before transferring to end-users. In most cases, users don't know that how data is collected and who has access to it. Some researchers (Song et al., 2017) and (Luo et al., 2020) have proposed protocols for IoT environments using cryptography. Although these models use cryptography, they have some limitations in preserving privacy. Potential Solution: Blockchain can be a potential solution for pre- serving privacy in IoT using encryption of data. While public Block- chain allows anyone to access data, private Blockchain can be a great solution for limiting Blockchain network users. Additionally, the smart contract can be used for making policies for accessing data.

5.8 Integration of Blockchain and IoT

From the above section, it can be depicted that Blockchain can provide the ultimate solution to trust and many security-related problems. However, integrating Blockchain into the IoT system is not an easy task. Blockchain was originated for high-speed processing machines but IoT is out of the way of it. In this section, first, we will discuss some issues of integrating Blockchain and IoT and then, we will discuss issues of integrating Blockchain in IoT to make it trusted.

Integration of Blockchain into IoT systems can solve many security-related problems. Secure data transfer over IoT network is the main challenge and Blockchain has a great advantage over it. Applications of Blockchain in IoT systems are enough to moti- vate us to use these two emerging technologies together. But the biggest challenge in front of the organizations and developers is the difference between the working principle and architecture of these technologies. Therefore, before concerning integration strategies we should discuss issues or challenges that can arise while integrating Blockchain and IoT.

Size of Blockchain: There is a huge difference between the operational and static size of data among Blockchain and IoT systems. The size of Blockchain-based technologies like Bitcoin and Ethereum has cut across 250 GB and 1 TB already which is a huge size against IoT systems.

Required Processing Power: For providing high security such as immutability, strong authentication, etc., Blockchain uses PoW and Consensus algorithms. These algorithms require high process- ing power and energy. On the other hand, IoT devices use light- weight protocols and processes with low consumption of energy.

Security: Many researchers see the integration of Blockchain with IoT systems as a security solution for IoT. However, this integration generates a serious issue of reliability of data coming from IoT devices. Blockchain can guarantee the integrity of data process- ing through it but only if it does not receive malicious data from IoT devices

Speed of Transactions: One of the biggest problems of the inte- gration of Blockchain with IoT is its transaction speed. It is a universal truth that systems that are integrated with IoT are relatively slower than other ones. In an IoT system, devices can generate huge data in real-time which may not synchronize with the speed of Blockchain. The processing speed of many Blockchain-based systems such as Bitcoin, Ethereum, etc. is not more than 4–5 transactions per second as of now.

5.8.1. Blockchain and IoT integration strategies

Integration issues discussed above can be mitigated to some extent by applying some smart integration strategies. Therefore, better deployment approaches of the Blockchain layer in the IoT communication process must be considered carefully. These approaches can vary from application to application of IoT and decide where the communication process between Blockchain and IoT will take place (Reyna et al., 2018).

Cloud/Fog and Edge-Based IoT-Blockchain Model: The development of Cloud and Fog computing has solved many resource-constrained related problems of IoT devices. We can transfer the computation load such that hashing, encryption-decryption, etc. from IoT devices to Fog and Cloud systems. Therefore, the utility of Fog/Cloud computing grows in the context of Blockchain and IoT integration because Blockchain needs a high amount of processing power, energy, and other related resources for function- ing. In the hybrid model, (See Fig. 16) IoT devices can communicate directly to Blockchain or through Fog/Cloud nodes. In this way, we can take advantage of IoT-IoT and IoT-Blockchain models.

