Digital Communications and Networks 9 (2023) 411–421

Contents lists available at ScienceDirect

Digital Communications and Networks

journal homepage: www.keaipublishing.com/dcan

Towards a blockchain-SDN-based secure architecture for cloud computing in smart industrial IoT

Anichur Rahman [a], Md Jahidul Islam [b], Shahab S. Band [c,**], Ghulam Muhammad [d,*], Kamrul Hasan [e], Prayag Tiwari [f]

[a] Department of Computer Science and Engineering, National Institute of Textile Engineering and Research (NITER), Constituent Institute of the University of Dhaka, Savar, Dhaka, 1350, Bangladesh
[b] Department of Computer Science and Engineering, Green University of Bangladesh, Dhaka, Bangladesh
[c] Future Technology Research Center, College of Future, National Yunlin University of Science and Technology, Douliou, Taiwan, China
[d] Department of Computer Engineering, College of Computer and Information Sciences, King Saud University, Riyadh, Saudi Arabia
[e] Department of Information and Communication Engineering, Hankuk University of Foreign Studies, South Korea
[f] Department of Computer Science, Aalto University, Finland

ARTICLE INFO

Keywords:
Smart IIoT
Blockchain
SDN
IoT
Security
Privacy
OpenFlow
SDN-Controller
Data security
Cloud computing
Cloud management

ABSTRACT

Some of the significant new technologies researched in recent studies include BlockChain (BC), Software Defined Networking (SDN), and Smart Industrial Internet of Things (IIoT). All three technologies provide data integrity, confidentiality, and integrity in their respective use cases (especially in industrial fields). Additionally, cloud computing has been in use for several years now. Confidential information is exchanged with cloud infrastructure to provide clients with access to distant resources, such as computing and storage activities in the IIoT. There are also significant security risks, concerns, and difficulties associated with cloud computing. To address these challenges, we propose merging BC and SDN into a cloud computing platform for the IIoT. This paper introduces "DistB-SDCloud", an architecture for enhanced cloud security for smart IIoT applications. The proposed architecture uses a distributed BC method to provide security, secrecy, privacy, and integrity while remaining flexible and scalable. Customers in the industrial sector benefit from the dispersed or decentralized, and efficient environment of BC. Additionally, we described an SDN method to improve the durability, stability, and load balancing of cloud infrastructure. The efficacy of our SDN and BC-based implementation was experimentally tested by using various parameters including throughput, packet analysis, response time, bandwidth, and latency analysis, as well as the monitoring of several attacks on the system itself.

1. Introduction

In today's interconnected world, cloud technology is seen as a crucial enabler of IT industry innovation. It is a model that provides consumers with various on-demand services and network access to shared databases of physical resources such as computation and storage. In this way, customers no longer need to purchase expensive hardware to access these services; instead, they can use commodity hardware (such as a laptop) connected to the internet, giving them the means to develop solutions to complex problems. Furthermore, cloud computing enables users to access resources from any location remotely, allowing for virtual collaboration. It enables users to improve resources relatively quickly, which was time-consuming with traditional hardware-based computing systems. Proper resource usage aids in mitigating the problem of over and under utilization [1,2]. Cloud computing provides a range of services like Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). Furthermore, cloud services are scalable, flexible, and reliable for users on demand [3]. Blockchain (BC) is another technology, but it is focused on security. Consequently, BC technology has sparked particular interest in the financial sector, and more broadly, wherever data security is a top priority. BC with the addition of secret sharing security enhancement is possible in cloud services with the improvement of data security [4]. Furthermore, BC technology helps detect malicious use by enforcing in the detection of providers to detect suspicious

* Corresponding author.
** Corresponding author.
E-mail addresses: anis_cse@niter.edu.bd (A. Rahman), jahid@cse.green.edu.bd (M.J. Islam), shamshirbands@yuntech.edu.tw (S.S. Band), ghulam@ksu.edu.sa (G. Muhammad), kamrul@hufs.ac.kr (K. Hasan), prayag.tiwari@ieee.org (P. Tiwari).

https://doi.org/10.1016/j.dcan.2022.11.003
Received 29 January 2022; Received in revised form 7 September 2022; Accepted 1 November 2022
Available online 12 November 2022

suppliers [5]. All of the technologies discussed above play an essential role in the most beneficial industry currently, the Industrial Internet of Things, also known as IIoT. In the smart IIoT scenario depicted in Fig. 1, automation is performed by exploiting the benefits of IoT, and system security is provided by a variety of security mechanisms. This is essentially a network-dependent application in which the majority of the work is done through the use of sensor devices, and the collected data is transferred from one sector of the business to another without the need for human intervention [6]. The IIoT-based industrial sector gets benefits from the automation procedure via the sensors, wireless networking devices, and models used for making important decisions based on data collected from network-connected sources [3,7]. However, the architecture of smart IIoT is primarily networking-dependent and thus, attracts intruders who wish to alter the data gathered for the processing of highly sensitive information [8].

A hash value is generated in this architecture to secure the information transmitted through the BC structure. Furthermore, BC stores the information in a public ledger where any changes can be detected by others connected to the ledger. As a result, no third party can interfere with the transaction [9]. Furthermore, because cloud computing is interconnected to numerous security issues and financial transactions, BC can strengthen the reliability of cloud computing functionalities [10]. Another emerging paradigm is SDN [11], which makes network management more straightforward and easier. It has found extensive applications in cloud computing, where networks are challenging to manage and troubleshoot. As previously stated, network performance is crucial to the quality of service provided to the end users, who access shared resources via the internet. SDN technology is used to control a network using program. It is easy to manage network issues with the use of SDN, as cloud computing is rife with them. Cloud computing is useless without a network since the resources are shared and transmitted to the users over the internet. Recent applications of SDN employ multiple controllers, which add a new dimension to the devices' network. As the number of people using this type of cloud computing has grown steadily in recent years, resource management and data security become a top priority. To manage the resources efficiently, SDN can be an effective solution that will trace the network's traffic and estimate the bandwidth of the network. The combination of new emerging technologies is crucial for protecting the data and making cloud activity easier.

