Design of a Cloud-Blockchain-based Secure Internet of Things Architecture

Deepti Rani, Nasib Singh Gill, Preeti Gulia
Department of Computer Science and Applications
Maharshi Dayanand University
Rohtak, Haryana
India

***Abstract*—The growing number of Internet of Things (IoT) objects and the operational and security challenges in IoT systems are encouraging researchers to design suitable IoT architecture. Enormous data generated in the IoT environment face several kinds of security and privacy challenges. IoT system generally suffers from several issues like data storage, safety, privacy, integrity, transparency, trust, and single point of failure. IoT environment is emerging with several solutions to resolve these problems. The main objective of this paper is to design a cloud-blockchain-based secure IoT architecture that provides advanced and efficient storage and security solutions to IoT ecosystem. Blockchain technology appears to be a decent choice to resolve such kinds of problems. Blockchain technology uses a hash-based cryptographic technique for information security and integrity. Cloud computing provides advanced storage solutions with several remote services to store, compute and analyze the data. The proposed IoT architecture is based on the integration of cloud and blockchain services, which aim to provide transparent, decentralized, and trustworthy and secure storage solutions. In addition to the standard layers (perception layer, network layer, processing layer, and application layer) the proposed IoT architecture in the present paper includes a service layer, a security layer, and a parallel management and control layer, which focus on the security and management of the entire IoT infrastructure.**

Keywords*—Internet of things; cloud computing; blockchain; iot architecture; security and services

I. Introduction

Data or information security in Internet of Things (IoT) environment is a significant challenge that is getting complicated due to the exponential expansion of IoT devices, applications, and services. In the last few decades, the idea of IoT has widely extended in human life. It brings more ease, upgrades work efficiency, and promotes the growth of national economy of a country. IoT is one of the most promising technologies of the current century which has largely inter-connected the universal things (devices) using various Internet services. The interconnected IoT devices produce a large amount of data that need to be collected, aggregated, stored, and processed privately and securely [1]. But at the same time, IoT technology brings massive security risks for its data and network system.

Security and privacy are the primary requirements for the successful integration of IoT in the society. Due to the absence of proper security, the growing and extensive IoT technology is exposed to various kinds of security and privacy issues [2]. Valuable data in its original form can be captured illegally by cybercriminals from storage (cloud or media) or while communicating over the network. An advanced security system is needed to secure large amount of data generated in IoT system. Data encryption is a worthy approach that provides secure data preservation and data transmission. Blockchain technology is an innovative approach using which data can be securely preserved and transmitted on a decentralized network. Data stored in blockchain is encrypted using secure hash functions (SHA-256 and Keccak-256) that is almost impossible to tamper with [3]. Data can’t be updated or deleted by third party due to immutability and integrity properties of blockchain technology. Data generated by various IoT devices can be stored and processed in network edge (device storage) or remote server itself. However, restricted capacity of IoT objects in terms of storage, computational power, and energy is a also significant challenge. Cloud computing provides scalability, management, simplicity, computation, storage and processing facilities to IoT infrastructure [4].

IoT is a large-scale information system that is generally designed using three logical layers which are the perception (sensing) layer, network layer, and application layer. Several researchers have designed many IoT architectures using these three layers for providing solutions to their respective targeted problems such as security and data processing. The present paper proposes an advanced IoT architecture that promotes the solutions for data storage, security, and management problems in IoT based smart environment.

Cloud computing provides centralized storage solutions to IoT infrastructure. It provides features like good scalability, robustness, elasticity, less cost, and power consumption that improves the performance and efficiency of IoT system. Blockchain, as discussed earlier is an innovative distributed technology that provides immutability, integrity, and security to manipulated data. Combining the blockchain technology with cloud infrastructure facilitates with more promising solutions to IoT environment [5]. Initially, the blockchain technology was designed for the security of the public digital ledger of Bitcoin cryptocurrency used for economic transactions only [6]. The Blockchain hypothesis is based on peer-to-peer network architecture in which transaction is not controlled by a single centralized entity. The transaction is stored and controlled in form of blocks in decentralized manner and these blocks are accessible to all participants of the blockchain network in a trustworthy manner [7]. Both these technologies have brought a great revolution in communication and information in various technical fields, including IoT.

Technologies and components used in IoT systems may create critical security concerns. So, it is important to protect IoT systems in every dimension of IoT infrastructure. Efficient approaches need to be designed for the security of IoT systems. CIA triad is a widely used security model that consists of three major key components: confidentiality, integrity, and availability. These security features must be targeted while designing IoT architecture and ensuring security in every related application area [8].

The proposed architecture presented in the present paper is motivated by several kinds of issues present in the IoT ecosystem. Most of the existing IoT applications suffer from several kinds of security issues (such as privacy, integrity, and single-point of failure) as well as resource related issues (memory, storage, etc.). An ideal IoT architecture must be designed to get rid of all of these problem. The main contributions of the paper are as follows:

- The paper focus on design of an organized IoT architecture utilizing the features of blockchain technology and cloud infrastructure which provide advanced and efficient security, storage and computational solutions.
- Authors in the present paper proposed a 7-layered (perception, network, transport, processing, service, security, application and parallel management and control) Cloud and Blockchain-enabled secure IoT architecture.

Section II presents a brief survey of related literatures. Section III gives a brief description of cloud computing, blockchain technology, and integrated cloud and blockchain technologies which will be deployed to design an advanced and secure IoT architecture. Section IV presents IoT architecture consisting of a perception (sensing) layer, network/ transport layer, processing layer, service layer, security layer, and a management and control layer. The proposed IoT architecture uses edge and fog services for processing, storage, and computation at the local level. This section also presents prominent cloud and blockchain technologies in an integrated form to provide better and innovative services. Section V presents the analysis of proposed cloud-blockchain-based secure IoT architecture and provides brief discussion of improvements done by proposed IoT architectures over recently proposed existing IoT architectures. Section VI concludes the entire research work presented in the present paper.

II. Related Work

Several researchers have conducted number of researches in the area of IoT which address various aspects of designing and modeling. Several researchers have proposed different IoT architectures on the basis of different concerns related to storage, security, communication and services.

Several IoT architectures have been explored in the present paper which vary in terms of the number of layers, type of layers, and terminologies used for layers. Sethi and Sarangi in [9] presented some basic and traditional IoT architectures which include 3-layers and 5-layers IoT architectures. Three layer architecture is composed of the perception layer, the network layer and the application layer. Five-layered architecture includes two additional layers which are the processing layer and the business layer. Wu et al. proposed a five-layer IoT architecture [10]. Many authors including Gokhale et al. [11] and Muhammad et al. [12] discussed the four-layer IoT architecture. However, 3-layer IoT architecture is very common and comprises three key layers [13-15]. Initially, three-layer architecture was accepted for IoT management systems. Four-layer IoT system architecture comprises the sensing layer, the network layer, the service layer, and the application layer. In this way, many pieces of research have been conducted by various researchers to design more advanced IoT architectures and every new research targeted a specific problem to be solved. Hence, the features and behavior of IoT architecture depend on the targeted problems.

In recent years, some architectures have been designed using several advanced technologies. Cloud computing provides cetral data processing facility. Cloud is a part of the middle layer that lies below to the application layer and above to the perception and the network layer [16]. IoT architecture proposed by Hassan and Eassa [4] was dedicated to smart home systems that was designed using cloud computing, context-awareness and some other building blocks.

In terms of IoT, data is significant digital asset that need to be stored with efficient and reliable security solutions. Some of the most recent IoT architectures focused on decentralized blockchain technology in order to provide security, immutablitity and trust to the data generated by IoT system. Many researchers have discussed about decentralized blockchain approach [17]. Zhou et al. in [18] proposed a blockchain-based secure IoT system that facilitates homomorphic computation and system security. Ullah et al. also discussed blockchain-based approach for providing security to IoT.