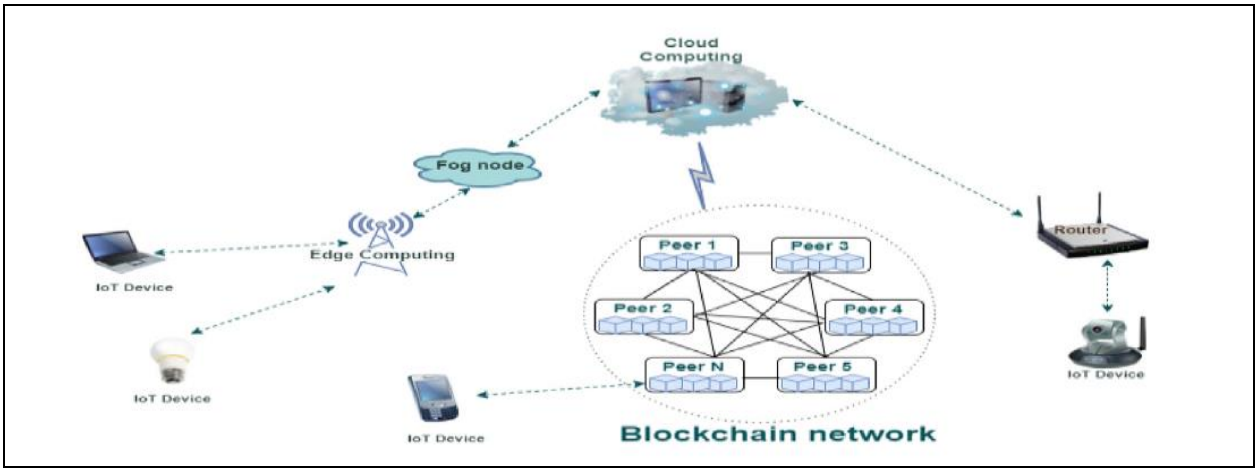

Figure 6 : Cloud/Fog and Edge-Based IoT-Blockchain Model

5.9. Comparative analysis of trust management techniques and discussion

A comparison of trust management techniques is shown in the table below. that do not use blockchain, it is fairly illustrative that most of the solutions don't handle enough trust parameters and trust-related threats utilizing the security and trust parameters. The methods employed in The model is unsafe since (Ben Saied et al.,2013) and (Mendoza and Kleinschmidt,2015) only addressed one trust parameter. Other approaches, such as the Attack-Resistant Trust Management Model, Asiri and Miri (2016), Mendoza and Kleinschmidt (2016), Wang et al. (2017), Kim and Keum (2017), Zandberg et al. (2019), and Zhang and Wu (2020), only addressed two or at most three of the five trust parameters, which is far below the current security objectives.

Trust Management Techniques without Blockchain.

Related Paper	Framework Type	Security Parameters					Attacks Addressed
		Authenti-cation	Access control	Adaptability	Integrity	Privacy	
(Chen et al., 2011)	Distributed	N	N	N	N	N	None
(Bao and Chen, 2012)	Distributed	N	N	N	N	N	None
(Ben Saied et al., 2013)	Distributed	N	Y	N	N	N	On-off, bad mounting, selective behavior
(Mendoza and Kleinschmidt, 2015)	Distributed	Y	N	N	N	N	On off attacks
(Attack-Resistant Trust Management Model)	Distributed	Y	Y	N	N	N	On-off, bad mounting, selective behavior, Sybil attack
(Asiri and Miri, 2016)	Decentralized	N	Y	Y	Y	N	NA
(Mendoza and Kleinschmidt, 2016)	Distributed	Y	N	N	Y	Y	Selective attack, on off attack
(Wang et al., 2017)	Distributed	Y	Y	Y	N	N	None
(Kim and Keum, 2017)	Centralized	Y	Y	N	N	N	Protect from IP based attacks
(Zandberg et al., 2019)	Centralized	Y	N	N	Y	Y	All types of related attacks
(El-Latif et al., 2020)	Centralized	Y	N	Y	Y	N	None
(Zhang and Wu, 2020)	Centralized	N	N	Y	Y	N	None

Table 2: Trust management without Blockchain.

This section provides a thorough comparison of trust management systems with and without Blockchain (See Table 3) based on five crucial trust and security factors, including authentication, access control, adaptability, integrity, and privacy as proof of work. According to our survey, the majority of Blockchain-based trust management approaches incorporate an authentication mechanism. Furthermore, access control, integrity, and privacy features are provided by Blockchain-based trust management approaches utilized in (Lahbib et al., 2019) to preserve security in IoT, although heterogeneity is still a problem with them. These solutions also handle significant security vulnerabilities including Bad mounting, ballot stuffing, and On-off. Techniques suggested in (Kataoka et al., 2018) and (Yang et al., 2018) don't provide scalability and privacy, making it challenging for them to be used in an IoT setting. While the models proposed in Pillai et al. (2019), Lahbib et al. (2019), Moinet et al. (2017), and Di Pietro et al. (2018) have good mechanisms for adaptability that make them flexible for the addition of new nodes and also support the heterogeneous environment of IoT, their lack of privacy makes them less reliable. Using Blockchain and quantum technology, the research articles (Abd El-Latif et al., 2021) and (Latif et al., 2021) addressed all aspects of security and trust. In conclusion, practically all security and trust aspects are addressed in order to ensure the security of sensor data in factories and other IoT applications. nonetheless, heterogeneity and privacy continue to be major issues.