Based on the analysis above, we propose a distributed, secure BC-based SDN-enabled control architecture for cloud computing. A distributed BC efficiently provides reliable and efficient security both privately and publicly in the cloud environment. The contributions of the paper are listed below:

- We propose a distributed structure to improve the reliability and speed of physical and logical data on cloud infrastructure for smart IIoT applications.
- We employ a distributed SDN-BC strategy with the asset of smart IIoT to improve the security, solitude, and secrecy of the presented architecture.
- In IIoT applications, we analyze the feasibility of a given cloud model in terms of various characteristics and assess its responsiveness to network threats.

Fig. 1. Process diagram of Smart Industrial Internet of Things.

Table 1 lists some of the notations. The remainder of the paper is organized as follows: Section 2 discusses the current work's background and literature reviews. In Section 3, we present a “DistB-SDCloud” architecture for cloud computing, which we also present in different ways. In Section 4, performance analysis and discussion are presented. Additional, in Section 5 we suggest the future scope of the study. Finally, in Section 6, the authors conclude this article, outlining the limitations of this work and future research plans.

2. Background and literature reviews

Recently, several researchers have published numerous articles on emerging technologies such as SDN, BC, smart IIoT, cloud computing, and other intelligent technological applications. This section provides a systematic literature overviews based on these technologies.

2.1. Software Defined Networking (SDN) with smart IIoT applications

SDN is a networking paradigm that helps the efficient network management and configuration. Alternatively, SDN is an intelligent component of smart IIoT applications. It can provide a logically centralized approach to data and network resources management. This orchestration and management strategy can be controlled by distinct and decoupled planes, as shown in Fig. 2. The SDN gateway offers forwarding capabilities to IoT devices, allowing them to enter the SDN environment. Sahay et al. discuss the application of SDN in the computer networking security, as the programmability of SDN offer network security improvements [12]. Using SDN for security detection and mitigation, the authors provide a detailed overview. An overview of SDN-based security in networking systems was provided by Shin et al. in Ref. [13]. As a result of this study, there was the potential to improve SDN features in various domains. The authors provided recommendations for future research on SDN security processes in various domains. Du et al. [14] present the SDN-based resource allocation to the Edge-Cloud Computing application. They derive the optimal pricing and the distribution process of cloud

Table 1
List of acronyms in alphabetical order.

Notations	Description
AI	Artificial Intelligence
API	Application Programming Interface
BC	BlockChain
BCF	BlockChain Fundamental
BCT	BlockChain Technology
CBR	Constant Bit Rate
CC	Cloud Computing
DoS	Denial of Service
DDoS	Distributed Denial of Service
DS	Data Security
DM	Data Management
IaaS	Infrastructure as a Service
IoT	Internet of Things
IIoT	Industrial Internet of Things
NFV	Network Function Virtualization
PaaS	Platform as a Service
PoW	Proof of Work
QoS	Quality of Service
RTR	Response to Request time
SaaS	Software as a Service
SC	Smart Contact
SDN	Software Defined Networking

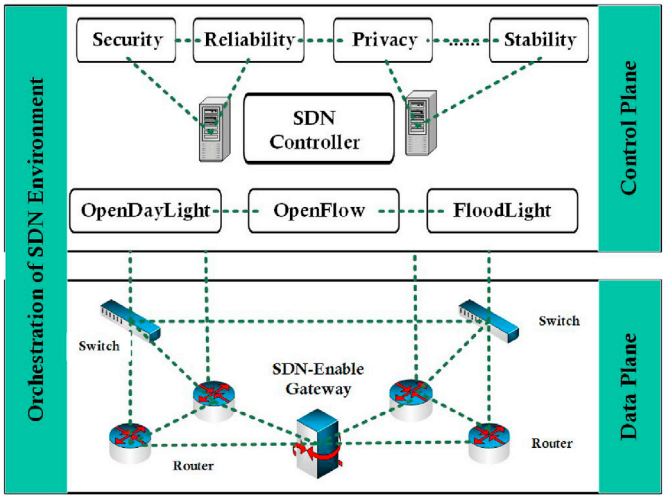

Fig. 2. SDN architecture.

computing resources based on the replicator dynamics of user benefit selection. Then, the authors provide the validated simulation results based on the stated user preference and computing resource pricing and distribution. Chaudhary et al. [15] discuss the application of an SDN-based communication mechanism for the smart IIoT-based networking system for providing a secured encrypted-based model. Because the smart IIoT produces a massive amount of data and all of which is highly sensitive, the authors propose an SDN-based solution for better data forwarding capabilities and secure data transmission in this scenario. Again, Bedhief et al. propose SDN and fog-based solutions for the minimization of delays in smart IIoT-based networks [16].

Machine learning and entropy-based mechanism are used to detect vulnerabilities. Abdelaziz et al. suggest a new controller cluster to address the issues of software-defined network reliability, manageability, fault tolerance, and interoperability [17]. Clustering in the control plane can significantly reduce transmission delay and packet loss. The authors claim that the scheme they present optimizes the controller's performance by achieving reasonable CPU utilization. Three existing SDN platforms have been presented with architectures: OpenFlow, OpenStack, and OpenDayLight [18]. The authors also discuss load balancing and security materials for the SDN framework to lower the cost of related issues.