III. Cloud Computing and Blockchain

The exponential growth of IoT technology creates massive and heterogeneous network traffic. Along with the information this technology generates lots of security issues. An ideal IoT architecture can efficiently deal with such affairs. It must be able to secure the entire IoT infrastructure throughout its layers and able to manage and control all the activities. The proposed framework utilizes cloud computing and blockchain to promote information security.

A. Cloud Computing

Cloud computing is the latest Internet-based technology that provides on-demand availability of resources such as data storage and computing power without direct management by the user. IoT data, services and incidents can be remotely stored, computed and processed over the Internet using cloud services and can be accessed whenever required. Cloud computing provides many services such as Platform as a service (PaaS), Infrastructure as a service (IaaS), and Software as a Service (SaaS) with affordable cost, scalability, faster speed, high flexibility, reduced complexity, and low risk [19], [20].

1) IaaS: It facilitates on-demand fundamental computing, networking and storage resources to consumers over the Internet on the basis of their request. It is composed of physical and virtual building blocks that provide the facility of execution of workloads and applications without worrying about storage and computation efficiency with little expenses.

2) PaaS: In this cloud computing system, users are facilitated with hardware, software and infrastructure services for developing, executing and managing applications without any expenditure and complexity. The users need to pay only for some resources they utilize. Cloud service providers like Microsoft Azure, Amazon Web Services (AWS), IBM, Google Cloud offer PaaS services.

3) SaaS: Cloud computing provides on–demand software services to the users without direct installing on the system. The users can remotely access these services over the Internet without complex hardware and software management.

B. Blockchain

Initially, blockchain technology was particularly introduced and adopted for Bitcoin cryptocurrency [6]. But in recent years, it is widely deployed in numerous application areas to keep digital records in decentralized and secure manner. It is a good choice for digital forensics to preserve digital evidences with high security, integrity, authenticity and confidentiality. It is a decentralized ledger technology that is anticipated on the peer-to-peer network [21].

A blockchain is a group of interconnected blocks used to store transactional data or events that are managed by all the participants without requiring a central authority manager. It stores event information in such a way that is virtually impossible to add, modify, or delete by unauthorized users. It allows all participating (authorized) users to generate and validate transactions in a peer-to-peer manner. Cryptography [22] and consensus [23] approaches are most significant components of blockchain technology.

Cryptography ensures the security and privacy of data and participants. Cryptographic hash functions are the most widely used techniques adopted by blockchain technology. The term ‘Blockchain’ is composed of block and chain where a chain is divided into many blocks. The initial block (genesis block) has no parent block and its value is set to zero. The consensus approach provides trust in an untrustworthy environment. It verifies the integrity and trust of the transactions. Being a decentralized technology, each block (node) in the blockchain network stores a copy of the ledger to protect data from a single point of failure.

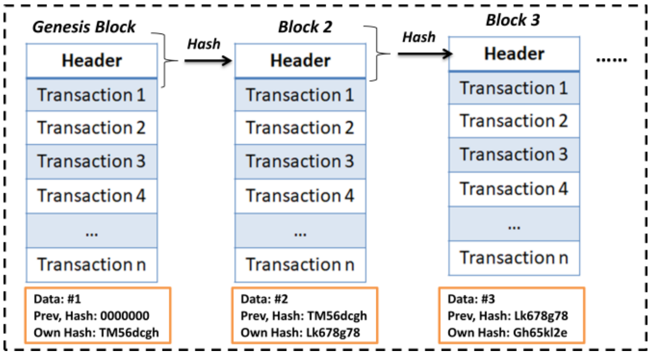

Fig. 1. Linked Blocks.

Fig. 1 shows how blocks are linked and arranged where only the first block has no parent (previous) block to it, hence its previous hash is automatically set to 0 and own hash value is generated for block 1. The hash value of block 1 is passed to block 2 and that value becomes its previous hash then the own hash value of block 2 is generated. The ledger in the blockchain contains a certain number of blocks whereas the first part contains a fact that needs to be stored in a database (e.g., network traffic logs, a record, etc.). The second part contains the header information. It includes the transaction hash, the hash of the previous hash, and the timestamp. This kind of storage makes a sequential chain of blocks [24]. When a new transaction or record needs to be added to a blockchain, first it will be added to a new block. The records added to the blocks in a blockchain can be verified individually using a hash function. Hash functions can ensure data integrity inside blockchain networks [25].

1) Selection of hash functions: A lightweight hash function must be used for block mining. The algorithm used for hashing must serve security using cryptography. The function should also fulfill certain conditions. The output size of a lightweight hash algorithm is 256 bits. If this size is reduced, the security strength also get reduced. The hash algorithms designed for IoT devices need to be designed specifically. These devices do not have sufficient memory of their own to calculate the area for implementation. So some microchips can be embedded in IoT for using cryptographic hash (like SHA-1 and SHA-2) [26].

2) Block structure: Fig. 2 presents the Structure of the Hash Chain or Block. A block structure is composed of a header and the body. The header consists of various fields like Version number, a timestamp, block size, and related transactions [27].

Every transaction generates a hash value to generate a unique Merkle root. Here, the cryptographic nonce is used for proof of the transaction in an encrypted manner i.e. called ‘proof-of-work’ or ‘proof-of-state’. Miner identifies a nonce that generates hash values according to the set value. Difficulty targets the time of block creation. Each block is generated by a distinct hash value. A Merkle tree is a type of binary tree that is formed of hash pointers. It is constructed from leaf nodes toward the head or root node.

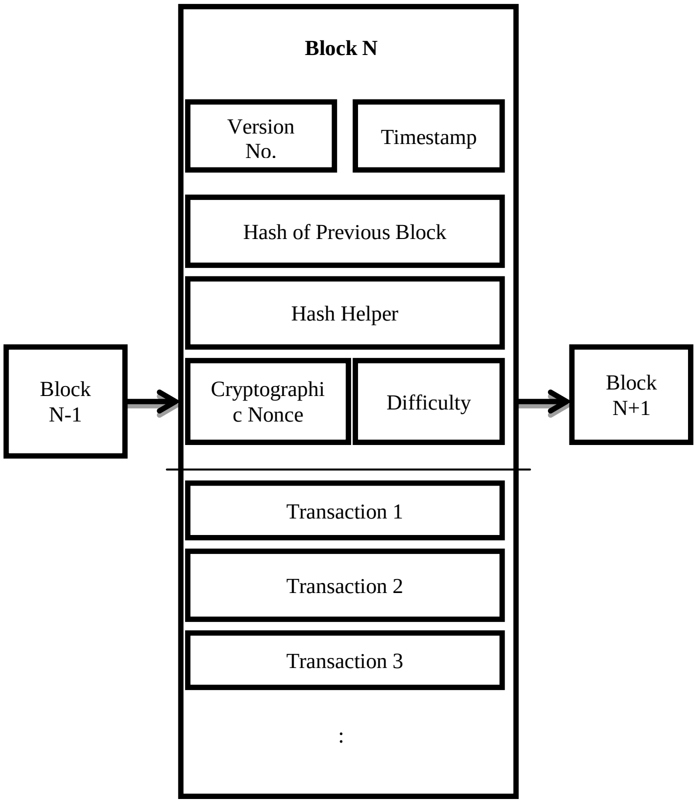

Fig. 2. Blockchain Block Structure [11].

C. Integrated Cloud and Blockchain-Based Internet of Things (BCoT)

The integration of cloud computing in IoT constructs a Cloud of Things (CoT) environment [28]. Cloud computing offers many opportunities in various technical areas including IoT. Cloud computing contributes to making IoT services flexible, scalable, and cost-effective. These services reshape the IoT environment and improve system performance by providing flexibility and robustness. However, the traditional cloud model is based on centralized communication [29]. IoT devices are connected, monitored, and managed by a central server in the cloud. If the centralized system is attacked, it may lead to the destruction of the whole system. An IoT architecture that adopts cloud computing needs a more advanced solution to make the infrastructure decentralized or distributed. It becomes difficult to scale the widespread centralized IoT infrastructure and its communication network requires many communication channels. Several concerns arise in the case of big communication networks like the requirement of a trusted third party (a central cloud server), high communication latency, and increased cost.