Trust Management Techniques using Blockchain.

Related Paper	Framework Type	Security Parameters					Attacks Addressed
		Authenti-cation	Access control	Adaptability	Integrity	Privacy	
(Lahbib et al., 2019)	Decentralized	Y	Y	N	Y	Y	Bad mounting, ballot stuffing, on off
(Beck et al., 2016)	Decentralized	Y	Y	N	Y	Y	Most of the IoT related attacks
(Huang et al., 2018)	Decentralized	Y	Y	N	Y	Y	None
(Goleman et al., 2018)	Decentralized	N	Y	Y	Y	Y	None
(Malik et al., 2019)	Decentralized	Y	Y	N	Y	Y	None
(Pillai et al., 2019)	Centralized	Y	Y	Y	Y	N	None
(Khalid et al., 2020)	Decentralized	Y	Y	Y	Y	Y	All types of related attacks
(Mohanta et al., 2019a)	Decentralized	N	N	Y	Y	N	None
(Lahbib et al., 2019)	Decentralized	Y	Y	Y	Y	N	self -promoting, bad mounting,ballot stuffing
(Moinet et al., 2017)	Centralized	Y	Y	Y	Y	N	All related attacks
(Kataoka et al., 2018)	Decentralized	Y	Y	N	Y	N	DoS,replay, eavesdropping
(Yang et al., 2018)	Decentralized	Y	Y	N	Y	N	DoS
(Kouicem et al., 2018)	Decentralized	Y	Y	N	Y	Y	None
(Di Pietro et al., 2018)	Decentralized	Y	Y	Y	Y	N	Ballot Stuffing, DoS, Privilege escalation
(Dedeoglu et al., 2019)	Decentralized	N	N	Y	Y	N	Malicious Sensor and gateway related attacks
(Ali et al., 2019)	Decentralized	Y	Y	Y	Y	Y	Mirai attack
(Shala et al., 2020)	Decentralized	Y	N	N	Y	N	Bad mounting attack
(Putra et al., 2020)	Decentralized	Y	Y	N	Y	N	Bad Mounting, Sybil attack
(Kouicem et al., 2020)	Decentralized	Y	N	Y	Y	N	Bad-mouthing, Ballot-stuffing, Cooperative
(Rathee et al., 2021)	Decentralized	Y	Y	N	Y	N	Node Tempering, Data Transit Attack
(Abou-Nassar et al., 2020)	Decentralized	Y	Y	Y	Y	Y	None
(Abd El-Latif et al., 2021)	Decentralized	Y	Y	N	Y	Y	message attack,man in middle attack, impersonation attacks
(Latif et al., 2021)	Decentralized	Y	Y	N	Y	Y	51% Attack, Network Layer attack

Table 3: Trust management with Blockchain.

(El-Latif et al., 2020) can address a number of problems, but Blockchain can make them sufficiently more efficient. The majority of trust management strategies not based on the blockchain employ machine learning to gauge node trust. Although machine learning produces reliable findings, the information that is given online may be changed. Therefore, the primary issue with conventional trust management methods is that the security of trust information transmitted over a network using conventional protocols is insufficient. The graph below shows a performance comparison between traditional trust management methods and Blockchain-based trust management methods based on five security metrics of trust.