2.2. BCT with smart IIoT

BC is a decentralized/distributed ledger that ignores the party involved in different transactions. It does its work correctly using consensus processes such as Proof-of-Work (PoW) and Proof-of-Stack (PoS). Meanwhile, as depicted in Fig. 3, it uses hash data to maintain communication from one block to the next. Furthermore, it can prevent information tampering and data hacking. Presently, this technology is being used in different fields like the IoT, smart IIoT, healthcare, electronic voting, cloud computing, and so on [19]. BC is a component of industrial IoT, where IIoT helps the efficient improvement of the desired

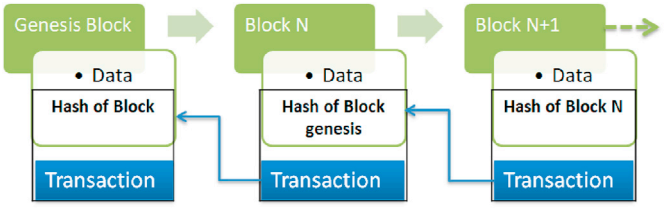

Fig. 3. BC procedure.

system's confidentiality. A significant amount of data must be shared in Industrial IoT and at present, the data sharing takes place on the cloud where BC is being used to authenticate the process with different kinds of encryption and decryption [20]. Anonymous schemes are used to create the standard IIoT credential, and, the identity lifecycle is adapted to the BC for the biometric identification in smart industry applications [21]. The service provisioning system in Industrial IoT is being performed by three parties using BC-based trusted access architecture [22]. A BC-based mechanism has been proposed by Wang et al. for secure data transmission, or the data verification [23]. In a similar study [24], they considered using a consortium BC to automatically control data transmission through a tactical data link. This research addressed issues like security, automaticity, and so on. Further, Awotunde et al. [25] presented a deep learning model with a rule-based feature selection toward intrusion detection through an IIoT network. Additionally, Chien [26] integrated of next-generation smart IIoT with BC for smart advancement. In a similar paper, Koens et al. mention BC technology and how to use it in a business setting [27]. They answer two fundamental questions: first, is BC needed, and if so, which BC is the best one. BC is often required to consider the results of this survey. The authors retain the BC in addition to other database technologies. Their schemes demonstrate some opposition, suggesting that no scheme is complete, and they fail to describe the limitations of BC technology. Huo et al. have surveyed the progress of BC research in the IIoT as well as stated future challenges [28]. They also evaluated the technical requirements of this technology.

2.3. BC with SDNs

Through the use of an SDN-intelligent gateway, IoT sensor data can be transformed from the sensor level to the SDN environment. SDN filters the data and BC, and efficiently manages all filtered data. Furthermore, a virtual communication layer is used to establish a connection between the SDN environment and the BC approach. This layer also offers virtualization technology [51] to establish an effective bonding with two methods, as depicted in Fig. 4. In the context of IoT architecture, Sharma et al. presented the DistBlockNet paradigm [50]. This platform offers two significant advantages for various networking technologies such as SDN and BC. The authors proposed a strategy to update the flow rule table by applying the BC technique and formalizing the flow rule table. They also measured the results using different metrics, and the analysis presented a better outcome relative to the surviving piece. Rahman et al. proposed the “DistBlockSDN” architecture with Network Function Virtualization (NFV) implementation for a smart city [43]. The authors used a BC

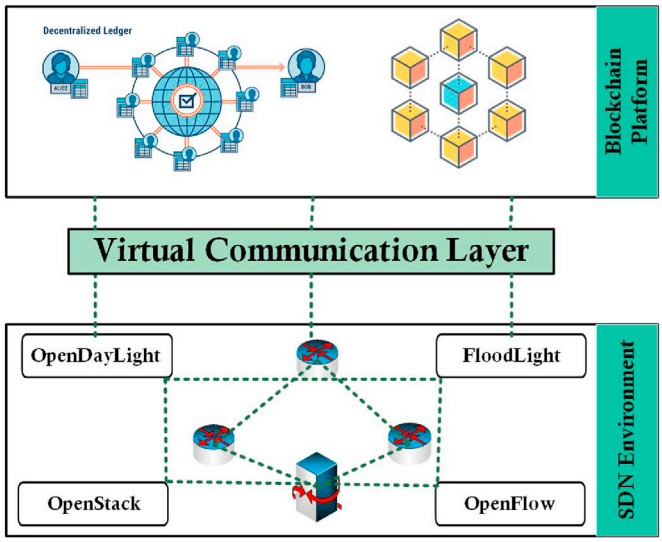

Fig. 4. An architecture combining SDN with Blockchain to provide security.

approach to achieve high security and privacy. Furthermore, they presented an algorithm for selecting the cluster head while consuming little energy. The authors evaluated the networks' performances using parameters like throughput and packet arrival rate. In another study, Navid et al. [52] presented a novel model to address IoT challenges by combining SDN and BC technologies for future 5G telecommunication networks.

2.4. BC-based security for cloud computing

Cloud computing is a model that allows for the remote delivery of hardware, software, storage, and other resources as services via the internet. Different implementation models have been developed according to the application scenario and business purpose, such as restricting access to cloud resources only to the employees of an enterprise. There can be personal, public, hybrid, and community deployment models, as reported in Fig. 5.

Gaetani et al. first presented some research questions based on BC for cloud computing [49]. They presented accurate, high-level solutions to these questions for the European project SUNFISH. In related research, Park et al. established the notion of BC technology, and some possible technological cloud computing directions [53]. They also presented a high-level security approach to cloud computing on various parameters based on the BC concept. In [54], BC technology was used to provide various security services to IoT forwarding devices. Cloud computing and Edge transparent computing technologies were described in detail in the study. Furthermore, the authors explicitly discussed BC measures to safeguard IoT networks from unauthorized threats. Similarly in [55], Sharma et al. introduced a new BC-based decentralized cloud platform with Software-Defined Networking (SDN) enabled controller fog nodes at the network's edge. They proposed an excellent combination of fog computing, SDN, and BC. Furthermore, the authors presented an architecture designed to support high availability, real-time data collection, enhanced scalability, security, and resiliency while maintaining low latency. They also evaluated parameters like throughput, response time, and accuracy in detecting real-time attacks. In addition to the traditional BC, artificial intelligence-based BC technology was used in the mechanism to provide cyber-physical security [56].

Table 2 summarizes the literature review that we have conducted, considering the critical technologies employed in each work and the issues that the authors attempt to address in a specific application. Moreover, where BC is used, we also report the considered implementation platform. After discussing various technologies, we intend to aggregate SDN and BC with IIoT applications to secure the cloud services. The SDN renders flexibility to the infrastructure and BC ensures the confidentiality of the smart IIoT services.