To achieve a legitimate solution, a decentralized ecosystem approach needs to be deployed in computing. Blockchain technology is based on peer-to-peer network architecture. The blockchain is a decentralization-based technology and it doesn’t depend on the central point of control for transaction management. It also reduces the risk of single-point failure occurring due to disruption of central authority [30]. Each node can be verified independently and the architecture built using blockchain technology ensures secure and robust operations [31]. Integration of blockchain and cloud computing in combined form provides several significant benefits [32]. The blockchain-based architecture uses a distributed storage and computing approach using virtual storage nodes. Blockchain uses a virtual decentralized storage system without using a central authority. Blockchain behaves as a layer among various cloud servers and end-users. Using only cloud services may lead to high-security issues because the centralized server is only responsible for the security and privacy of the entire communication network. Blockchain-as-a-service (BaaS) follows peer-to-peer communication that eliminates the requirement of a trusted third party. Adoption of blockchain technology integrating with cloud computing provides major benefits discussed below:

- Decentralization: It can solve the bottleneck problems occurring in centralized structures, such as single points of failure [33] as well as it also reduces the communication delay and power consumption in IoT devices. It also resolves traffic load balancing issues by establishing short routes [34].
- Enhanced Security and Privacy: For data processing, the Cloud of Things (CoT) need to depend on a third party i.e., a cloud service provider that raises privacy issue. Blockchain-based cloud of Things (BCoT) provides a trustworthy access control that enables only authorized users to access all the services automatically.
- Integrity: Blockchain resolves the problem of data integrity, management and control, and synchronization in distributed databases.
- Quality of Service (QoS): Cloud computing alone is unable to handle Quality of Service for many applications like reliability, real-time, and security. Edge computing is an alternative to cloud computing that can overcome these problems. But it has less scalability, and it is a costly solution. Integrated blockchain with cloud in IoT (BCoT) also resolves this problem [35].
- Immutability: Blockchain provides immutability due to the uniqueness of blocks with unique hash values.
- Scalability: Cloud provides a better storage facility. Integrating blockchain in IoT with the cloud provides better system scalability due to the consensus mechanism.
- Fault tolerance: Replication and redundancy are basic concepts behind fault tolerance which are handled in cloud computing [36].
- Cost optimization: Cloud system provides robust integration of massive data. It also provides distributed resource facility. It improves operational efficiency and reduces cost.
- Strong Authentication: Due to strong encryption and key concepts, a Blockchain-based system provides better authentication.

- Consensus: Consensus is used to establish trust. Consensus may differ in scalability, fault-tolerance, power consumption, etc. [37].

IV. Proposed IoT Architecture

So far, there is no generalized architecture of IoT that has been adopted globally and that can provide various advantages such as efficient storage, decentralized security, and proper data and event management and control altogether in a single IoT architecture. Different researchers have proposed different IoT architectures consisting of different numbers of layers. With the origination of IoT, initially, very simple architectures were proposed that describe the basic scheme of IoT. For many years, three layers architecture consisting of the perception (physical) layer, network layer, and application layer has been widely used. However, this architecture does not provide adequate information about IoT security. It is suitable just for development in the initial stage [10]. It was not sufficient for IoT development; hence a better model was required that can explain the features and inferences of IoT more appropriately.

A. *IoT Functional Building Blocks*

An ideal IoT framework must consists of all standard components (like sensors, actuators, devices, communication protocols, network and device controllers, etc). The model presented here is composed of seven layers and all the standardized modules (blocks) which are mandatory for an ideal IoT model. IoT system architecture consists of various functional building blocks to assist different utilities viz. sensing, actuation, identification, communication, and management [38], [39].

- Connected Objects (Heterogeneous Things): Internet-connected devices or things are the main components of an IoT system that include sensors, actuators, monitoring devices, Bluetooth Low Energy (BLE) devices, and Radio Frequency Identifiers (RFID). IoT devices are end nodes that can communicate with other connected nodes (devices and applications). These nodes can send and receive data, process the data locally, or get it processed by centralized servers or cloud-based back-ends. All connected nodes generate a certain amount of data in any form that is processed by a data analyzer to generate useful information.

- Communication: This block carries out communication between connected devices and remote servers. It contains components like communication protocols, network enabling devices, etc.

- Processes: Processes are the technologies or functions which are responsible for information processing. The main processes of IoT systems are communication, accumulation, and analysis.

- Services: IoT system performs several types of functions like device modeling, device control, device discovery, data analysis, data control, and data publishing. The service module includes various service-providing technologies such as cloud/fog/edge computing and blockchain technology.

- Management: The management layer contains various functions to govern or monitor activities and components of the entire IoT system.

- Security and Privacy: The security layer provides various functional approaches to secure IoT systems such as authentication, authorization, access control, integrity, privacy, and security.

- Application: The application layer works on the applications of IoT architecture. It functions as an interface for IoT systems and provides the required elements to monitor and control IoT systems. It also allows users to visualize and analyze the present status of the IoT system.

B. *Layers of Proposed IoT Architecture*

The proposed IoT framework also highlights the concept of the flow of data (information) over a network through an IoT infrastructure. The IoT architecture presented in this paper pays attention to the flow of information through six standard layers that is managed and controlled using a parallel layer. A standard architecture of an IoT system has been depicted in this paper. Fig. 3 presents the proposed IoT architecture enabled with integrated cloud computing and blockchain technology.

1) Perception layer: The perception layer also known as the sensing layer is a physical layer. This layer encompasses many types of sensors. The general idea behind this layer is to collect real-time data from heterogeneous sources such as connected physical and digital devices, controllers, and applications [10]. Sensors are the most important tools which contribute to sensing and collecting essential data from related sources. The sensor senses the presence of a physical thing or a quantity and collects value on a physical parameter e.g., temperature, pulse rate, etc. The sensor returns output in form of signals readable by humans. Transducers are the tools that convert signals from one form to another form. This layer is also known as the physical layer because it can collect data and values directly from devices. The components (Things) of this layer represent the front end of IoT. The ‘things’ are the uniquely identifiable devices carrying a unique IP address that makes them easily identifiable over the network. The perception layer contains various devices such as RFID tags and readers, GPS, cameras, etc. with important sensing technologies.

a) Controller: Microcontrollers are most widely used in IoT technology. A microcontroller operates at the physical/ abstraction layer running the selected operating system/real-time operation system, which provides operating facilities to IoT devices. A microcontroller is a single integrated chip (IC) embedded with a CPU, RAM, ROM memory, and peripherals. It is like a small computer itself. Many things are embedded in a single chip, and it provides lower performance than a microprocessor. But it is a much better choice for smart IoT devices, and its computing power is also sufficient for all IoT applications.