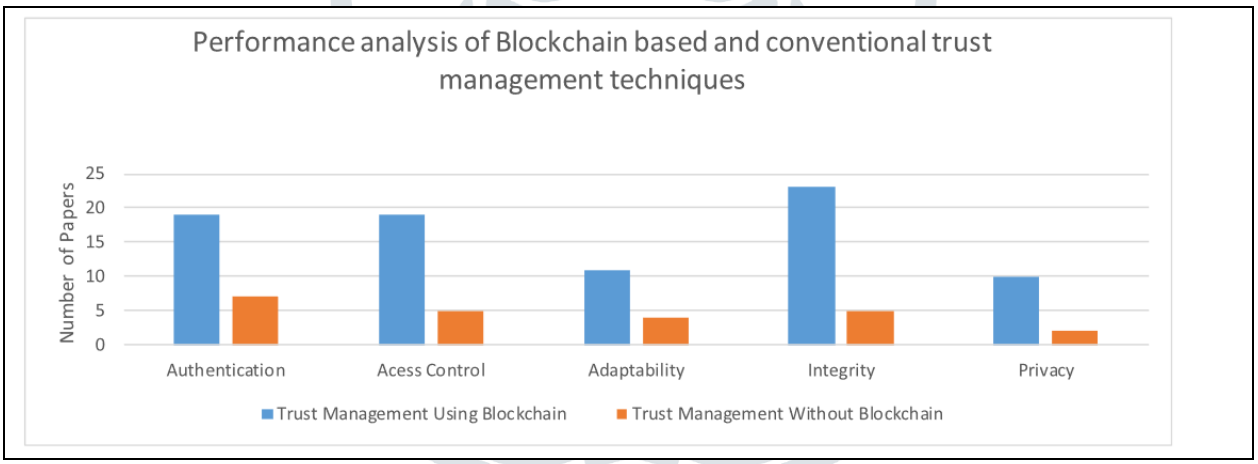

Figure 7: Performance analysis on both scenarios

The graph demonstrates how effectively blockchain-based trust management strategies perform in terms of the trust management evaluation criteria. Only a few conventional trust management techniques completely or effectively handle trust issues. Approximately 23 studies employed Blockchain-based trust management strategies out of the 35 techniques assessed, which effectively handled practically all trust criteria and broad threats but still lack flexibility. Only a few trust management techniques based on blockchain are flexible. The second problem with trust management strategies is privacy since the approaches and procedures they employ are insufficient to guarantee total privacy. In conclusion, Blockchain-based methods are far more secure than conventional ones.

5.10 Discussion: significance of blockchain in ensuring trust

It has been determined, after looking at a number of trust management approaches and models, that those models that use blockchain technology offer more security and protection against IoT vulnerabilities than those that do not. The security characteristics of blockchain offer great access control, tamper-proof rules, and transaction protection. Without Blockchain, trust management approaches cannot adequately secure the IoT. But when it comes to IoT network security, practically all Blockchain-based solutions perform outstandingly. Furthermore, by contrasting security and trust characteristics, we can clearly demonstrate the importance of Blockchain in managing trust. Without Blockchain, the majority of trust management approaches do not offer the ability of key security factors.

The security features of blockchain technology might be useful for managing trust. Blockchain uses distributed asymmetric cryptography to provide each node a distinct identity for safe authentication. The hash algorithms used in Blockchain, such as

SHA256, which is regarded as particularly powerful and generates a hash that is 32 bits long, maintain access control. It is quite difficult to break it. Blockchain allows for the addition of new blocks at any moment with the same specifications, making it adaptable to IoT. The Blockchain's smart contracts protect integrity and privacy.

Despite the potential advantages of blockchain technology, we learned from the review that its processing mechanism depends on challenging mathematical calculations like proof of work (PoW), proof of stake (PoS), and other techniques used by miners to validate legitimate transactions, making transactions slow and non-scalable. These consensus techniques may not work with IoT devices since they use a lot of memory and computing power. However, these problems may be resolved by using effective IoT and blockchain integration solutions. According to the results of our poll, maintaining confidence in the IoT may be done by calculating the reputation score or by securing the system to the point where everyone can transfer data without fear.

Traditional protocols calculated node reputations and trust ratings using a variety of methods, including machine learning and artificial intelligence. However, it might be difficult to transfer this calculated score securely. However, when it comes to the safe transfer of information, Blockchain-based systems offer a significant edge over conventional ones. We think that the security properties of Blockchain are almost enough to build a trustworthy IoT system. We might not require sophisticated trust management strategies in order to construct a trustworthy IoT system. As a consequence, by using Blockchain to make IoT systems sufficiently secure, the trust may be sustained without the need for trust management strategies.

VI. CHALLENGES

6.1. Blockchain and IoT integration issues

IoT system integration with blockchain technology can address a variety of security-related issues. The biggest issue with secure data transfer through IoT networks is that Blockchain has a significant edge over it. Applications of Blockchain in IoT systems alone are motivating enough for us to combine these two cutting-edge technologies. The mismatch between the functioning theory and architecture of these technologies, however, presents organizations and developers with their greatest problem. Therefore, before talking about integration techniques, we should talk about any problems or difficulties that may come up while merging Blockchain with IoT.

Size of Blockchain: The operational and static sizes of data across Blockchain and IoT systems varies significantly. In comparison to IoT systems, the size of blockchain-based technologies like Bitcoin and Ether-eum has already decreased to between 250 GB and 1 TB. For IoT devices, processing this data is almost difficult, which is a significant barrier to the integration of blockchain in IoT. Therefore, a comprehensive implementation of Blockchain in IoT systems is impractical due to its bulky size. By storing block data on the cloud and only storing partial and lightweight data, like hash chains, on IoT devices, cloud computing may be able to address the storage problem. However, it can create a conflict of the framework as cloud computing is a centrally con-trolled structure while Blockchain is distributed in nature.

