RESEARCH ARTICLE

INTERNATIONAL RESEARCH JOURNAL OF MULTIDISCIPLINARY TECHNOVATION

Asian Research Association

DOI: 10.54392/irjmt2433

BCSDNCC: A Secure Blockchain SDN framework for IoT and Cloud Computing

V. Sravan Kumar [a], Madhu Kumar Vanteru [b], Chandu Naik Azmera [c], Karthik Kumar Vaigandla [b, *]

[a] Department of Computer Science and Engineering, Balaji Institute of Technology and Science, Telangana- 506330, India
[b] Department of Electronics and Communications Engineering, Balaji Institute of Technology and Science, Telangana, India.
[c] Department of Computer Science and Engineering, CVR College of Engineering, Telangana-501510, India.
*Corresponding Author Email: vkvaigandla@gmail.com
DOI: https://doi.org/10.54392/irjmt2433
Received: 04-12-2023; Revised: 31-03-2024; Accepted: 12-04-2024; Published: 16-04-2024

Abstract: Rapid progress can be observed in the field of computer network technologies. Blockchain technology(BCT) presents a potentially viable alternative for effectively mitigating performance and security issues encountered in distributed systems. Recent studies have focused on exploring a number of exciting new technologies, including BlockChain (BC), Software-Defined Networking (SDN), and the Internet of Things (IoT). Various technologies offer data integrity and secrecy. One such technology that has been utilized for a number of years is cloud computing (CC). Cloud architecture facilitates the flow of confidential information, enabling customers to access remote resources. CC is also accompanied with notable security dangers, concerns, and challenges. In order to tackle these difficulties, we suggest integrating BC and SDN into a CC framework designed for the IoT. The fundamental flexibility and centralized capabilities of SDN facilitate network management, facilitate network abstraction, simplify network evolution, and possess the capacity to effectively handle the IoT network. The utilization of BCT is widely acknowledged as a means to ensure robust security inside distributed SDN (DSDN) and IoT networks, hence enhancing the efficacy of the detection and mitigation procedures.

Keywords: Blockchain, Cloud computing, Distributed denial-of-service, Distributed systems, Internet of Things, Security, Software-Defined Networking.

1. Introduction

The desire for enhanced network services has prompted the rapid advancement of computer network technologies in response to societal needs. In recent years, there has been a rapid evolution in the operational requirements of devices, as well as the limitations imposed by network connectivity. There has been increased attention from the research communities towards two significant advancements: SDN and BC. These innovations offer numerous prospects for secure and adaptable network management, which are crucial attributes in the swiftly expanding realm of the IoT. These technologies have the potential to be deployed in a variety of scenarios, each with its own set of benefits and downsides. The Rapid 5G wireless data transmission has greatly enhanced the reach and magnitude of the IoT by offering high-speed connectivity and communication capabilities. This enables billions of smart devices to connect to and access the Internet. These intelligent devices with diverse properties, including smart phones, sensors, and virtual reality devices, have resulted in the accumulation of substantial amounts of data [1].

In the last several years, machine learning (ML) has made significant advancements in different domains, including computer vision, pattern classification, and natural language processing. In recent times, there has been an increasing inclination towards the utilization of ML techniques in order to enhance the performance of IoT utilizations. Edge IoT devices transmit their unprocessed data to a distant data centre and conduct training in a centralized manner. This approach presents novel technical obstacles for the IoT network. SDN is considered a reassuring networking model that is compatible with the IoT. Heterogeneous devices possess varying requirements for network routing and forwarding when they engage in data transmission. The requirements can be readily implemented by the SDN network, based on its central design [2]. Switches are configured by controllers using the OpenFlow protocol, hence facilitating a more convenient and cost-effective process for configuration and extension. Switches are solely responsible for the task of forwarding packets. In contrast, within the conventional IP network, the configuration of switches and routers necessitates manual intervention due to their diverse origins from various manufacturers.

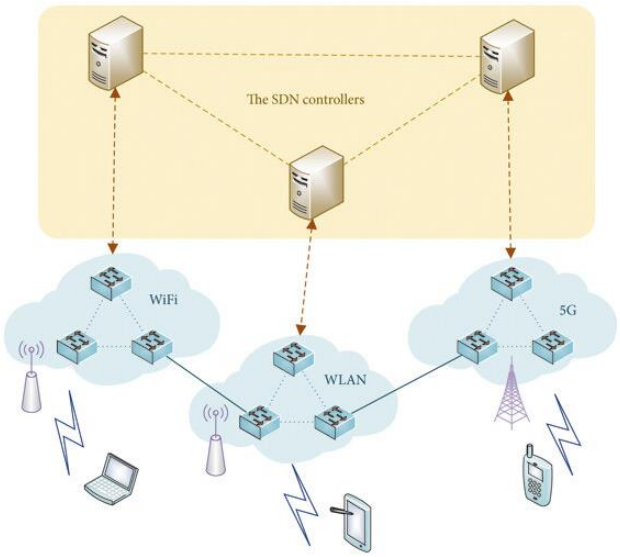

Figure 1. IoT network with support for multiple controllers enabled by SDN

In this approach, the network is partitioned into several domains and a number of controllers are deployed for the purpose of management. Figure 1 depicts the architectural framework of IoT networks with SDN-enabled multi-domains. inside the field of architecture, a diverse range of IoT devices are interconnected with SDN switches via both wireless and cable connections, including but not limited to 5G, WiFi, and WLAN. This heterogeneous IoT device design facilitates seamless communication and integration inside the network. A collective of controllers collaboratively oversee the entirety of the network.

The distributed nature of BCT has led to its recognition as a potential solution for enhancing the security of the IoT. Blockchains are commonly recognized as decentralized databases that distribute data between nodes within a network, ensuring the integrity and security of the stored information on the blockchain [3-4]. These are commonly employed in situations where the data necessitates trustworthiness without the requirement of validation from an external entity. The immutable nature of the stored data is a key characteristic of the blockchain. The latter is securely kept on the interconnected blocks of the chain using cryptographic links, rendering any attempts to modify it without significant resource allocation quite challenging. Blockchain technology has been utilized in several IoT contexts to enhance security [5]. Additionally, it has been applied to address the issue of DDoS attacks in IoT frameworks by using its characteristics of anonymity, decentralization, and auditability [6]. The architecture involves the utilization of IoT devices and SDN switches as data plane nodes. These nodes are responsible for generating traffic towards SDN controllers, which in turn employ machine and deep learning (DL) techniques to identify and mitigate harmful traffic. Consequently, individuals are able to behave in a suitable manner. Learning models often consist of a set of guidelines, methods, or advanced "transfer functions" that can be employed to detect patterns in IoT data pertaining to security issues, as well as to recognize and predict behaviour [7].

Cloud technology is widely recognized as a pivotal facilitator of innovation within the IT industry in the contemporary interconnected global landscape. CC offers a diverse array of services, including SaaS, PaaS, and IaaS. In addition, cloud services provide the qualities of scalability, flexibility, and reliability, catering to the needs of users as and when required. BCT is a distinct technological innovation that places a primary emphasis on enhancing security measures. As a result, blockchain technology has generated significant attention, particularly within the banking industry and other domains where ensuring data security is of utmost importance. Blockchain technology, when combined with the implementation of secret sharing security measures, has the potential to enhance data security in cloud services. In addition, BCT aids in the identification of harmful activities by implementing mechanisms to detect potentially questionable sources. In order to optimize resource allocation, SDN can serve as a viable option by effectively monitoring network traffic and accurately estimating network bandwidth. The integration of novel developing technologies plays a pivotal role in safeguarding data and enhancing the efficiency of cloud operations. The aforementioned study leads us to propose an architectural framework for CC that incorporates distributed and secure blockchain-based software-defined networking (BCSDN) control mechanisms. A distributed blockchain technology (DBCT) effectively ensures dependable and efficient security measures, catering to both private and public needs inside the cloud computing environment.

2. Back ground and Related works

Mobile Cloud Computing (MCC) represents a significant advancement in computing and is considered a viable solution for overcoming challenges by

transferring applications to cloud infrastructure that offers greater resources. This approach has the potential to enhance users' processing capabilities, extend battery life, and reduce latency. The cloud infrastructure provides additional resources, including wired-bandwidth, calculation of power, and storage, on demand. The primary obstacle to the effective implementation of MCC is the energy consumption of users and the significant task processing latency experienced, particularly by cell edge users, while accessing the wide area network for real-time jobs. In recent years, mobile edge computing (MEC) has gained popularity as a significant complement to MCC in order to effectively address the difficulties at hand. By equipping APs/e-NodeBs with a specific level of processing capabilities, they have the ability to function as edge nodes. This allows for the offloading of computationally intensive tasks to these nodes, resulting in efficient energy conservation and reduced delays. However, it is important to note that this approach is most effective when the computational demands are not excessively high. In recent years, MEC (Multi-access Edge Computing) has garnered significant attention across various disciplines.

To achieve the highest rational total profit for all miners and achieve a suitable equilibrium between the risks and rewards associated with BC mining, the researchers in put forward a strategy to optimise resource pricing and resource allocation concerns [8]. They also introduced a deep reinforcement learning (DRL) algorithm to determine the minimal solution considering the uncertainties posed by wireless channel constraints [9-10]. In this system transactions are generated by IoT devices, while MEC nodes located at base stations function as BC nodes and are potential candidates for committee membership [11]. The authors present a proposal for a secure framework for resource sharing and transactions in fog computing (FC) networks, utilizing BC technology. Additionally, they address the issue of requester and provider matching by employing a DRL algorithm.