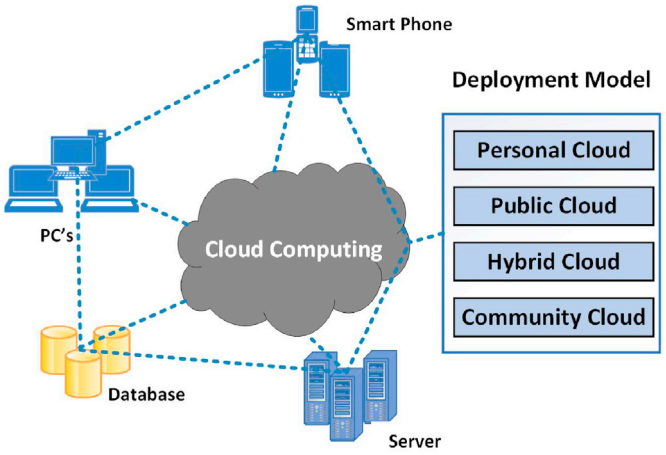

Fig. 5. A notional architecture of Cloud computing.

3. Proposed "DistB-SDCloud" architecture for cloud computing

To provide individual security and reliability to cloud applications, we propose a distributed, reliable, BC-based architecture framework that runs these tasks efficiently, as shown in Fig. 6. The presented architecture is divided into four distinct layers. These layers are–Data Extraction, SDN Environment, Distributed Secure BC Methodology, Cloud Computing Management, and Services for the smart IIoT applications.

3.1. Data Extraction using SDN techniques in smart IIoT applications

Several smart sensor-based devices (for example, an IoT forwarding host) can send sensor data through SDN-enabled gateways controllers, such as firewalls, switches, routers, and various data storage devices. These sensor data can be securely used in an SDN-based BC network for various operations. Furthermore, sensor data contributes to efficient performance in the distributed architecture for the smart IIoT environment. The SDN can then be separated into several planes using sensor data, including data, control, and implementation planes. Data plane operations refer to the collection of sensor data using multiple controllers, protocols, and platforms– OpenDayLight, OpenFlow, and OpenStack, respectively, in an SDN environment [57]. This layer allows for the efficient collection of sensor data using SDN from the smart IIoT system [15].

3.1.1. Data plane

As depicted in Fig. 7, the data layer is the lowest in the SDN architecture. This plane enables the SDN gateway to communicate properly with sensor-based devices (base station, switches, firewalls, data transfer, and so on). It offers two types of switches: virtual and software-based switches, which are commonly used with the Linux operating system. Another type is physical switches, which are related to hardware-based switches and take advantage of the higher flow of physical forwarding devices in the SDN infrastructure plane. These switches are responsible for forwarding and exchanging packets in network-based applications. In our architecture, the data plane collects the sensor data as it moves to and from the cloud computing environment in a smart IIoT design.

3.1.2. Control plane

The control plane is the core foundation of the SDN architecture and the foundation of network layer communication. Although there are multiple distributed controllers at the physical level, this plane provides a high-level abstraction, giving the applications a logically centralized view. Furthermore, this plane is responsible for the interaction between infrastructure and applications planes in the SDN architecture with smart IIoT applications. Consequently, it enables numerous networking services for the desired platform. The plane's functionalities are provided through several controllers such as POX, Floodlight, OpenDayLight, Openstack, and Beacon [58], as well as leveraging protocols like OpenFlow. Different interfaces are used to interact with devices: different interfaces–southbound, northbound, and east/west-bound. The southbound interface communicates with forwarding devices, while the northbound interface communicates with application fields; the east and westbound interfaces communicate with distributed controllers. Furthermore, this controller provides a highly flexible and stable architecture for data to flow into the cloud computing platform.

3.1.3. Application layer

The service layer is the topmost layer of the SDN. While the lower layers of the SDN-based scheme enable an effective dynamic updating of forwarding flow rules, the application layer for the smart IIot framework increases network infrastructure between the control and implementation platforms via virtual or physical forwarding. By leveraging the functionalities of the lower layers, the applications can realize complex network configuration and management, network data analytics, or specialized functions targeting specific scenarios such as large data

Table 2
Reviews of existing literature.

Works	Year	Used Technologies	Considered Framework	Implementation	Addressing Challenges	Blockchain Application Framework
Khezr et al. [29]	2022	IIoT, BC, and Edge Intelligence	Decentralized	Smart Transaction and Data Trading	Security & System failure	Hyperledger Fabric & Raft Consensus Mechanism.
Latif et al. [30]	2022	AI, BC, SDN, IoT	Centralized, Distributed	Cyber Physical Systems	Security and Energy management	Peer-to-Peer (P2P) communication networks
Firouzi et al. [31]	2022	Fog, Edge, Cloud Computing, AI	Distributed and Collaborative	Cloud Applications	Privacy-preserving and Security	–
Hewa et al. [32]	2022	IIoT, Fog, Cloud, BC	Distributed	Smart Contacts & Cloud Manufacturing	Security issues & Delay analysis	Hyperledger Fabric
Cao et al. [33]	2022	BC, SDN		Smart Industry	Industrial Energy Market	Consortium Blockchain
Bu et al. [34]	2021	IIoT, AI	–	Smart Industry	Production Optimization	–
Rahman et al. [35]	2021	IoT, BC, SDN	Centralized, Distributed	Cloud Computing	Energy & Privacy	–
Rahman et al. [36]	2021	IIoT, AI	Distributed	Smart City	Assured & real time communication	–
Michailidis et al. [37]	2020	IIoT, AI	–	Non-terrestrial Networks	Low latency & indicative delay	–
Nguyen et al. [38]	2020	Distributed Ledger	Decentralized	Smart Healthcare, Smart City, and Smart Industry	Steadfastness & Solitude	Ethereum & Hyperledger Fabric
Wei et al. [39]	2020	Distributed Ledger	Decentralized	Cloud Computing	Trustworthiness & Security	–
Yang et al. [40]	2020	BC, Cloud Computing	Centralized, Distributed	Cloud Computing	Reliability & Solitude	–
Xu et al. [41]	2020	BC, 6G	Distributed	Resource management	security	–
Hasan et al. [42]	2020	BC	Decentralized	Verification System	Trustworthiness & Privacy	Ethereum Transaction
Rahman et al. [43]	2019	BC, SDN	Centralized, Distributed	Smart City	Reliability & Privacy	Ethereum Network
Singh et al. [44]	2019	BC, SDN	Centralized, Distributed	Smart City	Trustworthiness & Privacy	Ethereum Network
Cech et al. [45]	2019	BC, SDN	Distributed	Fog Computing	Trustworthiness & Privacy	Hyperledger Network
Tuli et al. [46]	2019	Distributed Ledger	Distributed	IoT Networks	Reliability & Privacy	–
Deep et al. [47]	2019	Distributed Ledger	Decentralized	Cloud Computing	Security & Reliability	Ethereum
Li et al. [48]	2018	Distributed Ledger	Distributed	Cloud manufacturing	Data Availability & Privacy	Ethereum
Gaetani et al. [49]	2017	BC, Cloud Computing	Decentralized	Utility Computing	Reliability & Privacy	Ethereum
Sharma et al. [50]	2017	Blockchain, SDN	Centralized, Distributed	IoT Ecosystem	Reliability & Privacy	Ethereum Network