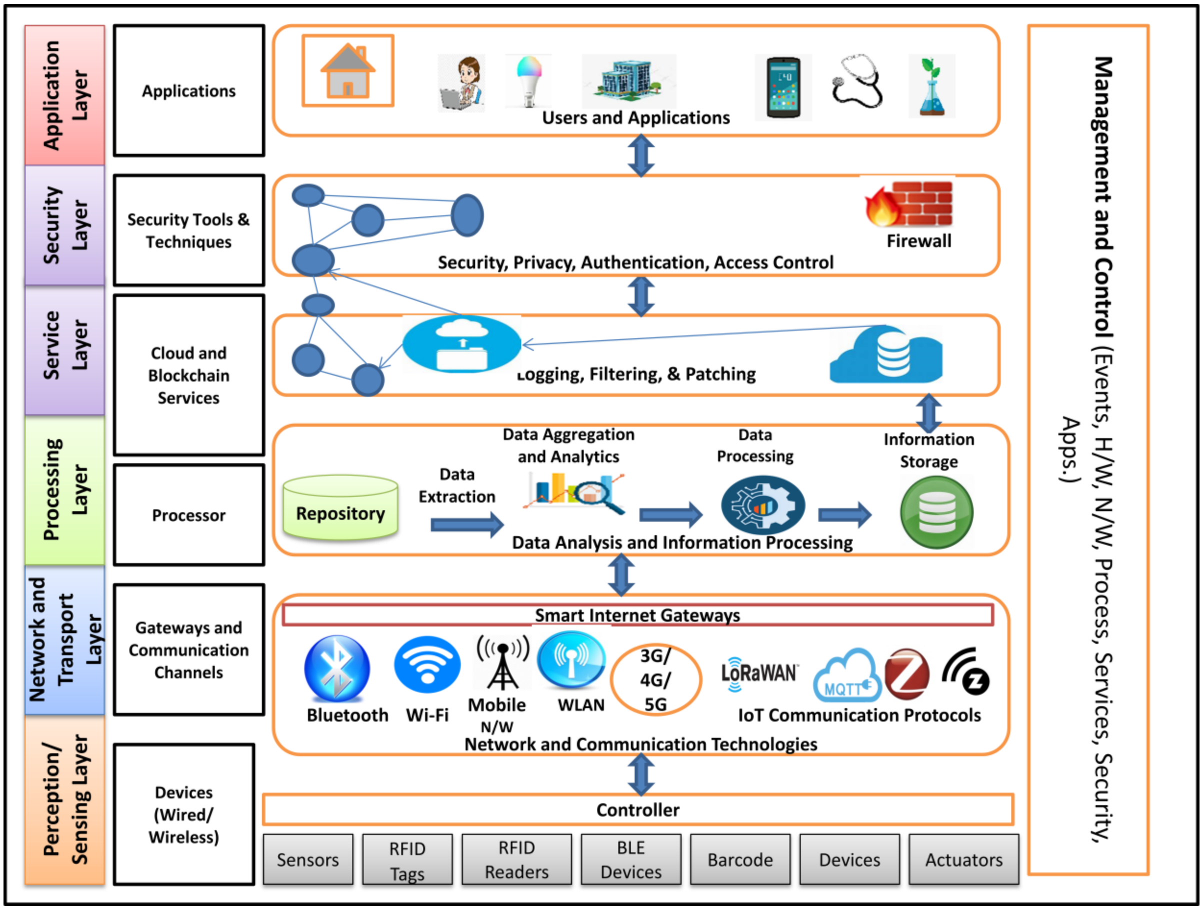
Application Layer
Security Layer
Service Layer
Processing Layer
Network and Transport Layer
Perception/ Sensing Layer
Applications
Security Tools & Techniques
Cloud and Blockchain Services
Processor
Gateways and Communication Channels
Devices (Wired/ Wireless)
Users and Applications
Firewall
Security, Privacy, Authentication, Access Control
Logging, Filtering, & Patching
Repository
Data Extraction
Data Aggregation and Analytics
Data Processing
Information Storage
Data Analysis and Information Processing
Smart Internet Gateways
Bluetooth
Wi-Fi
Mobile N/W
WLAN
3G/ 4G/ 5G
LoRaWAN
MQTT
IoT Communication Protocols
Network and Communication Technologies
Controller
Sensors
RFID Tags
RFID Readers
BLE Devices
Barcode
Devices
Actuators
Management and Control (Events, H/W, N/W, Process, Services, Security, Apps.)

Fig. 3. Blockchain-Enabled Secure IoT Architecture.

2) Network and transport layer: The transport layer receives data packets from the perception layer and transmits them to further layers using various network technologies viz. Bluetooth, Wi-Fi, wireless LAN, and various IoT communication protocols (HTTP, Zigbee, MQTT, Z-Wave, 6LoWPAN, LoRaWAN, etc.) [40]. This layer performs data management from storage to processing state of data leading to reliable data transportation [41].

a) Smart Gateway: It is not possible to directly connect many sensor networks and IoT. IoT and sensor networks consist of sink nodes and base stations. The role of the gateway is to collect the data from base stations and the sink nodes and generate a multi-hop communication structure. In this structure, multiple nodes develop and spread more widely. More heterogeneous data development requires more processing and comprehensive data analysis from the gateway. This structure also customizes the security according to the requirements of IoT and WSN. Sink nodes can efficiently handle the sensor nodes. Here, the gateway handles the heterogeneous data collected from various kinds of devices and networks.

3) Processing layer: In IoT systems, data is captured from devices and stored in datasets, and processed for further requirements. The processing layer is the brain of the IoT system that contributes to the analysis of event data and information processing. Events captured by different sensor devices are stored in datasets. An enormous amount of raw data is extracted from the data repository that is to be analyzed and processed. The processing layer operates on a real-time system and it is responsible for data security through encryption and decryption approaches.

The information gathered from smart IoT devices or end nodes is sent to the cloud [42]. The information is then processed through any processing technique (which could be AI/ Machine learning) for providing data to the user. A certain level of intelligence is added to the devices which makes the IoT system smart. Devices like sensors and actuators are added to the system which collects information from IoT devices and sends it to the cloud through a communication mechanism (Bluetooth, WiFi, Zigbee, etc.) [43].

4) Service layer: The service layer provides a rich set of functions for communication, processing, and storing. This layer is responsible for managing IoT services. Cloud and edge [44] are important IoT services. These services are required to enable IoT systems to meet the security, scalability, and speed requirements [45].

a) Cloud Computing: Technically, the cloud is not a mandatory part of an IoT system. Data storage and data processing take place remotely in the cloud rather than in the system itself. Most of the users store their data on Google

Drive rather than on personal computers. Google Drive uses Google cloud services. Cloud computing makes the Internet of Things more successful by enabling users to perform computing using the services provided over the Internet [46]. A large amount of data is generated by rapidly growing IoT technology that arises the problem of storing, processing, and accessing the data. The integration of cloud computing into the Internet of Things gives an innovative solution. Uploading and storing of sensory data streams take place on the cloud instead of the local device storage.

b) Edge Computing: In IoT edge, devices and sensors communicate real-time data to a network. Pairing the IoT with edge computing makes data processing much faster. In the absence of cloud computing, edge networks and edge computing approaches can control IoT system units individually. The combination of edge and the cloud provides much better development for IoT. Edge computing also reduces the load of data by aggregating it before uploading it to the cloud. Azure is a widely used IoT edge [47]. It allows for storing, processing, and analyzing large volumes of real-time data locally at the network edge. It saves time and resources to send all data to the cloud. Sensitive information is processed and packaged into several packages and sent securely to the cloud.

c) Fog Computing; Fog computing can be used as an alternative to edge computing. If gateways are not able to handle interoperability and trans-coding, this can be attained through fog computing. A fog network is established between the cloud and gateway network. Fog provides better and refined applications and services by extending conventional cloud computing [47]. Fog computing provides a virtual platform that provides storage, computation, and network services between IoT end nodes and the cloud [48]. Fog can provide better quality functioning to mobile nodes by positioning the proxies and access points according to nodes. Fog provides better communication than gateways. It can also include virtual sensor nodes and virtual sensor networks. By co-locating with the smart gateway, it provides low latency communication, temporary storage, better security, more privacy, and easy preprocessing of smart tasks like facilities [49].

d) Blockchain Services; Blockchain technology can be utilized to store digital information in a public database. Some widely known industries like Amazon and Microsoft Azure offer blockchain services i.e. Blockchain as a service (BaaS). A Group of digital information is stored in form of blocks in a hierarchical form. A unique encrypted code is assigned to each block that distinguishes them from each other. These blocks are generally designed using a hash mechanism combined with special programming techniques [50]. It provides improved security by removing human involvement. It uses Asymmetric key cryptography for transactions. Block of keys (public and private keys) are used for entire transactions. Signatures are validated using a private key and a public key verifies the signatures generated by a private key. The decentralization of blockchain makes it harder to tamper with the stored results. However, blockchain services are utilized only to store transactions. The transactions are verified, hashed, and stored in blocks in form of digital signatures.