3. Internet of Things (IoT)

The concept of the IoT, as well as its broader iteration known as the Internet of Everything (IoE), is a relatively recent development. The aforementioned development is widely regarded as a significant technological and economic advancement within the realm of emerging information technology and communication [12]. The IoT lacks a universally agreed-upon definition; however, it is commonly understood as an expansion of the existing Internet infrastructure to encompass all items capable of direct or indirect communication with electronic devices that are interconnected with the Internet. According to the ITU, the IoT is characterized as a worldwide framework that facilitates advanced services by connecting objects, whether they are physical or virtual, using existing or developing interoperable information and communication technologies. IoT devices commonly consist of sensor nodes, RFID (Radio Frequency Identification) tags, and wireless communication devices that are interconnected within a smart environment and connected to the Internet. These devices exhibit a wide range of variations and have become extensively utilized in several aspects of daily existence. The rapid advancement of interconnected devices with diverse attributes necessitates the evolution of future networks towards novel architectures. This adaptation is crucial to accommodate the growing volume of traffic and to assure the security of these networks. The contemporary internet landscape is plagued by the persistent challenge of security, owing to the escalating prevalence of sophisticated security breaches that necessitate effective countermeasures. Furthermore, the management of security assaults in the context of the IoT poses significant challenges. This is primarily attributed to the limited energy storage, data storage, and processing power inherent in IoT devices. Consequently, the conventional network security mechanisms that rely on firewall and intrusion detection/prevention systems (IDS/IPS) are not well-suited for addressing the security concerns associated with IoT [13]. The concept of the IoT is straightforward; nevertheless, numerous challenges arise due to the limited capability of linked devices to manage the communication and processing requirements of various applications. The IoT architecture that is frequently employed in SDN solutions, as represented in Figure 2, is widely utilized.

3.1 Distributed denial of service (DDoS) attack in IoT

The topic of discussion pertains to DDoS attacks within the realm of the IoT. IoT networks are susceptible to a diverse array of security vulnerabilities, encompassing malware, ransomware, phishing assaults, and DDoS attacks. Malicious software, commonly referred to as malware, has the capability to exploit vulnerabilities present in IoT devices. This exploitation can result in unauthorized access being obtained either to the compromised item itself or to other interconnected components within the network. Ransomware assaults encompass the process of encrypting data on IoT devices, which might yield particularly severe consequences within IoT networks. Phishing attacks have the potential to exploit vulnerabilities in IoT devices or facilitate the initiation of other forms of assaults, including but not limited to DDoS attacks. DDoS attacks targeting IoT networks exhibit distinct characteristics when compared to other forms of IoT assaults. The phenomenon can encompass a significant quantity of compromised devices, so endowing them with the ability to produce substantial volumes of network traffic.

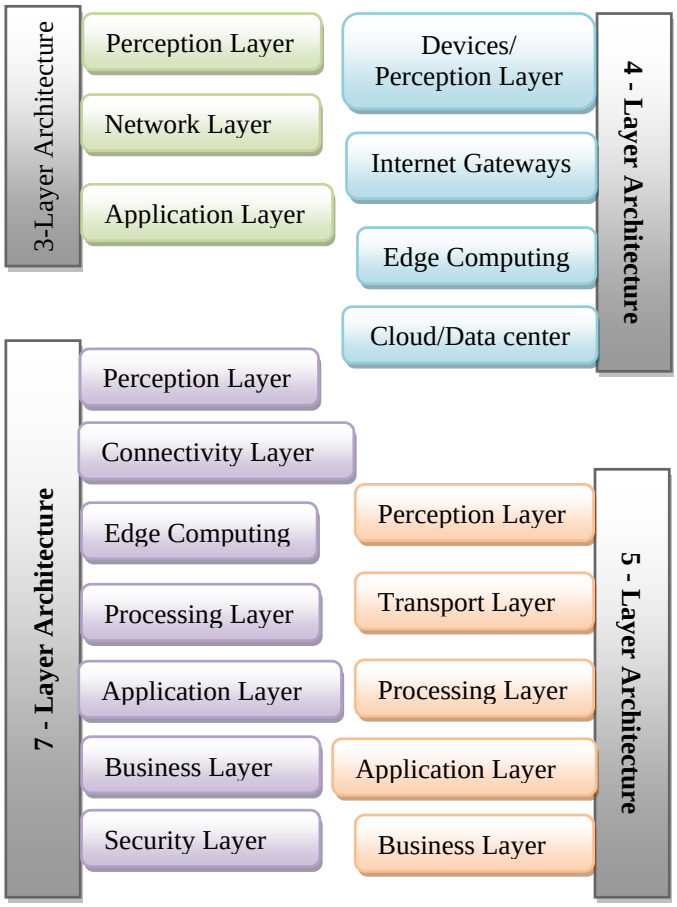

Figure 2. IoT Architecture

This phenomenon can potentially increase the challenges associated with detection and mitigation, consequently leading to extensive disruptions in network services. In contrast to other forms of IoT attacks that primarily aim to pilfer data or assume control over devices, DDoS assaults inside IoT networks possess the capacity to directly affect the accessibility of network services and devices. This can result in substantial disruptions to commercial operations or even essential infrastructure. DDoS assaults on IoT networks frequently entail the utilization of botnets, which are collections of infected devices that can be manipulated from a remote location by the perpetrator.

4. Software Defined Networking (SDN)

This section provides a concise introduction to SDN, followed by an analysis of the advantages and drawbacks associated with the integration of SDN technology into networking topologies. The fundamental structure of the SDN architecture is primarily delineated into three distinct components: The figure presented in Figure 3 illustrates the three distinct planes inside a system: the data, control, and application planes. SDN encompasses the utilization of interfaces that facilitate communication between devices operating within the control and the data planes. These interfaces facilitate communication between devices within a network. The primary objective of East-West application programming interfaces (APIs) is to facilitate the transfer of information across controllers, regardless of whether they belong to the same or separate organizations. Northbound APIs play a crucial role in enabling communication between network applications or services and controllers. These APIs serve various functions, including network security, management, and more. In contrast, southbound APIs facilitate the exchange of information between the controllers and data plane devices, including routers, physical switches, and virtual switches.

The OpenFlow protocol, as in [14], is widely recognized as the dominant standard for facilitating communication between the control and data planes. SDN not only streamlines network operations but also effectively mitigates the expenses associated with network administration. These benefits are offered by its programmable, centralized, vendor-neutral, and adaptable qualities. SDN is a network management methodology that operates by segregating the data plane from the control plane. The Open Networking Foundation provides a definition of SDN that encompasses three distinct planes for the control of a network infrastructure. The data plane is comprised of network devices such as routers and switches, which are responsible for the transmission of frames and messages.

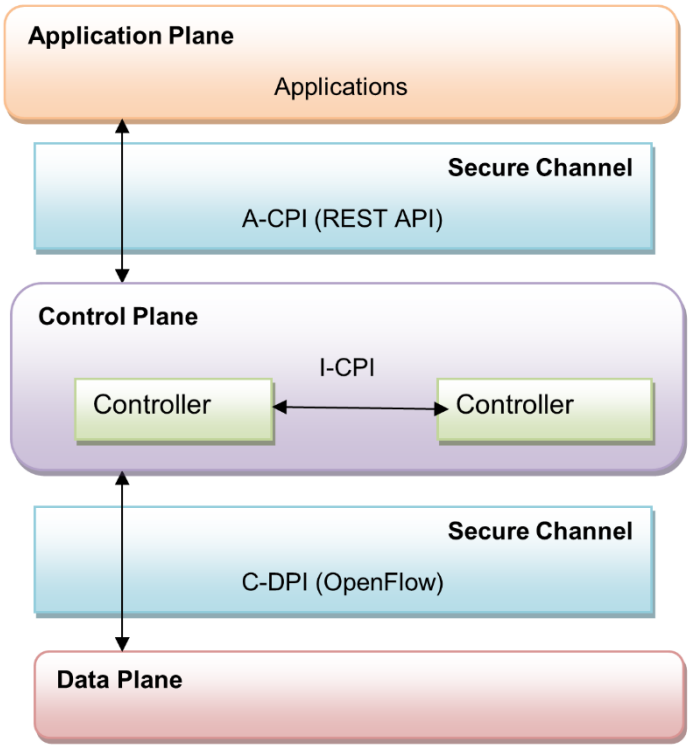

Figure 3. SDN architecture

These devices exhibit a deficiency in intelligence as they rely solely on the information contained inside their flow tables to determine their actions. The application plane is comprised of several software components that are tasked with executing operations that were traditionally performed by network devices, such as routing algorithms, firewalls, and load balancers. The programme is responsible for making the decisions that lead to the creation of entries in the flow tables. Information technology (IT) professionals are required to collaborate with various network hardware components such as switches, routers, and other devices. Additionally, they should possess the capability to modify ACLs, VLANs, and other related procedures. Furthermore, as industry expectations and consumer requirements continue to evolve on a daily basis, it becomes imperative for software developers, suppliers, and enterprises to actively participate in the implementation of novel services and functionalities. However, the dependence of enterprises on suppliers poses a barrier that hinders their ability to develop novel network applications and systems for their networks, mostly due to the extended production cycle of network hardware. As a result, contemporary data centres, suppliers, and organizations necessitate network designs that are more agile and adaptable.