centers. This layer enables services such as smart optimization, mobility management, load balancing, routing, switching, reliability, and network monitoring in the cloud networks, as depicted in Fig. 7.

3.2. Distributed Secure BC-SDN methodology

A BC [59] is a form of ledger or data system that enables the addition of many functionalities to be added to a distributed or decentralized, temperature-resistant facility, as depicted in Fig. 8. It is based on the identity node of the miner and the general members' requesting node. Simultaneously, BC can provide effective access control and security for system design. In essence, BC serves as a secure ledger for recording transactions. However, it does not save all user activity in central storage or database. Furthermore, at the user end, each user uses the same storage. They also keep all transaction activities and updated copies in the same place to ensure a consensus system. In the BC environment, each block can accurately deal with multiple transactions in the smart IIoT environment. Furthermore, every block is linked by a hash chain and contains detailed information such as a timestamp, records, existing hashes, previous data, and non-conflicting transactions. Based on this concept, we believe that BC is an appropriate technology for ensuring access control in the presented cloud environment. This approach is organized as follows: security and access policy [60].

3.2.1. Security and access policy

By combining a BC with a smart IIoT approach, we provide adequate security for our desired system model. This model prevents access of undesired users or unauthorized third parties performing access control, as well as dealing with data tampering and loss. Moreover, the user sends a request to the BC-based server, which then, takes the necessary action based on the request. This will be checked in the server database simultaneously. If this request is valid, the server sends a positive response to the user,allowing them to access the various services from the desired server; if the request is not valid, it is discarded.

3.2.2. BC and SDN convergence

This segment discusses the relationship between BC and SDN, which is depicted in Fig. 8. Initially, the data layer is responsible for adequately forwarding intelligent device information to another layer. Moreover, the data passing gateway stores all data to provide a secure platform. The authors established a secure platform, BC. This block helps a proffer secure the temporary database for processing the node data before entering the cloud applications. Furthermore, these cloud services can be managed by the desired user remotely. The entire process is executed by the SDN platform efficiently. SDN uses OpenFlow switch to conduct all activities in the desired application. After the completion of the convergence between BC and SDN, the user will be able to integrate various services such as security, remote routing, mobility, privacy, and virtualization into the cloud data management applications.

3.2.3. Block creation and validation

To provide security in the presented system, the authors have considered the distributed platform BC. The block creation and validation process of BC is depicted in Fig. 9. First, the authors send an encrypted block to the peer-to-peer networking environment. Then, these blocks are validated by networks nodes through the mining process. After

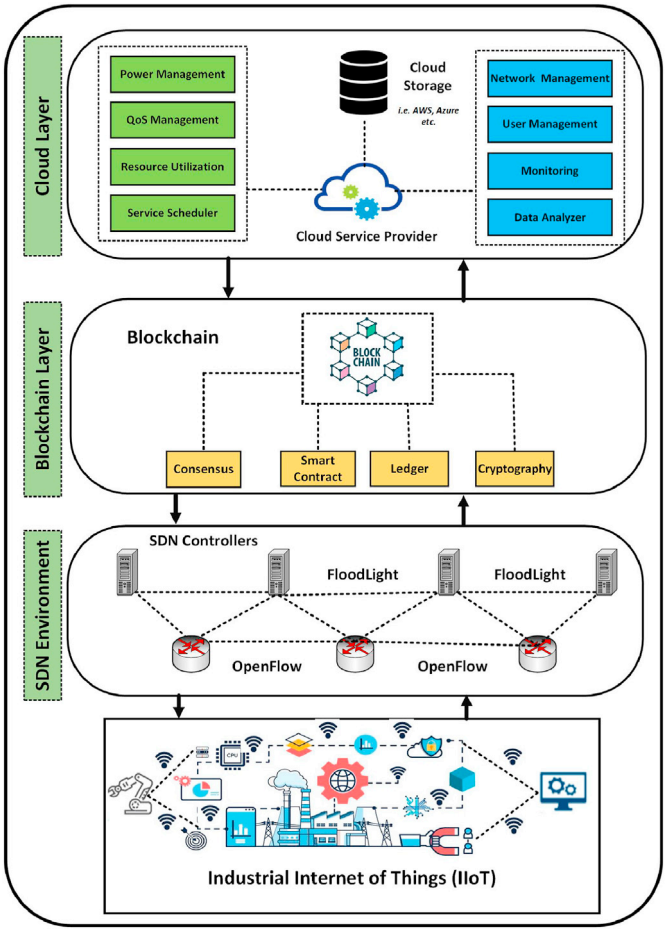

Fig. 6. Proposed "DistB-SDCloud" architecture.