5) Security layer: Security is the major requirement of IoT architecture. The IoT security layer takes responsibility for managing the security of various components of IoT across the entire infrastructure. The security layer is essential for the security of all the layers of IoT architecture. It makes the information secure before communicating between external and internal users. This layer collects the processed data from the processing layer and encrypts it before sending it over the network using a strong encryption algorithm or a combination of selected encryption algorithms. The legitimate receiver receives the encrypted information that could not be recognized by the illegitimate user [51]. However, securing only the information is not sufficient to secure an IoT infrastructure. It is required to follow all security measures to protect the IoT environment. Authentication and access control mechanisms are used to manage and improve the security system. Blockchain provides security solutions for storage as well as communication.

a) Device Security: Smart devices around the world can communicate with the services like servers or the cloud using Ethernet or Wi-Fi. But these devices are not well-equipped to manage the security concerns of Internet connectivity. The devices must be activated by security features. Security features embedded with hardware and firmware enable devices to handle security, authentication, encryption, proxies, caching, connection loss, timestamps, etc. Device security can be achieved using the following methods:

- Trusted platform module: IoT enabled chips could be embedded with cryptographic keys for the security of end nodes. Security chips containing the security protocols that can be deployed on the sensor devices and these protocols are called to recognize the security operations. Security operations include mutual authentication, mutual signature verification, etc. The security chips may be connected to the sensors using an SD card [52].

- A secure boot process can prevent unauthorized code from the device.

- Security patches must be updated regularly to protect from malware and threats.

b) Network/Communication Security: A communication network is a medium over which data is transmitted and received. Unsecure communication channels might be liable to serious security risks. The communication layer must be equipped with innovative security solutions. Data communication over the network should be encrypted for a secure connection. Data encryption protects communicating data from unauthorized access and information interception. IoT-centric messaging protocols (AMQP, MQTT) can use Transport Layer Security (TLS) cryptographic protocol for end-to-end data protection. However, firewall also works as an obstacle between a secure and insecure network. A firewall is like a physical security fence that monitors the network and attempts to block certain types of incoming suspected network traffic to prevent attacks on a private network. It does this by filtering both in and out network traffic. Blockchain is a smart security mechanism that provides end-to-end security to entire IoT architecture including cloud.

c) Service Layer Security: Modern IoT systems adopt cloud-based service solutions, which are vulnerable to privacy violations, and failure on a single point, Denial-of-service attacks [53]. Blockchain is an advanced technology that employs a cryptography approach to guarantee the security of distributed ledgers. It supports many advanced technologies such as hashing, elliptic-curve, and distributed consensus approach. Blockchain combined with services provides a promising solution. Cloud is a central system that can be exploited by attackers. Blockchain provides independent and distributed services utilizing public-key cryptography algorithms. Blockchain-based IoT system also facilitates access control.

d) Application layer Security: The application layer is the most sensitive and wider attack surface. Applications are directly exposed to users. The users could be authenticated or malicious actors. The security of the application layer depends on the type of application and the purpose of the application. Security needs to be customized to the unique situation [54]. Trade-offs accompanying strict security measures might be effective in preventing attacks. Application layer security also relies on the selection of communication protocols such as (HTTP, MQTT, CoAP, etc.) used with the system. Each protocol has its strategy to conduct user authentication. So it is important to be familiar with the pattern of each protocol for security improvements. Message Queuing Transport Protocol (MQTT) is the most widely used Client Server publish/subscribe messaging transport protocol. It is a simple, ideal, and above all lightweight messaging protocol used in end-to-end communication. MQTT can be used for telemetry to receive data from sensors and actuators and can command that remotely using the MQTT client library [55]. It supports various authentication mechanisms and Secure Socket Layer (SSL)/Transport Layer Security (TLS) based encryption for transport protection [56]. Application firewalls can be used to guard the application layer. However, firewalls must build and configure considering the specificity of applications. A highly secure application layer can protect other layers too from security breaches because most of the breaches enter through the application layer. It is important to consider security in the designing of protocols [57].

6) Application layer: The application layer is the top layer of IoT architecture. This layer directly interacts with outside users and delivers application-specific services to the users. All the communication from user to system passes through the application layer [58].

a) Authentication: The security mechanism is integrated with the application layer. A user who wants to access an IoT system first needs to pass through the authentication process. Using an identity identification mechanism, the unauthorized user is prevented to access the system.

b) Risk Assessment: The integration of effective security mechanisms in IoT provides an improved security structure.

c) Intrusion Detection: Several application-specific intrusion detection techniques are used with IoT to find security solutions. All the incoming and outgoing events are monitored and their logs are stored in databases which are analyzed for threat detection. An alarm is triggered on the occurrence of suspicious activity.

7) Management and control layer: IoT is an ecosystem where several heterogeneous devices (things) are connected using the Internet carrying distinct missions and functionalities. IoT management has been a challenging task for researchers [59]. In the network, the devices are connected and recognized with the help of their unique IP addresses. IoT device management is like ant colony management. This is a parallel layer that aims to provision, configuration, administration, monitor, and diagnostics of various assets utilized on IoT platforms. It also plays an important role to detect various challenges faced by connected devices.

a) Device Management and Control (DMC): IoT devices can be managed using various tools and techniques designed for IoT device management. IoT device management is used to maintain the security, connectivity, and efficiency of connected smart devices. Management and control Fundamental requirements of IoT device management are:

- Provisioning and Authentication: Provisioning is the process of registering an IoT device to ensure its reliability of an IoT device and authentication is the process through which only devices with valid credentials (certificate/key) are registered. It is necessary to protect the IoT system from malicious attacks.
- Configuration and Control: This is the process of installing a new device using some settings to enable it for working. But only installation does not ensure its performance, functionality, and security from threats. So while configuring the control settings must be fine-tuned for device maintenance and management.
- Monitoring and Diagnostics: To solve very issues, it is necessary to identify them first. A constant monitoring system provides the continuous logging of a device.
- Updates and Maintenance: The software is required to be updated frequently from the moment of installation for the flawless functionality of a device. Devices can be updated and maintained manually as well as remotely.

b) Network Management and Control (NMC): Network management is the process of operating, monitoring, and controlling an entire network to optimize its efficiency [60]. NMC is a diversified authority that provides various network management tools, techniques, protocols, and processes to the network administrator. Network management and control emphasize on management, monitoring, and control of various network components responsible for device connectivity and data communication. Several types of networks enabling devices (Bluetooth, router, gateways, switches, cables, etc), communicating protocols, technologies (Wi-Fi, 3G/4G, etc.), and services (Internet) are used for connectivity and communication. Network management and monitoring are developed every year and are launched in periodic seasons. NMC monitors and analyzes the network traffic that might contain normal as well as anomalous traffic patterns. Based on the nature of the traffic patterns, it is routed and controlled.

c) Data/Information management: Data management is the process to aggregate and analyzing overall collected valid data and refining it into information [61]. Large volumes of data are produced by different IoT devices and applications [62]. A perfect data management framework is needed that can efficiently collect, manage, and distribute data and must be compatible with existing software and hardware. Data collected from IoT devices are used for analytical purposes. IoT data is processed, managed, and analyzed locally using edge computing and at a centralized level using cloud computing.

d) Security and event management: End-to-end security management is essential for ensuring the privacy and security of IoT devices, services, information, and applications. It protects IoT systems from various attacks. Data, logs, and event monitoring and analysis make IoT systems enable them to protect themselves from various threats and vulnerabilities. But it is difficult to prevent all security risks so an efficient security event management process is required that could ensure rapid recovery. Real-time insight tools and audit trails provide facilities like monitoring, analytics, and log management which can be utilized to get the root cause of an event. This information can be used in digital forensic investigations as evidence.