4.1 DDoS Attack in SDN

The architecture and structure of SDN are associated with certain characteristics. The design aspects of this network topology distinguish it from typical ones. The qualities of SDN are advantageous in swiftly and efficiently protecting networks with enhanced adaptability. Nevertheless, the emergence of security problems in SDN can be attributed to a range of architectural errors. Consequently, there exist two methods to classify the design components of SDN. Therefore, there exist certain factors that contribute to the resilience of SDN against DDoS attacks, while other characteristics may potentially expose it to vulnerabilities. This section focuses on elucidating the distinguishing features of SDN when confronted with DDoS assaults. The following discussion highlights the vulnerability features of SDN in relation to DDoS attacks, as well as the specific target points of security concerns.

DDoS attacks are exhibiting an escalating trend in terms of their scale, frequency, intensity, and complexity on conventional networks. Nevertheless, SDN possesses a range of capabilities that can partially alleviate the impact of DDoS attacks. These capabilities include: (a) a holistic view of the network, (b) segregation of the control and data planes, (c) software-based analysis of traffic, (d) network programmability, and (e) the ability to update dynamic network policies. The enhanced security of the network is attributed to the utilization of a centralized control manager in the SDN network design. This allows for remote resolution of any disputes, thanks to the global transparency of the network. Additionally, the capability to adjust traffic forwarding rules in real time further contributes to the network's heightened security.

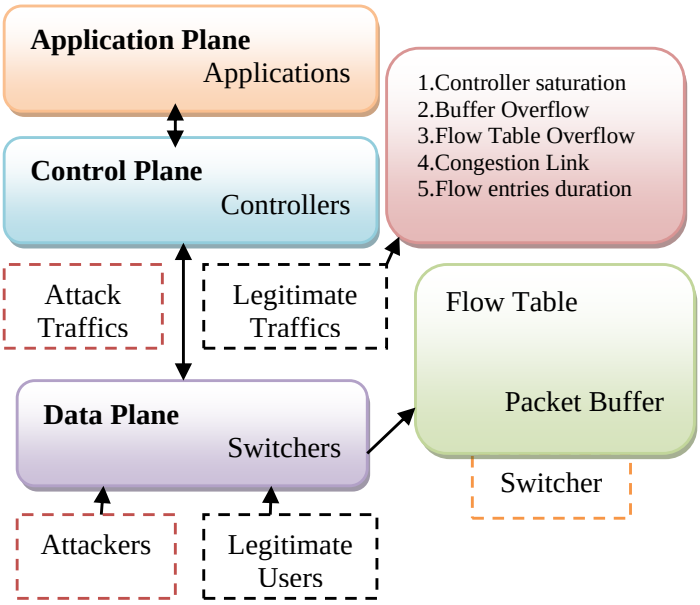

Figure 4. DDoS Attacks in a Software-Defined Network

Furthermore, the concentration of control in the controller, along with its public accessibility, gives rise to potential security issues, such as DoS and DDoS attacks. Both the single point of failure and single point of network failure could potentially be attributed to the SDN controller. The utilization of SDN technology on a consistent basis is expected to result in an exacerbation of security concerns.

DDoS assaults can be primarily categorized into two types: bandwidth depletion and network resources depletion, with the main objective of overwhelming the targeted network. Various attacks can target the data, control planes, and interfaces connecting these planes. The design of the SDN is being compromised by these attacks, rendering its maintenance equally challenging to that of a traditional network architecture. The list provided comprises many attacks that exploit the vulnerabilities of SDN architecture [15]. Figure 4 illustrates the spread of these assaults across several levels.

5. Blockchain Technology

We begin with a brief introduction of BC technology and its applications in networking topologies, and then we move on to a review of its advantages and disadvantages. BC is a database system that primarily focuses on storing data that is limited in size, often consisting of transaction records inside a given system [3-4]. The records are encrypted on an individual basis in order to maintain both security and anonymity. Additionally, all network nodes that are involved in the blockchain consensus agree on the authenticity of each record, thereby ensuring unanimous agreement on outcomes and fostering a sense of confidence. The advent of Bitcoin coincided with the emergence of BCT. Bitcoin is a type of virtual currency that was first established in 2008 by an individual using the pseudonym "Satoshi Nakamoto." The author released a scholarly document titled "Bitcoin: A Peer to Peer Electronic Cash System," in which the concept of direct online payment between two parties without the involvement of intermediaries is presented [16]. The primary purpose of this electronic cash system is to address the issue of double-spending, which arises from the inherent duplicability and potential for multiple uses of digital currency. The resolution to this issue is establishing a secure connection between each transaction, ensuring that they cannot be tampered with. The utilization of the public ledger serves the purpose of establishing a secure and unalterable connection between transactions. By utilizing this ledger, a network possesses the capability to authenticate the transaction history provided by the user for payment and ascertain that the coin in question has not been previously utilized.

When examining the relationship between BC and Bitcoin, it can be observed that Blockchain serves as a technology utilized by numerous cryptocurrencies, including Bitcoin, to facilitate secure and anonymous transactions. However, it is important to note that blockchain operates on a transparent system, whereas Bitcoin relies on the concept of anonymity. Bitcoin is commonly utilized for conducting transactions via the internet, whereas blockchain technology facilitates the transfer of many types of data and rights. The utilization of blockchain technology encompasses a wider range of applications, whereas Bitcoin is mostly confined to the exchange of digital money. Blockchain is commonly defined as a transparent and distributed system of ledgers, wherein digitally signed transactions are organized into blocks. Every block consists of a cryptographic hash value that establishes a connection between blocks, a timestamp, and transaction data. The design of BC data inherently prevents any modifications.

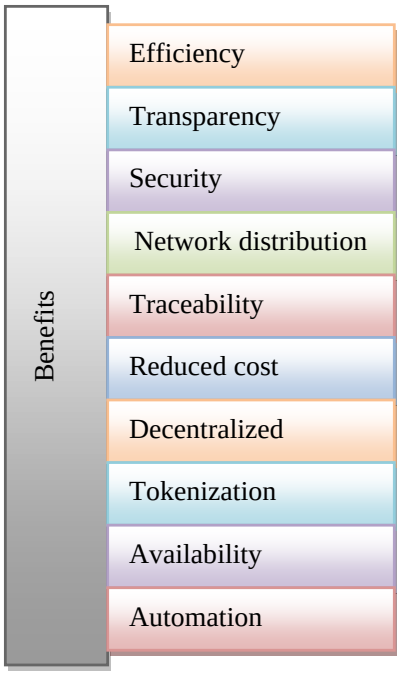

Figure 5. Benefits of BC

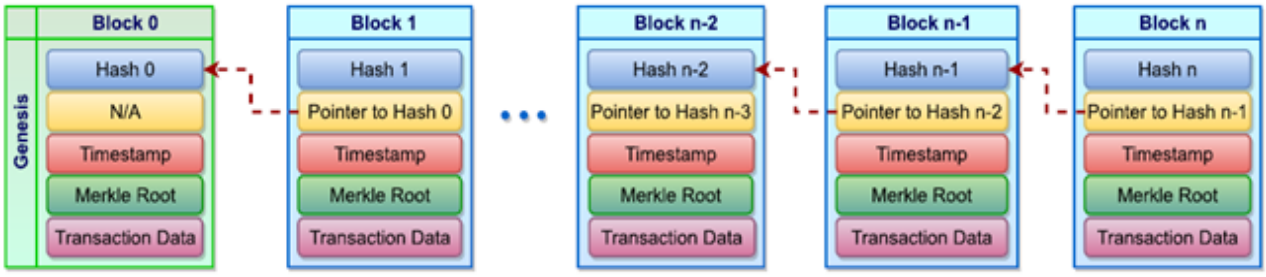

Figure 6. BC Overview with block data structures

The system in question is a decentralized and transparent ledger designed to efficiently and permanently document transactions between many participants. The advantages of BC are illustrated in figure 5.

The blockchain is a resilient digital ledger used to record economic transactions, capable of being configured to store not only financial transactions but also a wide range of valuable assets. The user's text does not contain any information. The implementation of blockchain technology eliminates the necessity for government intervention and ensures a complete absence of fraudulent activities through the process of consensus validation. By removing the participation of intermediaries, instantaneous transactions can be conducted without incurring transaction costs. Despite the numerous positives, blockchain technology does has certain drawbacks, one of which is its inherent volatility. The potential for an escalation in societal criminal activities arises from the utilization of anonymous transactions that cannot be traced by external entities or nodes inside the network.

Figure 6 depicts a schematic illustration of the BC structure at a higher level. In general, every block consists of several components including a sequence number, a hash value, a reference to the previous block through its hash value, a timestamp, and a collection of transaction data. The primary objective is to uphold an unchangeable and protected record of these transactions. The hash pointer data serves the purpose of establishing the position of a block within the chain. The local hash, commonly derived from the hash of a Merkle tree root, is employed to verify the integrity of the information included by the transactions stored in the block. Figure 7 displays the uses of BC, whereas Figure 8 illustrates various types of BC.