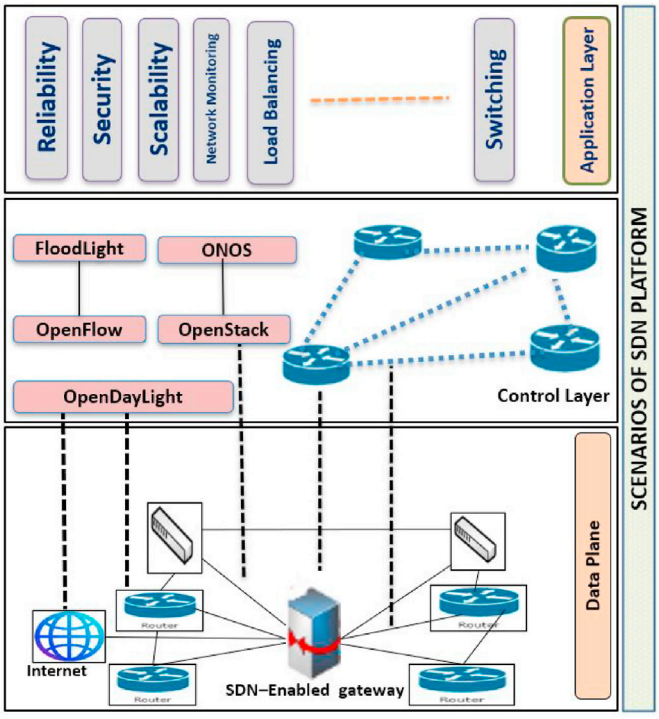

Fig. 7. Layered-based performance of SDNs.

validating the process, the block is created as a novel data block. Furthermore, this block is appended to the BC network as a new block. Finally, the distributed ledger is efficiently updated.

3.3. Attack mitigation in cloud environment BC-based SDN approach

SDN is extremely vulnerable to cyber-attack. Some of the most common attacks are DDoS attacks [61], DoS attacks, flooding attacks, and many more, now that the cloud environment is fundamental to various innovations. Attacks on this cloud storage scenario have become a significant attraction for many intruders. The overall system could be down for some time because of these attacks. We also proposed a method to recognize and block these attacks to address this problem so that the device can operate efficiently. The mechanism of the BC has been used to support the SDN controllers. The controller will detect potential attacks according to this instruction. The second issue is the avoidance or defense after the intruder has been identified. In the BC approach, the data packets are transmitted block by block. In this case, only the authorized blocks can take their place, and unauthorized blocks are discarded from the chain.

3.4. Cloud Computing Management and services

Our proposed model enhances various services in the cloud computing environment by using a distributed BC approach. This BC-based SDN architecture provides benefits like flexibility, accessibility, security, and privacy when retrieving, and storing numerous resources in the cloud computing platform. Without the involvement of the SDN approach, BC alone [54] cannot provide improved reliability, high stability, a logically centralized controller, and an increased load balancing capability in the proposed architecture. While the accessibility and availability of services and resources in the cloud eventually depend on internet speed, cloud computing resources perform better with Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) when the presented architecture correctly, as depicted in Fig. 10.

4. Performance analysis and discussion

4.1. Performance measurement parameters

To evaluate the performance of the proposed architecture, we have considered two main parameters, namely, throughput and communication overhead.

We calculated the throughput using equation Eq. (1).

$$Throughput = \frac{\sum_{n=i}^{n} CBRrece}{Simulation\ Time} \tag{1}$$

CBR is the abbreviation for Constant Bit Rate.

We also use Eq. (2) to calculate the communication overhead.

$$Communication\ Overhead = \frac{\sum RTRPacket}{\sum CBRrece} \tag{2}$$

RTR indicates the Response to Request time.

4.2. Environment setup

To create the environment in which our proposed system will operate, we have used Mininet as a network emulator, with the Mininet-Wifi module to stimulate a wireless network configuration. OpenStack was used as a cloud storage platform, and OpenFlow was chosen as the protocol within the SDN architecture. Our tests were conducted on a computer running the Ubuntu (Linux) operating system, with a Core(TM)-i7 processor, 3.40 GHz CPU, and 500 GB of hard drive space. Furthermore,

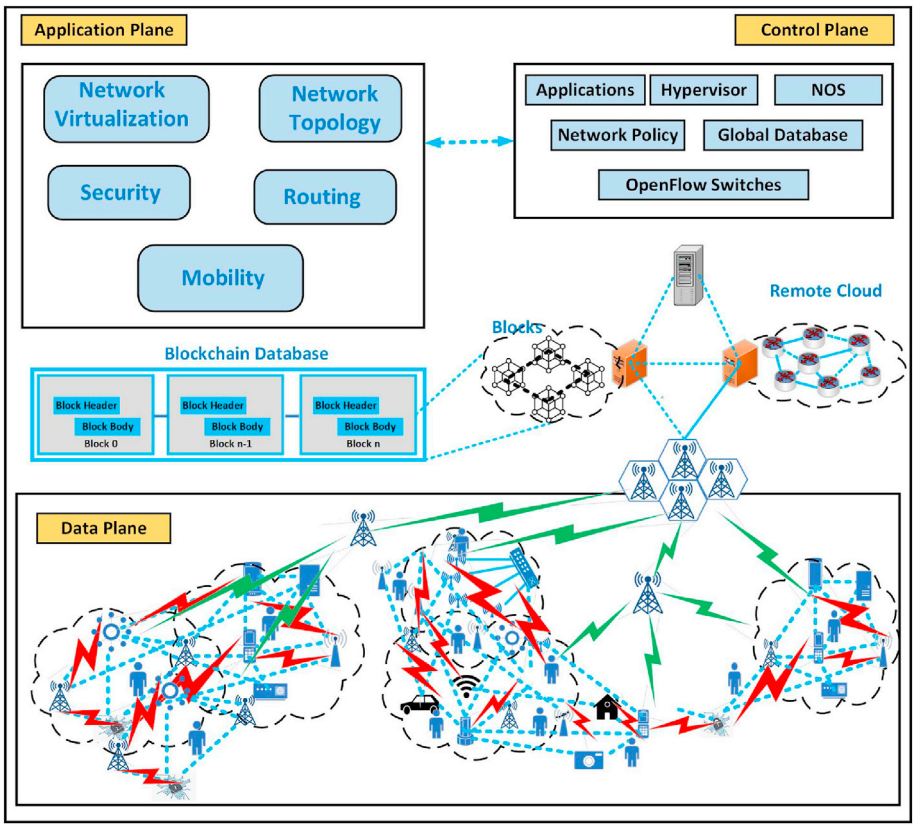

Fig. 8. BC and SDN convergence.