Required Processing Power: For providing high security such as immutability, strong authentication, etc., Blockchain uses PoW and Consensus algorithms. These algorithms require high process- ing power and energy. On the other hand, IoT devices use light- weight protocols and processes with low consumption of energy. Protocols used by Blockchain and IoT systems are completely dif- ferent from each other based on required processing power and energy. So, making them compatible with each other is another arduous task.

Security: Many researchers see the integration of Blockchain with IoT systems as a security solution for IoT. However, this inte-gration generates a serious issue of reliability of data coming from IoT devices. Blockchain can guarantee the integrity of data process- ing through it but only if it does not receive malicious data from IoT devices. There can be so many reasons for corruption of data in IoT such as failure of devices, fake devices, hacked IoT networks, and devices, etc. There can be a problem of working together on security protocols followed by IoT and Blockchain. For example, IoT application layer protocols MQTT and CoAP use secure commu- nication protocols like TSL may not work well with Blockchain. So, we need to find a secure way of integrating Blockchain with IoT systems.

Anonymity of Users and their Privacy: Although Blockchain successfully addressed the privacy of data issue over its network, this may not be true always in the case of integration with IoT. We have discussed how full Blockchain block data and security cryptogra- phy protocols cannot be processed in IoT devices due to their lim- ited resources. So, the removal of this complexity invites attackers and forces us to compromise with security. Furthermore, every block in Blockchain shares the same information which is beneficial for the immutability of data but it creates user anonymity issues also.

Speed of Transactions: One of the biggest problems of the inte- gration of Blockchain with IoT is its transaction speed. It is a uni-versal truth that systems that are integrated with IoT are relatively slower than other ones. In an IoT system, devices can generate huge data in real-time which may not synchronize with the speed of Blockchain. The processing speed of many Blockchain-based systems such as Bitcoin, Ethereum, etc. is not more than 4–5 transactions per second as of now. Furthermore, Blockchain is not originated for holding and processing such data that can be produced by IoT. This gap in transaction speed can create a bottleneck for IoT transactions.

VII. CONCLUSION

7. Conclusion and future work

A trustworthy IoT system must maintain data integrity and privacy, have strong user authentication and permission, and be adaptable to varied environments. This study offered a thorough analysis of current trust management studies that employ traditional and Blockchain-based tech- niques in order to provide useful insight on the relevance of Blockchain to achieve these aims. After that, we discussed some of the key problems and difficulties associated with a safe and reliable IoT and made an effort to use Blockchain to overcome these problems. We also identified several approaches and problems for integrating blockchain with IoT. Finally, we compared and evaluated five crucial factors for maintaining IoT trust, including authentication, access control, adaptability, integrity, and privacy.

As a result, it is evident that Blockchain technology can solve most trust factors and has a number of benefits over traditional security techniques in assuring IoT trust. Additionally, Blockchain not only increases the security of IoT systems but also lessens the vulnerability of the network to threats. Blockchain may be utilized as a service for information exchange and resource allocation among devices. Blockchain and IoT together have great potential. With the help of modern technology, several of blockchain's shortcomings, such a low transaction rate and a lack of flexibility, may be overcome. These difficulties may be the subject of future investigation. Emerging IoT and blockchain-based technologies like Holochain and Hashgraph can be combined to overcome these restrictions.

Even though this study came to the conclusion that current Blockchain and IoT integration solutions can all but eliminate the bulk of security and trust issues, effective IoT and Blockchain integration still poses difficulties. As a consequence, in-depth investigation may be done to create efficient IoT and Blockchain integration solutions.

REFERENCES

[1]. Lee, J. (2018). A blockchain future for internet-of-things security

[2]. Sharma, S., Kaushik, B., 2019. A survey on internet of vehicles: Applications, security issues & solutions. Veh. Commun. 20

[3]. Muthuramalingam, S., Bharathi, A., Rakesh kumar, S., Gayathri, N., Sathiyaraj, R., Balamurugan, B., 2019. Iot based intelligent transportation system (iot-its) for global perspective: a case study. Intell. Syst. Ref. Libr. 154, 279–300

[4]. Ghasempour, Alireza, 2019. Internet of things in smart grid: Architecture, applications, services, key technologies, and challenges. Inventions 4 (1), 22.