There are multiple iterations of blockchain technology, and a categorization of these iterations is provided in [1]. The initial iteration is a publicly accessible blockchain, serving as an inclusive platform that enables participation, transaction execution, and mining for all individuals. The term "permission less" is used to describe this system, as it lacks any access restrictions and grants all participants the ability to both read and write transactions.

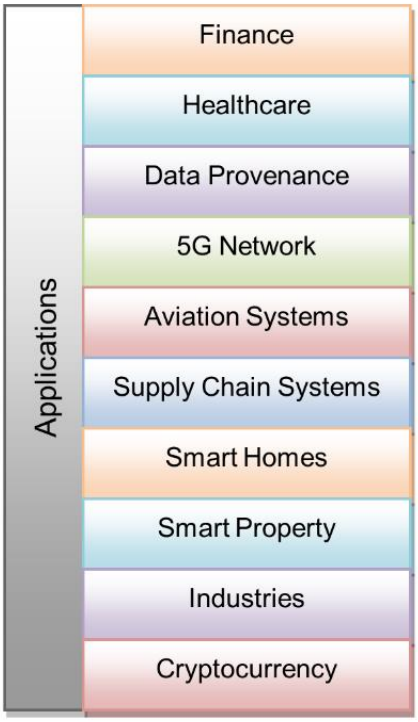

Figure 7. Applications of BC

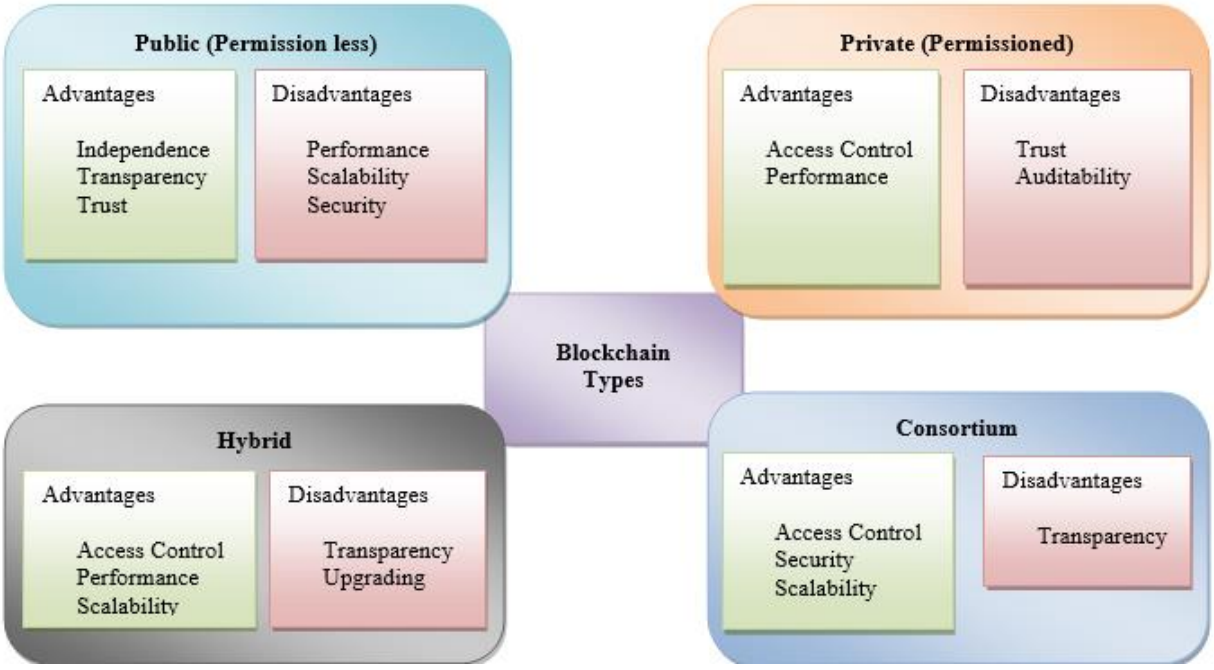

Figure 8. BC - types

Private blockchains, also known as permission blockchains, were created to facilitate the private sharing and transfer of data. In these blockchains, the process of mining is regulated by designated hosts, typically an organization, and access to the blockchain is limited to particular entities. The hybrid solution under consideration is the consortium blockchain, characterized by a combination of private and public elements. In this framework, a certain group of specified nodes assumes the responsibility of validating blocks and establishing consensus. Furthermore, these nodes possess the authority to determine the inclusion of other nodes inside the network and grant permission for mining activities.

5.1 BC with SDNs

The transformation of IoT sensor data from the level of the sensors to the SDN environment can be facilitated by employing an SDN-intelligent gateway. SDN effectively filters and handles data from both the network's control plane and data plane, ensuring efficient data management.

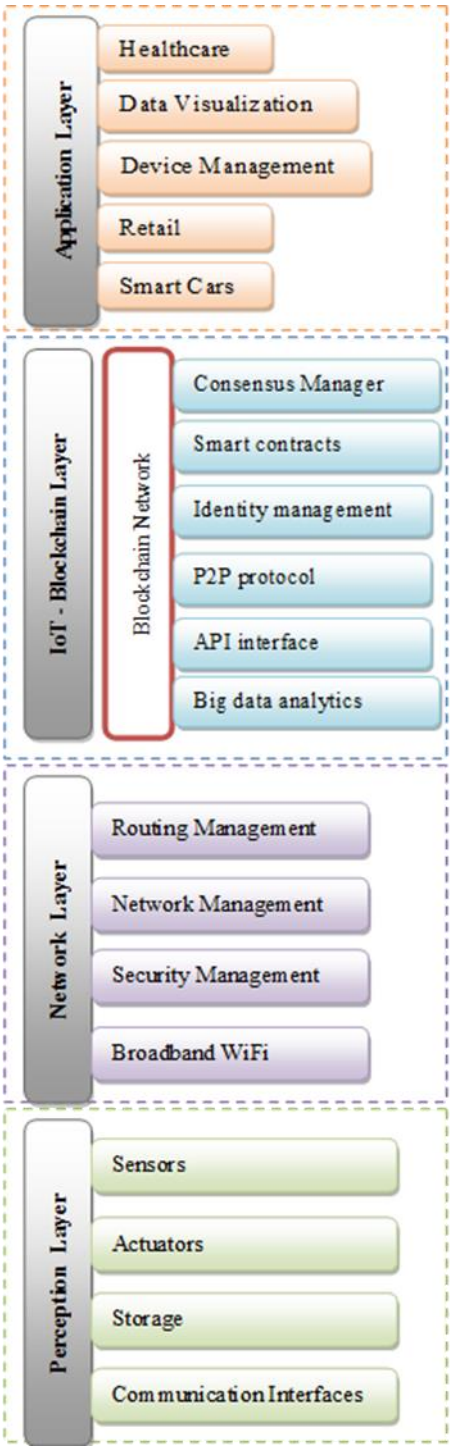

Figure 9. Architecture of IoT with blockchain

In addition, a VLC is employed to build a connection between the SDN environment and the BC technology. The virtualization technology provided by this layer facilitates a strong connection through two methods, as seen in Figure 9. Sharma et al. introduced the DistBlockNet concept inside the framework of IoT architecture [17]. This platform presents two notable benefits for diverse networking technologies, including SDN and BC. The proposed solution put out by the authors involves the utilization of the BC technique to update the flow rule table, with the formalization of said table. Additionally, the researchers conducted measurements using various metrics, and the subsequent analysis revealed a more favourable outcome in comparison to the remaining fragment. The DBCSDN design, incorporating Network Function Virtualization (NFV), was proposed by Rahman *et al.* [18] for the purpose of enabling smart city functionalities. The researchers employed a Byzantine fault-tolerant technique in order to attain a heightened level of security and privacy. In addition, the authors introduced a methodology for the selection of the cluster head that minimizes energy consumption. The authors assessed the performance of the networks by analyzing metrics such as throughput and packet arrival rate (PAR). In a separate study, Navid *et al*. [19] introduced an innovative

framework that integrates SDN and BC technologies to tackle the issues posed by the IoT in upcoming 5G telecommunication networks.

5.2 BCT with IoT

BC is a distributed ledger that does not consider the parties involved in transactions. BC is part of industrial IoT, which enhances system confidentiality efficiently. Industrial IoT requires extensive data sharing, currently done on the cloud using BC for authentication and encryption/decryption. The IoT credential uses anonymous techniques, and the identity lifecycle is modified to BC for biometric identification in smart industry applications. Huo *et al.* [20] reviewed BC research in IoT and identified future problems. In addition, they evaluated the technical specifications of the technology. Figure 10 shows a security architecture which combines SDN with Blockchain.