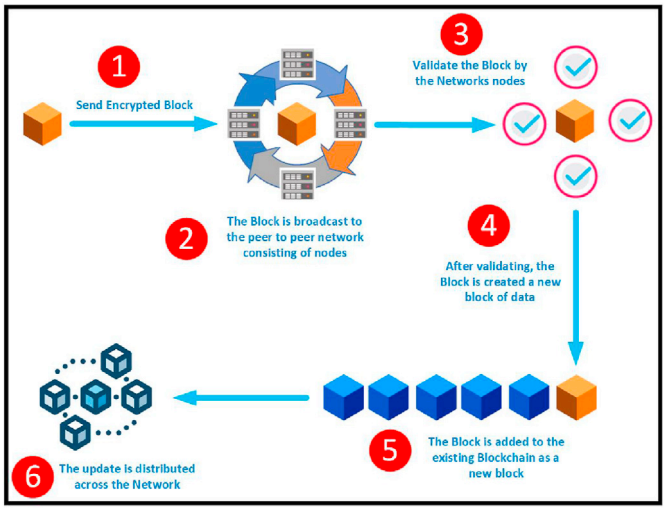

Fig. 9. Block creation and validation.

we used Wireshark to sniff traffic flowing into the network to test the effectiveness of our SDN-based BC network. Table 3 summarizes the parameters used in our simulation environment.

4.3. Performance evaluation of BC with SDN controller in cloud computing environment

4.3.1. Throughput

Throughout this section, we have assessed the performance of our proposed model using various metrics such as throughput, packet arrival rate, and file transfer operation. First, as depicted in Fig. 11, we

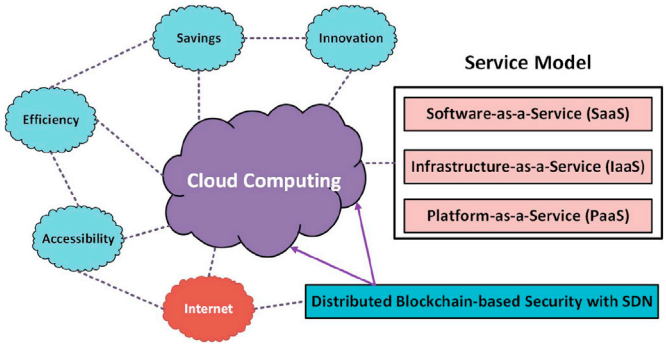

Fig. 10. Distributed BC-SDN based Cloud computing services.

calculated throughput using the number of nodes. Meanwhile, throughput comparisons between OpenFlow-based SDN and our proposed architecture "DistB-SDCloud" are being conducted and are graphically depicted in this figure. Furthermore, we discovered that the throughput remains nearly constant when the number of nodes is reduced. However, as the number of nodes increases, the throughput increases as well. Finally, we compared our proposed "DistB-SDCloud" framework to one that uses only SDN and OpenFlow, and discovered that our proposed scheme outperforms the other.

4.3.2. Packet analysis

Fig. 12 depicts the system performance when dealing with an increasing number of packets. To the end, this figure compares the bandwidth (GB/s) to the current packet arrival rate (thousand/s), comparing the results of our proposed system to an OpenFlow-based SDN. The tested packet rates range from 190 to more than 1400 packets per second for both tested models. According to Fig. 12, we can

Table 3
Simulation environment.

	Parameters Name	Values
General Parameters	Packet Analyzer	Wireshark
	Platform for cloud storage	OpenStack
SDN Parameters	SDN Controllers	5
	OpenFlow switches	4
	Gateways	2
	SDN Routing Protocol	OpenFlow
Blockchain Parameters	Blockchain platform	Ethereum
	Number of transactions	Variable
	Block header	80 bytes
	Proof type	Proof of Work (PoW)
Others Parameters	Simulation Area	1000 m × 1000 m
	Number of IoT devices	1–50
	Simulation Times	500 s
	Data Rate	12 Mbps
	Initial Energy Values of IoT devices	12–15 j
	Initial Trust value	5 j
	Node Transmit Packet Size	100–512 bytes

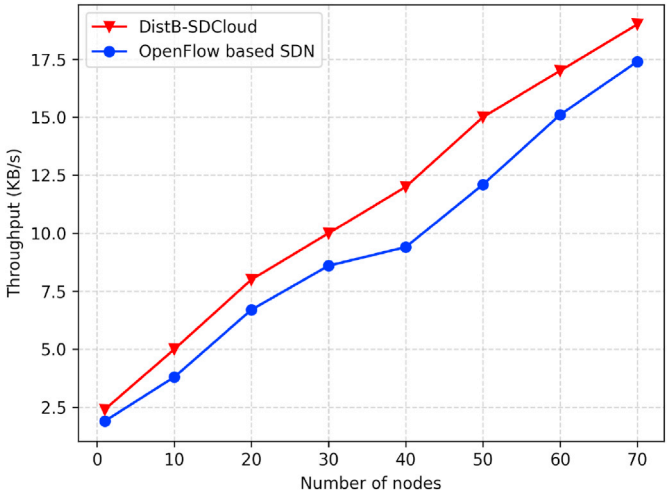

Fig. 11. Throughput comparisons according to the number of nodes in the network.