[5]. Alaa, M., Zaidan, A.A., Zaidan, B.B., Talal, M., Kiah, M.L.M., 2017. A review of smart home applications based on Internet of Things.

[6]. Abraham, S., Beard, J., Manijacob, R., 2017. Remote environmental monitoring using Internet of Things (IoT). GHTC 2017 - IEEE Glob. Humanit. Technol. Conf. Proc. 2017-Janua, 1–6.

[7]. Gnoni, M.G., Bragatto, P.A., Milazzo, M.F., Setola, R., 2020. Integrating IoT technologies for an ‘‘intelligent” safety management in the process industry, in: Procedia Manufacturing. Elsevier B.V., pp. 511–515

[8]. Boyes, H., Hallaq, B., Cunningham, J., Watson, T., 2018. The industrial internet of things (IIoT): An analysis framework. Comput. Ind. 101, 1–12

[9]. Muangprathub, J., Boonnam, N., Kajornkasirat, S., Lekbangpong, N., Wanichsombat, A., Nillaor, P., 2018. IoT and agriculture data analysis for smart farm.

[10]. Khachane, P. (2016). IOT-Architecture-Standards-Protocols

[11]. Khan, R., Khan, S.U., Zaheer, R., Khan, S., 2012. Future internet: The internet of things architecture, possible applications and key challenges, in: Proceedings - 10th International Conference on Frontiers of Information Technology, FIT 2012.

[12]. Jabraeil Jamali, M.A., Bahrami, B., Heidari, A., Allahverdizadeh, P., Norouzi, F., 2020.IoT Architecture. pp. 9–31. Jesus, Emanuel Ferreira, Chicarino, Vanessa R.L., de Albuquerque, Célio V.N., Rocha, Antônio A. de A., 2018. A Survey of How to Use Blockchain to Secure Internet of Things and the Stalker Attack. Secur. Commun. Networks 2018, 1–27.

[13]. Frustaci, Mario, Pace, Pasquale, Aloi, Gianluca, Fortino, Giancarlo, 2018. Evaluating critical security issues of the IoT world: Present and future challenges. IEEE Internet Things J. 5 (4), 2483–2495.

[14]. Fortino, Giancarlo, Fotia, Lidia, Messina, Fabrizio, Rosaci, Domenico, Sarne, Giuseppe M.L., 2020. Trust and Reputation in the Internet of Things: State-of-the-Art and Research Challenges. IEEE Access 8, 60117–60125.

[15]. Djedjig, N., Tandjaoui, D., Romdhani, I., Medjek, F., 2018. Trust management in the internet of things, in: Security and Privacy in Smart Sensor Networks. IGI Global, pp. 122–146.

[16]. Minoli, D., & Occhiogrosso, B. (2018). Blockchain mechanisms for IoT security.

[17]. Zaddach, J. et al. (2018). AVATAR: A framework to support dynamic security analysis of embedded systems' firmwares. NDSS. Chen et al. (2016)

[18]. Zhang et al. 2017. A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications

[19]. Sathish A.P. Kumar, (2016). Security in internet of things: Challenges, solutions and future directions

[20]. Ouaddah, H., Mousannif, A.A., Elkalam, & Ouahman, A.A. (2017). Access control in the Internet of things: big challenges and new opportunities. Jan.

[21]. Alcaraz, C., Roman, R., Najera, P., & Lopez, J. (2013). Security of industrial sensor network-based remote substations in the context of the Internet of things. Ad Hoc Networks, vol. 11. Butun et. al., 2014

[22]. Kshetri, N. (2017). Can blockchain strengthen the internet of things? In Prof. 19(4), 68–72).

[23]. Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the Internet of Things. IEEE Access 4, 2292–2303

[24]. Conoscenti, M., Vetró, A., & Martin, J.C.D. (2016). Blockchain for the Internet of Things: a systematic literature review. In: 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), pp. 1–6.

[25]. Paszu, S. (2018). Hyperledger vs Ethereum: a comparison

[26]. Swan, M. (2015). Blockchain: Blueprint for a new economy. O'Reilly Media, Inc.