6. Cloud Computing (CC)

In the contemporary digital age, an extensive multitude of websites are hosted on the World Wide Web(WWW). The maintenance of the hosted site requires a stack of servers, resulting in significant expenses. It is imperative that the traffic rate of the servers remains consistent, and it is essential to regularly monitor and manage them. There will be a requirement to employ more personnel for the purpose of organizing and maintaining these servers. Data centers are responsible for the storage of all data. The ongoing dedication to addressing server maintenance concerns, as well as potential employee distractions, may impede our progress towards accomplishing our company objectives. Research issues in CC are illustrated in figure 11. In order to mitigate the challenges associated with maintenance, our organization has decided to implement the utilization of CC. CC is a widely used approach that involves the utilization of a distributed network of distant computers for the purpose of storing, managing, and processing data from various geographical locations throughout the globe. It is employed as a substitute for a localized server or an individual computing device. CC services involve the delivery of data and applications to an organization's devices via the internet and also offers numerous benefits by integrating data centres, resources, and servers. These services operate under a pay-per-use model, as per the established regulations. The services can be accessed globally, enabling enhanced collaboration among employees at a reduced cost. The software residing in the cloud will undergo automatic updates, hence enhancing the cloud's manageability. The service consumer will possess authority over the documents stored in the cloud. Due to the inherent flexibility of cloud data, it is imperative to address the various security and privacy concerns that arise, as well as the susceptibility to potential assaults. In instances where there is a significant influx of users, it is possible for the cloud infrastructure to have periods of reduced availability. Figure 12 represents applications, and figure 13 represents disadvantages of CC.

6.1 BC Based Security for CC

CC is a paradigm that facilitates the provision of hardware, software, storage, and other resources as services through distant means, specifically via the internet. Various design approaches have been devised based on the specific application situation and business objectives, such as the restriction of cloud resource access exclusively to personnel inside an enterprise.

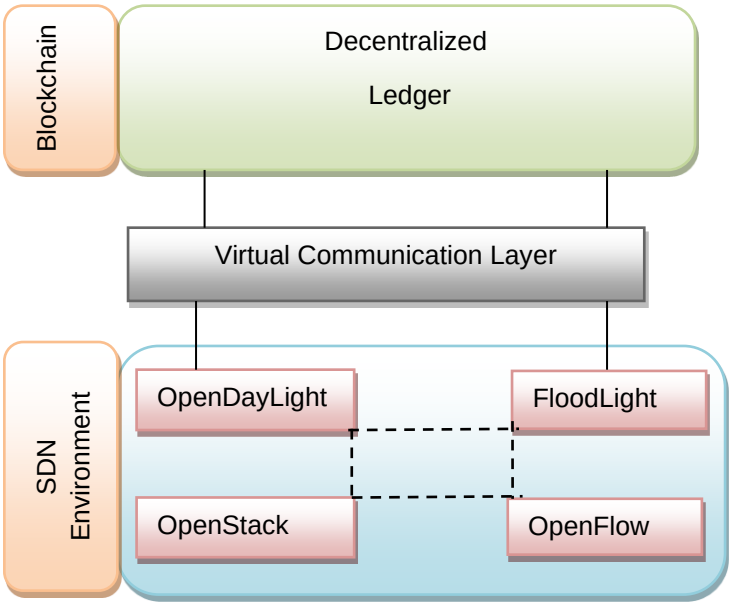

Figure 10. A security design that combines SDN and Blockchain

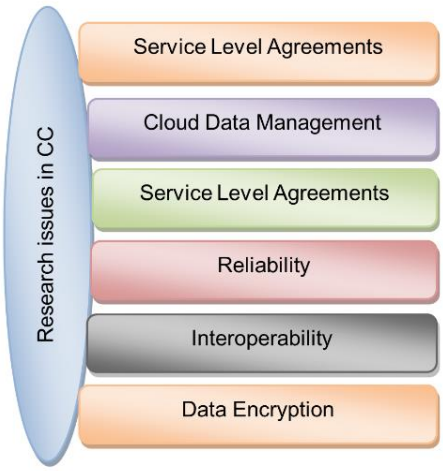

Figure 11. Research issues in CC

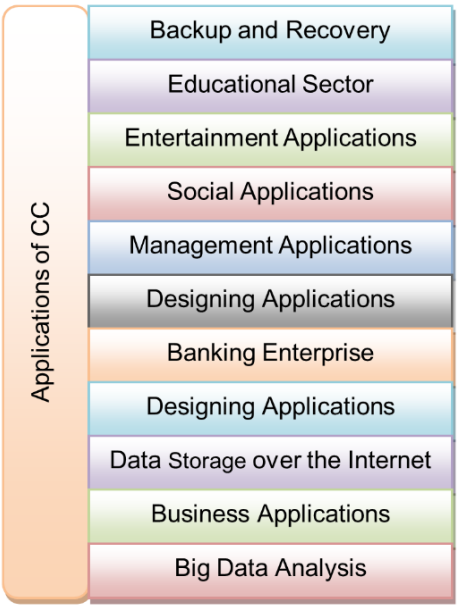

Figure 12. CC-applications

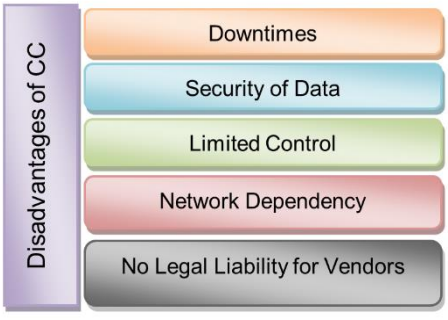

Figure 13. Disadvantages of CC

According to the findings presented in Figure 14, various deployment models exist, including personal, public, hybrid, and community models. The research questions pertaining to BCT in CC were initially introduced by Gaetani *et al.* [21]. The researchers provided precise and sophisticated solutions to address the inquiries pertaining to the European project SUNFISH. Park *et al.* [22] introduced the concept of BCT and explored potential prospects for technological advancements in cloud computing. The authors have introduced a comprehensive security methodology for cloud computing, which encompasses multiple aspects and is rooted in the concept of business continuity.

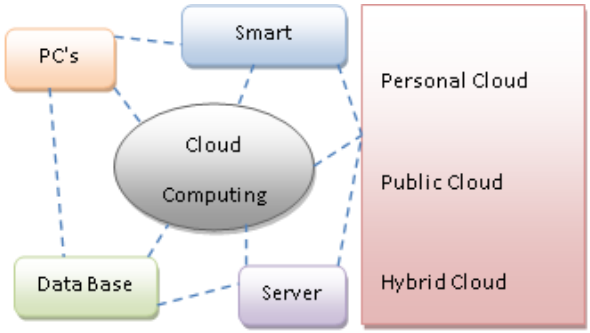

Figure 14. Cloud computing: architecture

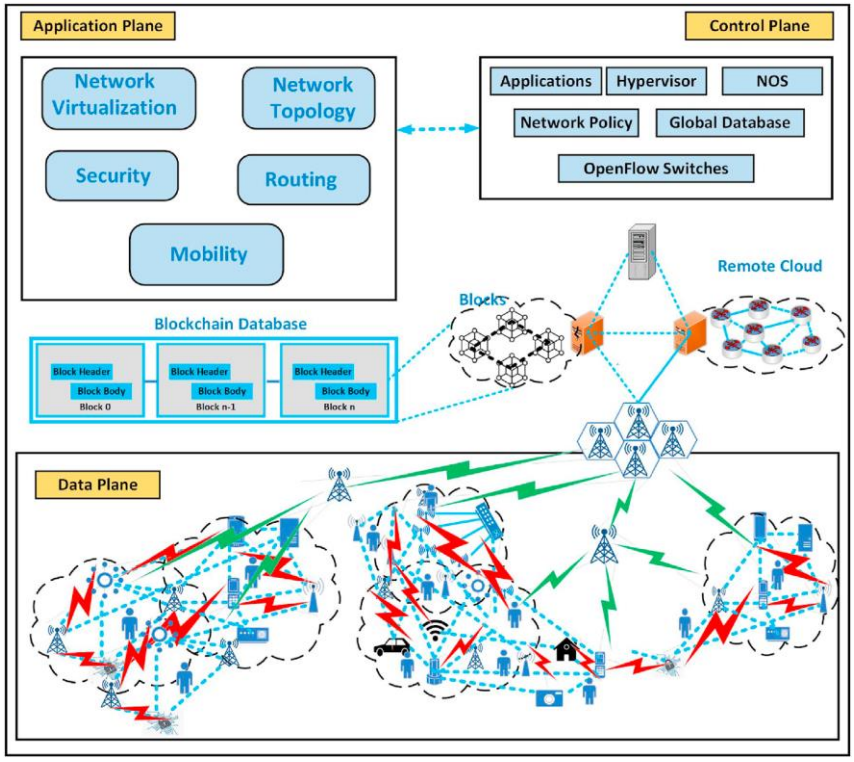

Figure 15. Convergence of BC-SDN

In a previous study [23], blockchain technology was employed to offer a range of security services to forwarding devices in the IoT. This article provided a description of CC and edge transparent computing technologies. In addition, the authors engaged in specific discussion regarding the implementation of BC procedures as a means to protect IoT networks from unauthorized threats. In a previous study [24], Sharma et al. presented a novel decentralized cloud platform based on blockchain (BC) technology. This platform incorporates fog nodes equipped with a SDN enabled controller, strategically positioned at the network's edge. The authors bring up a compelling integration of FC, SDN, and BCT. In addition, the authors introduced a proposed framework that is specifically engineered to facilitate robustness, immediate data acquisition, improved capacity for growth, safeguarding measures, and adaptability, all while ensuring minimal time delay. The researchers also assessed other characteristics, including throughput, response time, and accuracy in the detection of real-time threats. Furthermore, alongside the conventional BC, the implementation of artificial intelligence (AI) based BCT was employed within the system to enhance cyber-physical security.