V. Comparative Analysis and Discussion

Most of the well-known existing IoT architectures generally composed of three or four layers. Traditional IoT architectures do not focus on the storage efficiency and security properties altogether. IoT architecture proposed in the present paper collectively focused on these necessary properties in order to design an efficient IoT architecture. Integrating cloud computing and blockchain technology into IoT ecosystem can provide endless solutions to various kinds of security and storage issues. Table I briefly presents comparative analysis of proposed cloud-blockchain-based secure IoT architectures with some recently proposed advanced IoT architectures.

Quereshi et al. in [63] proposed a cloud-based IoT architecture to overcome the problems of storage and resources. Das et al. in [64] proposed a smart IoT architecture integrating cloud computing with IoT mechanisms. The approaches proposed in [63] and [64] resolve storage and resource related problems. But the centralized storage and access facilies provided by cloud computing may create data security, integrity, and privacy issues. The data stored on cloud platform can be easily compromised by unauthorized users. Author in [65] presented a white paper with his research work that consists of an IoT architecture. The proposed architecture focused on connectivity, data management and application analytics. Qiu et al. in [66] proposed an IoT architecture dynamic blockchain technology. This architecture facilitates decentralized storage with trust, transparency and security. Hou et al. in [67] proposed an IoT architecture using the Blockchain technology. This architecture provides good performance in terms of security, integrity, authentication, reliability and trust. However, storage and scalability still remain significant issues. Which can be resolved by storing the data on cloud platform integrating with blockchain technology. Sharma et al. in [68] focused on advantages of blockchain technology while designing the IoT architecture.

TABLE I. Comaparative Analysis of Proposed Cloud-Blockchain-Based Secure IoT Architecture with Existing IoT Architectures

Literatures	Research Gap	Improvements by proposed Architecture
Qureshi et al. [63]	Security and integrity issues due to centralized storage	Integration with Blockchain technology provides better security and integrity.
Das et al. [64]	Data protection, integrity, security issues	Integrating with Blockchain technology resolves security and integrity issues.
A. Hakim [65]	Not focused on security and resource problems	Focused on security, integrity and storage solutions
Qiu et al. [66]	Focused on bitcoin; Storage issue	Provides advantages of cloud and blockchain technologies and it is not application-specific
Hou et al. [67]	Lack of scalability	Cloud computing can overcome the scalability issue.
Sharmaet al. [68]	Focused only on advantages of blockchain	Proposed architecture consideres advantages as well as disadvantages of cloud and blockchain

IoT architecture proposed in present paper considers the advantages as well as disadvantages of cloud computing and blockchain technology. There are several disadvantages of both of these technologies beside their advantages that must be fixed while implementing them into IoT ecosystem.

VI. Conclusion and Future Scope

The paper presents a design of integrated cloud and blockchain-based secure IoT architecture to resolve various kinds of data security and storage challenges. The proposed cloud-blockchain-based secure IoT architecture is composed of seven layers. In addition to various layers (perception layer, network layer, processing layer, and application layer) which are very common in existing IoT architectures and generally included in the design of every IoT architecture, the proposed IoT architecture includes three additional layers namely the service layer, the security layer, and the management and control layer. Blockchain technology provides end-to-end security solutions with trust, integrity, reliablility and reduces many types of challenges in IoT infrastructure. The service layer is the key layer of IoT architecture that uses integrated features of cloud computing and blockchain. This approach provides decentralized or distributed services in an IoT environment that overcomes various challenges occuring due to centralized communication. It prevents single points of failure, high communication costs, and the need for a central agent. It also provides several security benefits by using advanced cryptographic mechanisms like hashing to encrypt data and events in an IoT environment. The management and control layer placed in parallel to the entire architecture contributes to monitoring, managing, and controlling various activities and components throughout the IoT system. A secure and well-managed IoT architecture is the basic requirement of successful IoT technology. It is highly needed for realizing the dream of smart cities. Therefore, the proposed IoT architecture can be of greatly helpful for researchers as well as can be used in industries and other private and government sectors for building smart infrastructures. In future, the proposed IoT architecture can be deployed for developing different applications in IoT infrastructure with high security and efficiency.

REFERENCES

[1] S. Bhardwaj and S. Harit, “SDN-Enabled Secure IoT Architecture Development: A Review”, *Inventive Communication and Computational Technologies*, 599-619, 2022. https://doi.org/10.1007/978-981-16-5529-6_47.

[2] M. R. Raza, A. Varol, & W. Hussain, “Blockchain-based IoT: An Overview,” In: *2021 9th International Symposium on Digital Forensics and Security (ISDFS),* June 2021, pp. 1-6, IEEE. https://doi.org/10.1109/ISDFS52919.2021.9486360.

[3] S. Sharma, A. Parihar, and K. Gahlot, “Blockchain-Based IoT Architecture,” In: P. Raj, A. K. Dubey, A. Kumar, P. S. Rathore (eds) Blockchain, Artificial Intelligence, and the Internet of Things. EAI/Springer Innovations in Communication and Computing. Springer, Cham, 2022. https://doi.org/10.1007/978-3-030-77637-4_10.

[4] A. Z. Hassan Samah and E. E. Ahmed, “A Proposed Architecture for Smart Home Systems Based on IoT, Context-awareness and Cloud Computing,” (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 13, No. 6, 2022.

[5] H. Ullah, M. Abu-Tair, A. Ali, K. Rabbani, J. Daniel, J. Rafferty, Z. Lin, P. Morrow, and G. Ducatel, “IoT security using Blockchain,” In *Essentials of Blockchain Technology*, Chapter 8, pp. 169-188, Chapman and Hall/CRC, 2019.

[6] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review,”* 21260, 2008.

[7] F. Tschorsch, & B. Scheuermann, “Bitcoin and beyond: A technical survey on decentralized digital currencies,” *IEEE Communications Surveys & Tutorials*, Vol. 18, No. 3, pp. 2084-2123, 2016.

[8] Butun, I., Almgren, M., Gulisano, V., & Papatriantafilou, M. (2020). Intrusion Detection in Industrial Networks via Data Streaming. In Industrial IoT (pp. 213-238). Springer, Cham.

[9] P. Sethi and S. R. Sarangi, “Internet of Things: Architectures, Protocols, and Applications,” Journal of Electrical and Computer Engineering. Hindawi, Vol. 2017, Article ID 9324035, pp. 1-25. https://doi.org/10.1155/2017/9324035.

[10] M. Wu, T. J. Lu, F. Y. Ling, J. Sun, & H. Y. Du, “Research on the architecture of Internet of Things,” In *2010 3rd international conference on advanced computer theory and engineering (ICACTE)* , Aug. 2010, Vol. 5, pp. V5-484. IEEE.

[11] P. Gokhale, O. Bhat, S. Bhat, “Introduction to IOT,” International Advanced Research Journal in Science, Engineering and Technology, Vol. *5*, No. 1, pp. 41-44, 2018.

[12] M. U. Farooq, M. Waseem, A. Khairi, & S. Mazhar, “A critical analysis on the security concerns of internet of things (IoT),” International Journal of Computer Applications, Vol. 111, No. 7, pp. 1-6, 2015. https://doi.org/10.5120/19547-1280.

[13] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, & W. Zhao, “A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications,”. *IEEE internet of things journal*, Vol. *4,* No. 5, pp. 1125-1142, 2017. https://doi.org/10.1109/JIOT.2017.2683200.

[14] H. A. Khattak, M. A. Shah, S. Khan, I. Ali, & M. Imran, “Perception layer security in Internet of Things,” Future Generation Computer Systems, Vol. 100, pp. 144-164, 2019. https://doi.org/10.1016/j.future.2019.04.038.