[27]. Nguyen, QK (2016). Blockchain-A ̄nancial technology for future sustainable development. In Green Technology and Sustainable Development (GTSD), Int. Conf., pp. 51–54, IEEE

[28]. Lu, Y (2017). Industry 4.0: A survey on technologies, applications and open research issues. Journal of Industrial Information Integration, 6, 1

[29]. Crosby, M, P Pattanayak, S Verma and V Kalyanaraman (2016). Blockchain technology: Beyond bitcoin. Applied Innovation, 2,

[30]. Zheng, Z, S Xie, H Dai, X Chen and H Wang (2017). An overview of blockchain technology: Architecture, consensus, and future trends. In Big Data (BigData Congress), 2017 IEEE Int. Congress, pp. 557–564, IEEE

[31]. Dinh, T., Wang, J., Chen, G., Liu, R., Ooi, B.C. &Tan, K.L.. (2017). Blockbench: A framework for analyzing private blockchains. In Proc. 2017 ACM Int. Conf. Management of Data, pp. 1085–1100, ACM

[32]. Rathee, Geetanjali, Balasaraswathi, M., Chandran, K. Prabhu, Gupta, Sharmi Dev, Boopathi, C.S., 2021. A secure IoT sensors communication in industry 4.0 using blockchain technology. J. Ambient Intell. Humaniz. Comput. 12 (1), 533–545.

[33]. Latif, Shahid, Idrees, Zeba, Ahmad, Jawad, Zheng, Lirong, Zou, Zhuo, 2021. A blockchain-based architecture for secure and trustworthy operations in the industrial Internet of Things. J. Ind. Inf. Integr. 21, 100190.

[34]. B, A.Z.O., B, B.B., B, K.S., 2018. Using Blockchain for IOT Access Control. Springer International Publishing.

[35]. Yavari, Mostafa, Safkhani, Masoumeh, Kumari, Saru, Kumar, Sachin, Chen, Chien- Ming, He, Debiao, 2020. An Improved Blockchain-Based Authentication Protocol for IoT Network Management. Secur. Commun. Networks 2020, 1–16

[36]. Pillai, A., Sindhu, M., Lakshmy, K. V., 2019. Securing Firmware in Internet of Things using Blockchain, in: 2019 5th International Conference on Advanced Computing and Communication Systems, ICACCS 2019. pp. 329–334.

[37]. Yohan, A., Lo, N.W., 2019. An Over-The-Blockchain Firmware Update Framework for IoT Devices. DSC 2018–2018 IEEE Conf. Dependable Secur. Comput. 1–8

[38]. Ferrag, M.A., Maglaras, L.A., Janicke, H., Jiang, J., Shu, L., 2017. Authentication Protocols for Internet of Things: A Comprehensive Survey. Secur. Commun. Networks

[39]. Vossaert, J., Lapon, J., De Decker, B., Naessens, V., 2013. User-centric identity management using trusted modules. Math. Comput. Model. 57 (7-8), 1592– 1605.

[40]. Liu, Y., Zhao, Z., Guo, G., Wang, X., Tan, Z., Wang, S., 2018. An identity management system based on blockchain. Proc. - 2017 15th Annu. Conf. Privacy. Secur. Trust.PST 2017, 44–53

[41]. Haddouti, S. El, 2020. 3rd International Conference on Advanced Communication Technologies and Networking, CommNet 2020. 3rd Int. Conf. Adv. Commun. Technol. Networking, CommNet 2020 1–7

[42]. Musonda, C., 2019. Security, Privacy and Integrity in Internet Of Things - A Review. ICTSZ Int. Conf. ICTs Lusak, Zambia (12th -13th December 2018 146–152. Muthuramalingam, S., Bharathi, A., Rakesh kumar, S., Gayathri, N., Sathiyaraj, R., Balamurugan, B., 2019. Iot based intelligent transportation system (iot-its) for global perspective: a case study. Intell. Syst. Ref. Libr. 154, 279–300

[43]. Aman, M.N., Sikdar, B., Chua, K.C., Ali, A., 2018. Low Power Data Integrity in IoT Systems 4662.

[44]. Bhattacharjee, S., Salimitari, M., Chatterjee, M., Kwiat, K., Kamhoua, C., 2018. Preserving Data Integrity in IoT Networks Under Opportunistic Data Manipulation. Proc. - 2017 IEEE 15th Int. Conf. Dependable, Auton. Secur. Comput. 2017 IEEE 15th Int. Conf. Pervasive Intell. Comput. 2017 IEEE 3rd Int. Conf. Big Data Intell. Compu 2018-Janua, 446–453.