7. Proposed Distributed BC-SDN based CC (DBCSDNCC) architecture

In order to enhance the security and dependability of cloud applications, we present an architecture framework that is distributed and reliability, based on BC technology. This framework effectively executes the necessary activities, as illustrated in figure 15.

7.1 SDN approaches for Data Extraction in IoT

Numerous intelligent sensor-based devices possess the capability to transmit sensor data via SDN-enabled gateway controllers, encompassing firewalls, switches, routers, and diverse data storage devices.

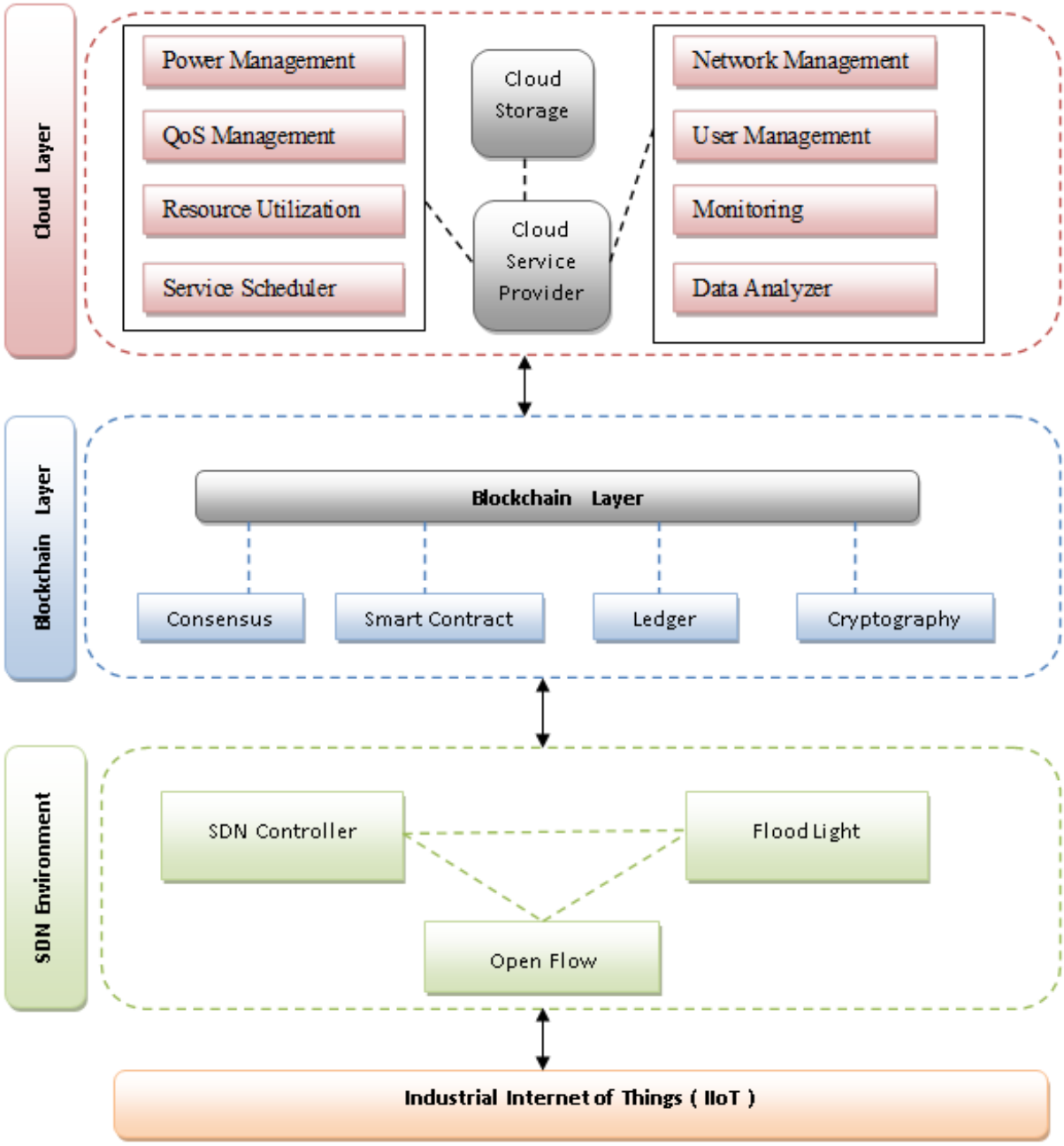

Figure 16. Proposed DBcSDNCc Architecture

The utilization of sensor data inside a SDN-based BC network can be conducted in a safe manner to support a range of operational activities. In addition, the use of sensor data plays a crucial role in enhancing the operational efficiency within the distributed architecture of the intelligent Industrial IoT ecosystem. The SDN architecture can be partitioned into multiple planes based on sensor data, encompassing the data, control, and implementation planes. Data plane operations encompass the process of gathering sensor data within an SDN environment, utilizing various controllers, protocols, and platforms such as OpenDayLight, OpenFlow, and OpenStack. The inclusion of this layer facilitates the effective acquisition of sensor data through the utilization of SDN within the intelligent IIoT system.

7.2 Secured DBC-SDN

A blockchain (BC) is a type of ledger or data system that allows for the incorporation of numerous features into a distributed or decentralized, temperature-resistant facility, as illustrated in Figure 16. The identity node of the miner and the asking node of the general members serve as the basis for this. Concurrently, BC has the potential to offer efficient access control and enhance security measures in system architecture. Essentially, blockchain technology functions as a tamper-proof digital ledger for the purpose of recording transactions. Nevertheless, it fails to retain all user activity within a centralized store or database. Moreover, each user at the user end utilizes identical storage. In order to maintain a consensus system, all transaction activities and updated copies are stored in a centralized

location. In the context of blockchain technology, each block has the capability to effectively process many transactions within the smart IIoT environment. In addition, each block is connected through a hash chain and encompasses comprehensive data including a timestamp, records, existing hashes, preceding data, and non-conflicting transactions. Based on the aforementioned concept, it is our contention that BC is a suitable solution for effectively managing access control within the cloud environment under consideration. The present methodology is structured in the subsequent manner: the security and access policy are delineated.

7.3 Methods for Mitigating Attacks in Cloud Environments using a BC-SDN Architecture

SDN has a significant susceptibility to cyber-attacks. Several types of assaults are frequently encountered in the realm of CC, including DDoS attacks, DoS attacks, flooding attacks, and several more. These attacks have become increasingly prevalent due to the critical role that the cloud environment plays in facilitating various advancements. The cloud storage scenario has increasingly been a focal point for numerous attackers seeking to launch attacks. The duration of the system's downtime may be prolonged due to the occurrence of these assaults. Additionally, we have presented a methodology for the identification and prevention of such attacks in order to mitigate this issue and enhance the operational efficiency of the device. The utilization of the BC mechanism has been employed to provide support for SDN controllers. The controller will identify potential attacks in accordance with the provided instruction. The subsequent concern pertains to the act of evading or protecting against an intruder subsequent to their identification. The data packets in the BC method are transmitted in a sequential manner, with each block being broadcast individually. In this scenario, just the approved blocks are eligible for inclusion, while any unauthorized blocks are excluded from the blockchain.

7.4 Management of CC and Related Services

The proposed architecture improves the functionality of different services inside the cloud computing environment through the use of a distributed BCT. The SDN architecture implemented in British Columbia offers several advantages, including enhanced flexibility, improved accessibility, heightened security, and increased privacy for the retrieval and storage of multiple resources within the cloud computing platform. The suggested architecture lacks better dependability, high stability, a logically centralized controller, and increased load balancing capacity without the use of the SDN approach [23]. The performance of cloud computing resources, specifically SaaS, PaaS, and IaaS, is influenced by the accessibility and availability of services and resources in the cloud, which are ultimately contingent upon internet speed. This performance is optimized when the architectural design, as illustrated in Figure 17, is implemented accurately.

8. Performance Evaluation and Discussion

This section focuses on the examination of the performance of the distributed blockchain based SDN cloud computing (BCSDNCC) concept. The performance of our proposed model has been evaluated through the use of diverse measures, including throughput, PAR, and file transfer operation.

Throughout: In Figure 18, we computed the throughput by considering the quantity of nodes. Currently, a comparison of throughput is being undertaken between OpenFlow based SDN (OFSDN) and DBCSDNCC architecture. The results of this comparison are visually shown in the figure.