[15] R. Mahmoud, T. Yousuf, F. Aloul, & I. Zualkernan, “Internet of things (IoT) security: Current status, challenges and prospective measures,” In *2015 10th international conference for internet technology and secured transactions (ICITST), Dec. 2015,* pp. 336-341. IEEE. https://doi.org/10.1109/ICITST.2015.7412116.

[16] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, “Internet of Things (IoT): a vision, architectural elements, and future directions,” Future Generation Computer Systems, Vol. 29, Issue 7, pp. 1645–1660, 2013. https://doi.org/10.1016/j.future.2013.01.010.

[17] Q. Wang, X. Zhu, Y. Ni, L. Gu, & H. Zhu, “Blockchain for the IoT and industrial IoT: A review,” *Internet of Things*, Vol. 10, No. 2, 100081, 2020. https://doi.org/10.1016/j.iot.2019.100081.

[18] J. Zhou, Z. Cao, X. Dong, & A. V. Vasilakos, “Security and privacy for cloud-based IoT: Challenges,”. In *IEEE Communications Magazine*, Vol. 55, No. 1, pp. 26-33, 2017. https://doi.org/10.1109/MCOM.2017.1600363CM.

[19] P. Srivastava, & R. Khan, “A review paper on cloud computing,” *International Journal of Advanced Research in Computer Science and Software Engineering,* Vol. *8, No.* 6, pp. 17-20, 2018. https://doi.org/10.23956/ijarcsse.v8i6.711.

[20] M. Humayun, “Role of Emerging IoT Big Data and Cloud Computing for Real Time Application,” (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 11, No. 4, 2020, https://doi.org/10.14569/IJACSA.2020.0110466.

[21] W. Dai, C. Dai, K. -K. R. Choo, C. Cui, D. Zou and H. Jin, "SDTE: A Secure Blockchain-Based Data Trading Ecosystem," in *IEEE Transactions on Information Forensics and Security*, Vol. 15, pp. 725-737, 2020, https://doi.org/10.1109/TIFS.2019.2928256.

[22] S. Aggarwal, R. Chaudhary, G. S. Aujla, N. Kumar, K-K. R. Choo, & A. Y. Zomaya, “Blockchain for smart communities: Applications, challenges and opportunities,” Journal of Network and Computer Applications, Vol. 144, pp. 13-48, 2019, https://doi.org/10.1016/j.jnca.2019.06.018.

[23] M. Wazid, A. K. Das, S. Shetty, & M. Jo, “A tutorial and future research for building a blockchain-based secure communication scheme for Internet of intelligent things,” *IEEE Access*, Vol. 8, pp. 88700-88716, 2020, https://doi.org/10.1109/ACCESS.2020.2992467.

[24] E-H Diallo, O. Dib, K. Al Agha, “A scalable blockchain-based scheme for traffic-related data sharing in VANETs,” Blockchain: Research and Applications, Vol. 3, Issue 3, 100087, 2022, https://doi.org/10.1016/j.bcra.2022.100087.

[25] J. Ali, T. Ali, Y. Alsaawy, A. S. Khalid, & S. Musa, “Blockchain-based smart-IoT trust zone measurement architecture,” In *Proceedings of the International Conference on Omni-Layer Intelligent Systems* , pp. 152-157, May 2019. https://doi.org/10.1145/3312614.3312646.

[26] B. Seok, J. Park, & J. H. Park, “Blockchain-based smart-IoT trust zone measurement architecture,” *Applied Sciences*, Vol. *9*(18), 3740, 2019. http://doi.org/10.3390/app9183740.

[27] H. Guo, X. Yu, “A survey on blockchain technology and its security,” Blockchain: Research and Applications, Vol. 3, Issue 2, 100067, 2022, https://doi.org/10.1016/j.bcra.2022.100067.

[28] M. S. Karunarathne, S. A. Jones, S. W. Ekanayake, & P. N. Pathirana, “Remote monitoring system enabling cloud technology upon smart phones and inertial sensors for human kinematics,” In *2014 IEEE Fourth International Conference on Big Data and Cloud Computing,* Dec. 2014, pp. 137-142. IEEE, http://doi.org/10.1109/BDCloud.2014.62.

[29] B. Kantarci, & H. T. Mouftah, “Sensing services in cloud-centric Internet of Things: A survey, taxonomy and challenges,” In *2015 IEEE International Conference on Communication Workshop (ICCW)*, June 2015, pp. 1865-1870. IEEE. http://doi.org/10.4018/978-1-5225-1832-7.ch022.

[30] M. D. Nguyen, N. T. Chau, S. Jung, and S. Jung “A demonstration of malicious insider attacks inside cloud iaas vendor,” International Journal of Information and Education Technology, Vol. *4*, No. 6, pp. 483-486, 2014. http://doi.org/10.7763/IJIET.2014.V4.455.

[31] M. Ma, G. Shi, & F. Li, “Privacy-oriented blockchain-based distributed key management architecture for hierarchical access control in the IoT

scenario,”. *IEEE access,* Vol. 7, pp. 34045-34059, 2019, https://doi.org/10.1109/ACCESS.2019.2904042.

[32] J. Zou, D. He, S. Zeadally, N. Kumar, H. Wang, & K. R. Choo, “Integrated Blockchain and Cloud Computing Systems: A Systematic Survey, Solutions, and Challenges,” *ACM Computing Surveys (CSUR),* Vol. 54, Issue 8, pp. 1-36, 2021, https://doi.org/10.1145/3456628.

[33] L. Zhou, L. Wang, Y. Sun, P. Lv, “BeeKeeper: A Blockchain-Based IoT System with Secure Storage and Homomorphic Computation,” *IEEE Access*, Vol. 6, pp. 43472–43488, 2018, https://doi.org/10.1109/ACCESS.2018.2847632.

[34] T. Wang, "A Study on the Innovative Use of Blockchain in the Human Resources Service Industry", *Wireless Communications and Mobile Computing*, Vol. 2022, Article ID 7798595, 11 pages, 2022, https://doi.org/10.1155/2022/7798595.

[35] T. Mai, H. Yao, N. Zhang, L. Xu, M. Guizani, & S. Guo, “Cloud mining pool aided blockchain-enabled internet of things: An evolutionary game approach,” *IEEE Transactions on Cloud Computing, 2021*. https://doi.org/10.1109/TCC.2021.3110965.

[36] S. Abbas, M. A. Talib, A. Ahmed, F. Khan, S. Ahmad, & D-H. Kim, “Blockchain-based authentication in internet of vehicles: a survey,” *Sensors*, Vol. 21, No. 23, p. 7927, 2021, https://doi.org/10.3390/s21237927.

[37] W. Viriyasitavat and D. Hoonsopon, “Blockchain characteristics and consensus in modern business processes,” Journal of Industrial Information Integration Vol. 13, pp. 32–39, 2019, https://doi.org/10.1016/j.jii.2018.07.004.

[38] P. P. Ray, “A survey on Internet of Things architectures,” *Journal of King Saud University-Computer and Information Sciences*, Vol. 30, No. 3, pp. 291-319, 2018, https://doi.org/10.1016/j.jksuci.2016.10.003.

[39] S. Sebastian, & P. P. Ray, “Development of IoT invasive architecture for complying with health of home,” *Proceedings of I3CS, Shillong*, 2015, pp. 79-83.

[40] G. Sharma, S. Vidalis, N. Anand, C. Menon, & S. Kumar, “A Survey on Layer-Wise Security Attacks in IoT: Attacks, Countermeasures, and Open-Issues,” *Electronics,* Vol. 10, No. 19, 2365, 2021, https://doi.org/10.3390/electronics10192365.

[41] T. Hardjono and N. Smith, “Cloud-based commissioning of constrained devices using permissioned blockchains,” In *Proceedings of the 2nd ACM international workshop on IoT privacy, trust, and security,* May 2016, pp. 29-36, https://doi.org/10.1145/2899007.2899012.