[45]. Liu, B., Yu, X.L., Chen, S., Xu, X., Zhu, L., 2017. Blockchain Based Data Integrity Service Framework for IoT Data. Proc. - 2017 IEEE 24th Int. Conf. Web Serv. ICWS 2017,468–475

[46]. Hang, L., Kim, D.H., 2019. Design and implementation of an integrated iot blockchain platform for sensing data integrity. Sensors (Switzerland) 19,2228

[47]. Siris, V.A., Dimopoulos, D., Fotiou, N., Voulgaris, S., Polyzos, G.C., 2020. Decentralized authorization in constrained IoT environments exploiting interledger mechanisms. Comput. Commun. 152, 243–251.

[48]. Siris, V.A., Dimopoulos, D., Fotiou, N., Voulgaris, S., Polyzos, G.C., 2019. OAuth 2.0 meets blockchain for authorization in constrained IoT environments. ArXiv 364–367.

[49]. Liu, Yinqiu, Wang, Kun, Qian, Kai, Du, Miao, Guo, Song, 2020. Tornado: Enabling Blockchain in Heterogeneous Internet of Things Through a Space-Structured Approach. IEEE Internet Things J. 7 (2), 1273–1286

[50]. Song, Tianyi, Li, Ruinian, Mei, Bo, Yu, Jiguo, Xing, Xiaoshuang, Cheng, Xiuzhen, 2017. A Privacy Preserving Communication Protocol for IoT Applications in Smart Homes. IEEE Internet Things J. 4 (6), 1844–1852.

[51]. Luo, Xi, Yin, Lihua, Li, Chao, Wang, Chonghua, Fang, Fuyang, Zhu, Chunsheng, Tian, Zhihong, 2020. A lightweight privacy-preserving communication protocol for heterogeneous IoT environment. IEEE Access 8, 67192–67204.

[52]. Reyna, A., Martín, C., Chen, J., Soler, E., Díaz, M., 2018. On blockchain and its integration with IoT. Challenges and opportunities. Futur. Gener. Comput. Syst. 88, 173–190.

[53]. Ben Saied, Y., Olivereau, A., Zeghlache, D., Laurent, M., 2013. Trust management system design for the Internet of Things: A context-aware and multi-service approach. Comput. Secur. 39, 351–365.

[54]. Mendoza, Carolina V.L., Kleinschmidt, João H., 2015. Mitigating on-off attacks in the internet of things using a distributed trust management scheme. Int. J. Distrib. Sens. Networks 11 (11), 859731

[55]. Asiri, S., Miri, A., 2016. An IoT trust and reputation model based on recommender systems. 2016 14th Annu. Conf. Privacy. Secur. Trust. PST 2016, 561–568.

[56]. Mendoza and Kleinschmidt, 2016), (Wang et al., 2017), (Kim and Keum, 2017) and (Zandberg et al., 2019) and (Zhang and Wu, 2020

[57]. Lahbib, A., Toumi, K., Laouiti, A., Laube, A., Martin, S., 2019. Blockchain based trust management mechanism for IoT. IEEE Wirel. Commun. Netw. Conf. WCNC 2019-April, 1–8.

[58]. Ali, J., Ali, T., Alsaawy, Y., Khalid, A.S., Musa, S., 2019. Blockchain-based smart-IoT trust zone measurement architecture. ACM Int. Conf. Proceeding Ser. Part F1481, 152–157

[59]. Kataoka, K., Gangwar, S., Podili, P., 2018. Trust list: Internet-wide and distributed IoT traffic management using blockchain and SDN. IEEE World Forum Internet Things, WF-IoT 2018 - Proc. 2018-Janua, 296–301

[60]. Pillai, A., Sindhu, M., Lakshmy, K. V., 2019. Securing Firmware in Internet of Things using Blockchain, in: 2019 5th International Conference on Advanced Computing and Communication Systems, ICACCS 2019. pp. 329–334.

[61]. Abd El-Latif, A.A., Abd-El-Atty, B., Mehmood, I., Muhammad, K., Venegas-Andraca, S. E., Peng, J., 2021. Quantum-Inspired Blockchain-Based Cybersecurity: Securing Smart Edge Utilities in IoT-Based Smart Cities. Inf. Process. Manag. 58 (4), 102549.

[62]. El-Latif, Ahmed A. Abd, Abd-El-Atty, Bassem, Venegas-Andraca, Salvador E., Elwahsh, Haitham, Piran, Md. Jalil, Bashir, Ali Kashif, Song, Oh-Young,Mazurczyk, Wojciech, 2020. Providing End-to-End Security Using Quantum Walks in IoT Networks. IEEE Access 8, 92687–92696