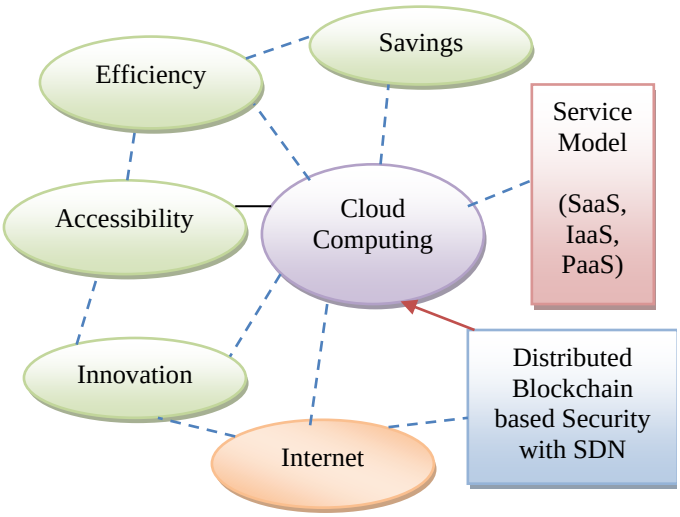

Figure 17. DBC-SDN based CC services

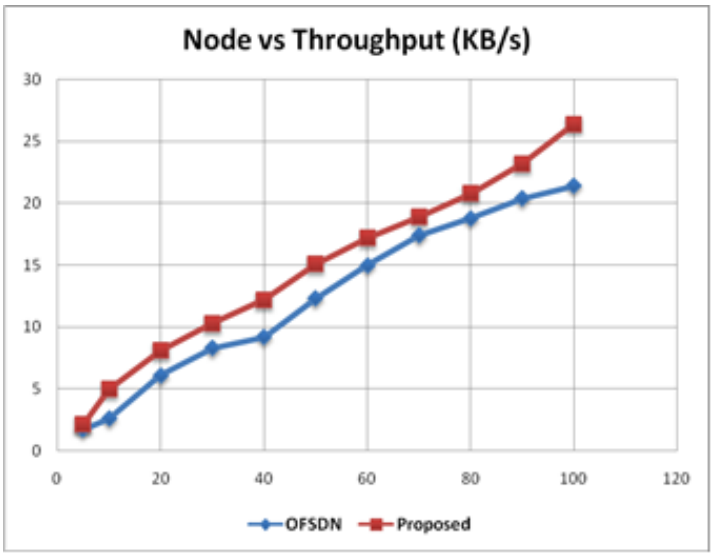

Figure 18. Nodes vs Throughput

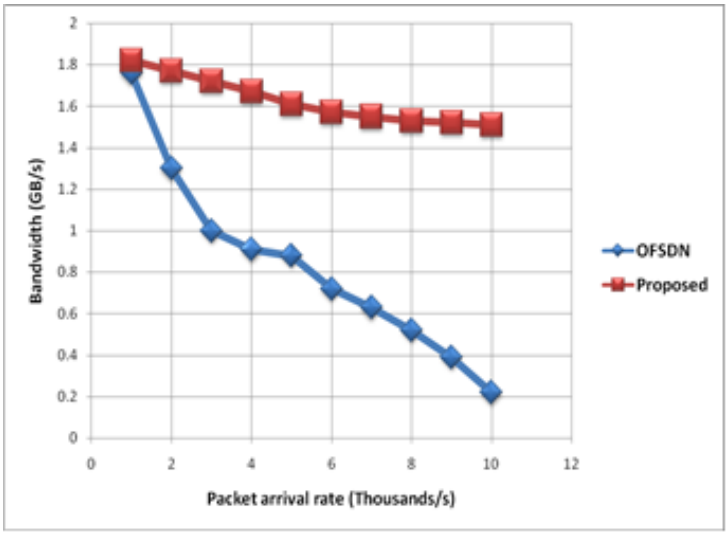

Figure 19. Packet arrival rate vs bandwidth

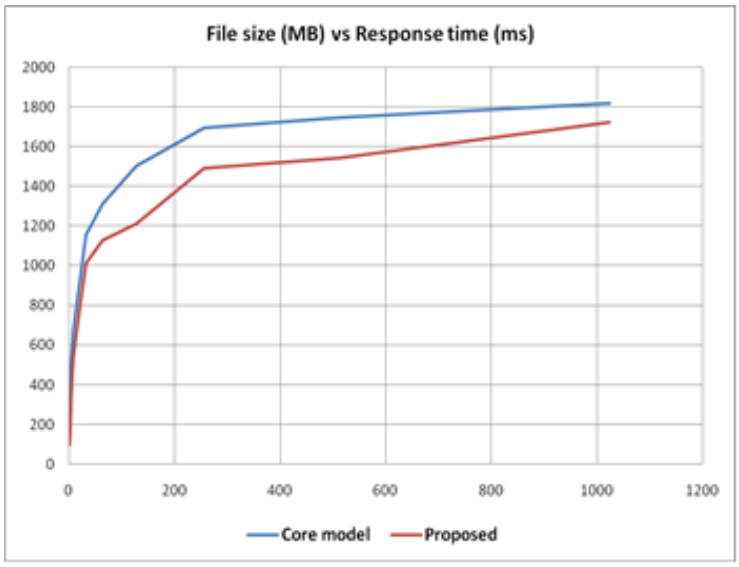

Figure 20. File size vs response time

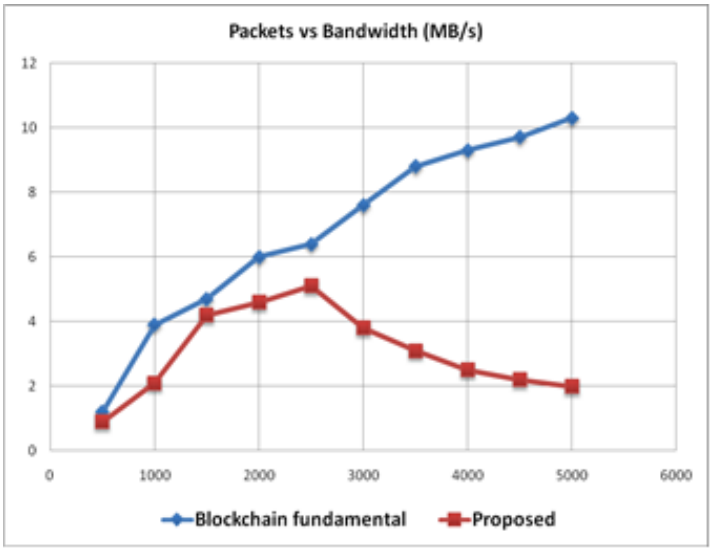

Figure 21. Packets vs bandwidth

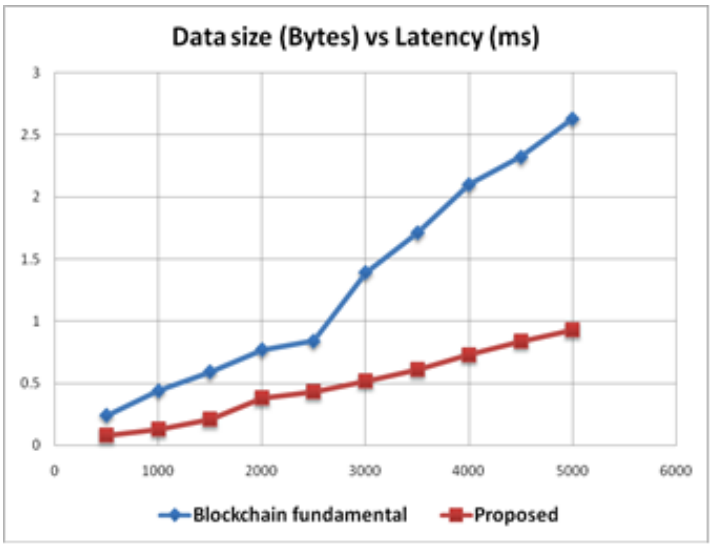

Figure 22. Data size vs Latency

Additionally, it was found that the throughput exhibits a somewhat stable trend as the quantity of nodes is decreased. Nevertheless, it is seen that there is a positive correlation between the number of nodes and the throughput, indicating that an increase in the former leads to a corresponding increase in the latter. In conclusion, a comparative analysis was conducted between our suggested DBCSDNCC framework and a framework that solely relies on OFSDN. The results of this analysis revealed that our proposed scheme exhibits superior performance in comparison to the alternative framework.

8.1 Packet Analysis

Figure 19 illustrates the performance of the system as the number of packets increases. In conclusion, this figure presents a comparison between the bandwidth (gigabytes per second) and the current packet arrival rate (thousands per second), showcasing the outcomes of our suggested system in contrast to an OFSDN solution. It is observed that with OFSDN, there is a significant reduction in bandwidth as the packet rate is increased. In contrast, our provided model demonstrates consistent performance even at heightened attack rates and when subjected to the most severe tested packet, hence substantiating its resilience against abrupt surges in loads resulting from either malicious or intentional actions.

8.2 Response Time

Figure 20 illustrates the performance of file operations for both the core and provided models. The presented data in this graphic illustrates the relationship between response time and file size in file transfer activities. As the file size increases, there is a corresponding increase in the response time. Nevertheless, the proposed model regularly demonstrates a superior response time performance in

comparison to the core model. Furthermore, it was also noted that our model demonstrated the ability to attain significant file sizes in comparison to the current core-based approach.

8.3 Bandwidth

Figure 21 illustrates the comparative analysis between the proposed system and the Blockchain fundamental (BCF) model. Furthermore, the authors took into consideration the use of SDN controllers and the OFSDN in order to construct the intended network. Subsequently, protocol-based rules were employed to quantify the bandwidth of many packets.

8.4 Latency

The performance of the suggested framework is optimal when the number of packets is high. Alternatively, the latency might be represented based on the amount of the data. The suggested system exhibits enhanced responsiveness compared to the BCF paradigm due to its integration with SDN. The relation between data size and latency is illustrated in figure 22.