[42] D. Rani and N. S. Gill, “Review of various IoT standards and communication protocols,” International Journal of Engineering Research and Technology, Vol. 12, No. 5, pp. 647-657, 2019.

[43] M. El-Hajj, A. Fadlallah, M. Chamoun, & A. Serhrouchni, “A survey of internet of things (IoT) authentication schemes,” *Sensors*, Vol. 19, No. 5, p. 1141, 2019, https://doi.org/10.3390/s19051141.

[44] C. Luo, L. Xu, D. Li, & W. Wu, “Edge computing integrated with blockchain technologies,” In *Complexity and Approximation*, Vol. 12000, pp. 268-288). Springer, Cham, 2020, https://doi.org/10.1007/978-3-030-41672-0_17.

[45] Y. Li, L. Zhu, M. Shen, F. Gao, B. Zheng, X. Du, S. Liu & S. Yin, “CloudShare: Towards a cost-efficient and privacy-preserving alliance cloud using permissioned blockchains,” In *International Conference on Mobile Networks and Management,* Springer, Cham, 2017, pp. 339-352. https://doi.org/10.1007/978-3-319-90775-8_27.

[46] O. Ali, M. K. Ishak, M. K. L. Bhatti, I. Khan, & K. I. Kim, “A Comprehensive Review of Internet of Things: Technology Stack, Middlewares, and Fog/Edge Computing Interface,” *Sensors*, Vol. 22, No. 3, p. 995, 2022, https://doi.org/10.3390/s22030995.

[47] M. Aazam, & E. N. Huh, “Fog computing and smart gateway based communication for cloud of things,” In *2014 International conference on future internet of things and cloud,* Aug. 2014, pp. 464-470. IEEE, https://doi.org/10.1109/FiCloud.2014.83.

[48] F. Bonomi, R. Milito, J. Zhu, & S. Addepalli, “Fog computing and its role in the internet of things,” In *Proceedings of the first edition of the MCC workshop on Mobile cloud computing,* Aug. 2012, pp. 13-16, https://doi.org/10.1145/2342509.2342513.

[49] S. S. Sarmah, “Application of Block chain in Cloud Computing,” *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, Vol. 8, No. 12, pp. 4698-4704, 2019. http://doi.org/10.35940/ijitee.L3585.1081219.

[50] M. Burhan, R. A. Rehman, B. Khan, & B. S. Kim, “IoT elements, layered architectures and security issues: A comprehensive survey,” *Sensors*, Vol. 18, No. 9, p. 2796, 2018, https://doi.org/10.3390/s18092796.

[51] Rashmi, “IoT (Internet of Things) Concept and Improved Layered Architecture,” International Journal of Engineering Development and Research (IJEDR), Vol. 6, No. 2, pp. 481-484.

[52] F. Li, Y. Shi, A. Shinde, J. Ye, & W. Song, “Enhanced cyber-physical security in internet of things through energy auditing,”. *IEEE Internet of Things Journal,* Vol. 6, No. 3, pp. 5224-5231, 2019, https://doi.org/10.1109/JIOT.2019.2899492.

[53] H. Zhang, & L. Zhu, “Internet of Things: Key technology, architecture and challenging problems,” In *2011 IEEE International Conference on Computer Science and Automation Engineering* , Vol. 4, pp. 507-512, June 2011, IEEE, https://doi.org/10.1109/CSAE.2011.5952899.

[54] R. Ratra, P. Gulia, N. S. Gill, “Evaluation of Re-identification Risk using Anonymization and Differential Privacy in Healthcare,” International Journal of Advanced Computer Science and Applications, Vol. 13, No. 2, 2022, https://doi.org/10.14569/IJACSA.2022.0130266.

[55] S. Madakam, , R. Ramaswamy, S. Tripathi, “Internet of Things (IoT): A literature review,” *Journal of Computer and Communications,* Vol. 3, pp. 164-173, 2015. http://doi.org/10.4236/jcc.2015.35021.

[56] D. Thangavel, X. Ma, A. Valera, H. X. Tan, & C. K. Y Tan, “Performance evaluation of MQTT and CoAP via a common middleware,” In *2014 IEEE ninth international conference on intelligent sensors, sensor networks and information processing (ISSNIP), Apr. 2014,* pp. 1-6. IEEE, http://doi.org/10.1109/ISSNIP.2014.6827678.

[57] E. Rescorla, “The transport layer security (TLS) protocol*,” version 1.3* (No. rfc8446), Aug. 2018.

[58] H. Zhang, & L. Zhu, “Internet of Things: Key technology, architecture and challenging problems,” In *2011 IEEE International Conference on Computer Science and Automation Engineering, June 2011,* Vol. 4, pp. 507-512. IEEE, http://doi.org/10.1109/CSAE.2011.5952899.

[59] A. R. H. Hussein, “Internet of things (IOT): Research challenges and future applications,” *International Journal of Advanced Computer Science and Applications,* Vol. 10, No. 6, pp. 77-82, 2019. http://doi.org/10.14569/IJACSA.2019.0100611.

[60] M. Aboubakar, M. Kellil, & P. Roux, “A review of IoT network management: Current status and perspectives,” *Journal of King Saud University-Computer and Information Sciences,* Vol. 34, Issue 7, pp. 4163-4176, 2022. https://doi.org/10.1016/j.jksuci.2021.03.006.

[61] M. Abu-Elkheir, M. Hayajneh, & N. A. Ali, “Data management for the internet of things: Design primitives and solution,” *Sensors*, Vol. 13, No. 11, pp. 15582-15612, 2013 https://doi.org/10.3390/s131115582.

[62] A. Chahal, P. Gulia, N. S. Gill, “Different analytical frameworks and bigdata model for Internet of Things,” Indonesian Journal of Electrical Engineering and Computer Science Vol. 25, No. 2, Feb. 2022, pp. 1159-1166, https://doi.org/10.11591/ijeecs.v25.i2.pp1159-1166.

[63] Z. Qureshi, N. Agrawal, & D. Chouhan, “Cloud based IOT: Architecture, application, challenges and future,” International Journal of Scientific Research in Computer Science, Engineering and Information Technology, Vol. 3, No. 7, pp. 359-368, 2018.

[64] D. Das, S. Banerjee, U. Biswas, “Cloud-Based Smart IoT Architecture and Various Application Domains,” In: Al-Turjman, F. (eds) Trends in Cloud-based IoT. EAI/Springer Innovations in Communication and Computing. Springer, Cham, 2020, https://doi.org/10.1007/978-3-030-40037-8_11.

[65] A. El Hakim, “Internet of Things (IoT) System Architecture and Technologies,” (IoT) System Architecture and Technologies, White Paper., v1.0, pp. 1-6, 2018 https://doi.org/10.13140/RG.2.2.17046.19521.

[66] H. Qiu, M. Qiu, G. Memmi, Z. Ming, M. Liu, “A Dynamic Scalable Blockchain Based Communication Architecture for IoT,” In: Qiu, M. (eds) Smart Blockchain. SmartBlock 2018. Lecture Notes in Computer

Science(), Vol. 11373. Springer, Cham, 2022, https://doi.org/10.1007/978-3-030-05764-0_17.

[67] M. Hou, T. Kang and L. Guo, “A Blockchain Based Architecture for IoT Data Sharing Systems,” *2020 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, 2020, pp. 1-6, https://doi.org/10.1109/PerComWorkshops48775.2020.9156107.

[68] S. Sharma, A. Parihar, K. Gahlot, “Blockchain-Based IoT Architecture,” In: Raj, P., Dubey, A.K., Kumar, A., Rathore, P.S. (eds) Blockchain, Artificial Intelligence, and the Internet of Things. EAI/Springer Innovations in Communication and Computing. Springer, Cham, 2022, https://doi.org/10.1007/978-3-030-77637-4_10.