9. Conclusion

The distinct potentials of SDN, BC, and IoT technologies are attracting significant interest in research fields. Despite the potential synergy and complementarity of SDN, BC, and IoT, there has been less research conducted to exploit the combined benefits of these approaches. This article examines the potential for transformative outcomes resulting from the integration of blockchain technology with CC. The primary focus is on addressing significant problems related to security and performance. The growing prevalence of IoT devices in various aspects of our everyday lives and extensive service sectors necessitates a heightened focus on ensuring the security and effective management of the substantial volumes of data they produce. SDN has emerged as a viable method for effectively managing the network traffic created by IoT devices. Concurrently, BCT provides a secure and decentralized platform for facilitating data sharing and trust management. In recent times, there has been a notable surge in the demand for cloud computing services, particularly within the context of the innovative IoT ecosystem, resulting in a significant rise in the number of clients availing such services. However, cloud computing encounters several security dangers, issues, and obstacles. In order to mitigate these potential risks, scholars have put forth a variety of recommendations and methodologies. This article presents the "DBCSDNCC" architecture as a means to augment the security and secrecy of CC methodologies when used to IoT applications. In our forthcoming research endeavours, we aim to proficiently use this architectural approach across a range of applications, including the realms of FC and EC environments. The suggested system paradigm would be increasingly dependent on technologies such as SDN, IoT, and BC.

References

[1] D. Puthal, N. Malik, S.P. Mohanty, E. Kougianos, G. Das, Everything you wanted to know about the blockchain: Its promise, components, processes, and problems. IEEE Consumer Electronics Magazine, 7(4), (2018) 6–14. https://doi.org/10.1109/MCE.2018.2816299

[2] Z. Shah, I. Ullah, H. Li, A. Levula, K. Khurshid, Blockchain based solutions to mitigate distributed denial of service (ddos) attacks in the Internet of Things (IoT): A survey. Sensors, 22, (2022) 1094. https://doi.org/10.3390/s22031094

[3] R. Yadav, Ritambhara, K.K. Vaigandla, G.S.P. Ghantasala, R. Singh, D. Gangodkar, (2022) The Block Chain Technology to protect Data Access using Intelligent Contracts Mechanism Security Framework for 5G Networks. 2022 5th International Conference on Contemporary Computing and Informatics (IC3I), IEEE, Uttar Pradesh, India. https://doi.org/10.1109/IC3I56241.2022.10072740

[4] K.K. Vaigandla, R. Karne, M. Siluveru, M. Kesoju, Review on Blockchain Technology: Architecture, Characteristics, Benefits, Algorithms, Challenges and Applications. Mesopotamian Journal of CyberSecurity, 2023, (2023) 73–85. https://doi.org/10.58496/MJCS/2023/012

[5] A. Heidari, N.J. Navimipour, M. Unal, A Secure Intrusion Detection Platform Using Blockchain and Radial Basis Function Neural Networks for Internet of Drones. IEEE Internet Things Journal, 10(10), (2023) 8445-8454. https://doi.org/10.1109/JIOT.2023.3237661

[6] R. Chaganti, B. Bhushan, V. Ravi, (2022) The role of Blockchain in DDoS attacks mitigation: Techniques, open challenges and future directions. arXiv. https://doi.org/10.48550/arXiv.2202.03617

[7] U. Islam, A. Muhammad, R. Mansoor, M.S. Hossain, I. Ahmad, E.T. Eldin, J.A. Khan, A.U. Rehman, M. Shafiq, Detection of distributed denial of service (DDoS) attacks in IOT based monitoring system of banking sector using machine learning models. Sustainability, 14(14), (2022) 8374. https://doi.org/10.3390/su14148374

[8] J. Du, W. Cheng, G. Lu, H. Cao, X. Chu, Z. Zhang, J. Wang, Resource pricing and allocation in MEC enabled blockchain systems: An A3C

deep reinforcement learning approach. IEEE Transactions on Network Science and Engineering, 9(1), (2021) 33-44. https://doi.org/10.1109/TNSE.2021.3068340

[9] F. Fu, Y. Kang, Z. Zhang, F. R. Yu, & T. Wu, Soft actor–critic DRL for live transcoding and streaming in vehicular fog-computing-enabled IoV. IEEE Internet of Things Journal, 8(3), (2020) 1308-1321. https://doi.org/10.1109/JIOT.2020.3003398

[10] Z. Zhang, Q. Zhang, J. Miao, F.R. Yu, F. Fu, J. Du & T. Wu, Energy-efficient secure video streaming in UAV-enabled wireless networks: A safe-DQN approach. IEEE Transactions on Green Communications and Networking, 5(4), (2021) 1892-1905. https://doi.org/10.1109/TGCN.2021.3095315

[11] W. Wu, D. Sun, K. Jin, Y. Sun, P.Si, Proximal policy optimization-based committee selection algorithm in blockchain-enabled mobile edge computing systems. IEEE China Communications, 19(6), (2022) 50–65. https://doi.org/10.23919/JCC.2022.06.005

[12] K.K. Vaigandla, (2022) Communication Technologies and Challenges on 6G Networks for the Internet: Internet of Things (IoT) Based Analysis. IEEE, 2nd International Conference on Innovative Practices in Technology and Management (ICIPTM), India. https://doi.org/10.1109/ICIPTM54933.2022.9753990

[13] M.A. Karne, M.R. Karne, M.V.K. Kumar, & A. Arunkumar, Convolutional Neural Networks for Object Detection and Recognition. Journal of Artificial Intelligence, Machine Learning and Neural Network, 3(2), (2023) 1-13. https://doi.org/10.55529/jaimlnn.32.1.13

[14] S. Saraswat, V. Agarwal, H.P. Gupta, R. Mishra, A. Gupta, T. Dutta, Challenges and solutions in software defined networking: A survey. Journal of Network and Computer Applications, 141, (2019) 23–58. https://doi.org/10.1016/j.jnca.2019.04.020

[15] A.L. Yaser, H. Mousa, M. Hussien, Techniques for DDoS Attack in SDN: A Comparative Study. IJCI. International Journal of Computers and Information, 9(2), (2022) 64-73. https://dx.doi.org/10.21608/ijci.2022.133407.1073

[16] C.T.S. Xue, F.T.W. Xin, Benefits and Challenges of The Adoption of Cloud Computing in Business. International Journal on Cloud Computing: Services and Architecture (IJCCSA), 6(6), (2016) 1-15. https://doi.org/10.5121/ijccsa.2016.6601

[17] P.K. Sharma, S. Singh, Y.S. Jeong, J.H. Park, Distblocknet: a distributed blockchains-based secure sdn architecture for iot networks. IEEE Communication Magazine, 55(9), (2017) 78–85. https://doi.org/10.1109/MCOM.2017.1700041

[18] A. Rahman, M.J. Islam, F.A. Sunny, M.K. Nasir, (2019) Distblocksdn: a distributed secure blockchain based sdn-iot architecture with nfv implementation for smart cities. 2nd International Conference on Innovation in Engineering and Technology (ICIET), IEEE, Bangladesh. https://doi.org/10.1109/ICIET48527.2019.9290627

[19] N. Rajabi, & J. Qaddour, SDIoBoT: a software-defined internet of blockchains of things model. International Journal of Internet of Things, 8(1), (2019) 17-26.

[20] R. Huo, S. Zeng, Z. Wang, J. Shang, W. Chen, T. Huang, S. Wang, F.R. Yu, Y. Liu, A comprehensive survey on blockchain in industrial internet of things: motivations, research progresses, and future challenges, IEEE Communications Surveys & Tutorials, 24(1), (2022) 88–122. https://doi.org/10.1109/COMST.2022.3141490

[21] E. Gaetani, L. Aniello, R. Baldoni, F. Lombardi, A. Margheri & V. Sassone, (2017) Blockchain-based database to ensure data integrity in cloud computing environments. Italian Conference on Cybersecurity, Venice, Italy.

[22] J.H. Park, J.H. Park, Blockchain security in cloud computing: use cases, challenges, and solutions, Symmetry, 9(8), (2017) 164. https://doi.org/10.3390/sym9080164

[23] M. Rehman, N. Javaid, M. Awais, M. Imran, N. Naseer, (2019) Cloud based secure service providing for iots using blockchain. IEEE Global Communications Conference (GLOBECOM), IEEE, USA. https://doi.org/10.1109/GLOBECOM38437.2019.9013413

[24] P.K. Sharma, M.Y. Chen, J.H. Park, A software defined fog node based distributed blockchain cloud architecture for IoT. IEEE Access, 6, (2017) 115–124. https://doi.org/10.1109/ACCESS.2017.2757955

Authors Contribution Statement

V. Sravan Kumar : Conceptualization, methodology, software, validation, supervision, result analysis; Madhu Kumar Vanteru: Methodology, Data collection, Writing; Azmera Chandu Naik: Conceptualization, Formal analysis, validation; Karthik Kumar Vaigandla :

Conceptualization, visualization, supervision , Writing-review and editing.

Funding

No funding or grants was received for this research work

Competing Interests

The authors declare that there are no conflicts of interest regarding the publication of this manuscript.

Has this article screened for similarity?

Yes