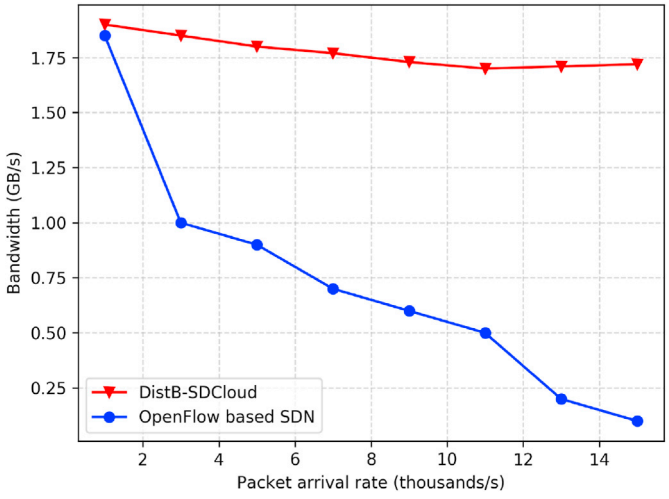

Fig. 12. Bandwidth measured varying on the packet arrival rate.

see that when the packet rate increases (which could be, for example, a sign of a network attack), the bandwidth is drastically decreased in the OpenFlow-based SDN. On the contrary, the performance of our presented model remains unaltered, even when the attack rate is increased and the highest tested packet is used, proving its robustness against suddenly increased loads caused by malicious or intended activities.

4.3.3. Response time

Fig. 13 depicts the performance of file operations for the core and presented models. This figure reports the response time for file transfer operations when the file size is varied. Indeed,the file size increases, the response time also increases. However, the proposed model consistently reports a lower and thus better response time performance compared to the core model. Moreover, we also observed that our model could achieve considerable file sizes compared with the existing core-based system.

4.3.4. Bandwidth and latency analysis

We analyze another performance parameter bandwidth based on the number of packets. According to the analysis of Yazdinejad et al., we have measured our performance of bandwidth and delay using the BCF [62] method. Fig. 14 depicts the outcomes between the proposed system "DistB-SDCloud" and the BCF model. Moreover, the authors considered SDN controllers and SDN-based OpenFlow protocol to build the desired network. They then used protocol-based rules to measure the bandwidth for several packets.

Initially, both models show the performace is almost nearest in the networking environment, which was exactly the same when the packet number was 500. When the number of packets is increased, the presented model performs better than the BCF model. On attaching SDN-controllers, the system model achieved scalability, reliability, and network stability; thus, it outperformed the BCF model. The proposed framework performs best when the packet number is 2500. Fig. 15 alternatively, depicted the latency based on the data size. Because of SDN (switches, controllers) involvement, the proposed system "DistB-SDCloud" can respond faster than the BCF model.

4.4. Performance analysis in different attacks environment

After comparing throughput, packet arrival rate, and reaction time, we discovered that our proposed model outperforms an OpenFlow-based SDN model, in terms of throughput, packet arrival rate, and reaction time.

In this section, we also discuss the complexity of our architecture 's CPU usage during network attacks. Fig. 16 depicts the analysis of CPU usage for DDoS attacks on our infrastructure when multiple services are running in the background. Furthermore, we based a learning set to record CPU consumption during a DDoS attack. This figure also illustrates the average CPU consumption in different apps based on the "DistB-SDCloud" scheme when DDoS attacks are launched. The simulated attack began at a value of about 1.1, and the attack rate increased over time. When we examine the evolution of CPU use over time, we can see how it rises in a short period, then swiftly drops to lower levels, demonstrating that "DistB-SDCloud" can provide a solid defense against this attack.

4.5. Discussion

This study combines two leading technologies, SDN and BC, to maximize efficiency and security in a cloud computing infrastructure. One essential finding is that combining BC and SDN improves security and increases the overall throughput, while maintaining adequate response times and CPU utilization under control, especially in the context of network attacks.

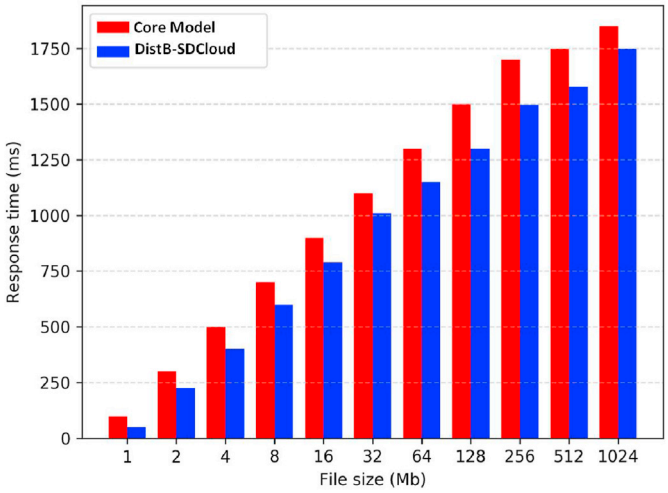

Fig. 13. Response time for variable-sized file transfers.

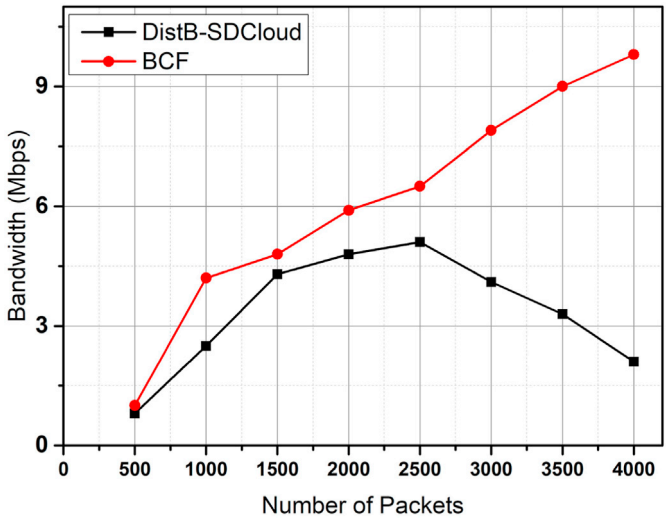

Fig. 14. Bandwidth vs. number of packets.

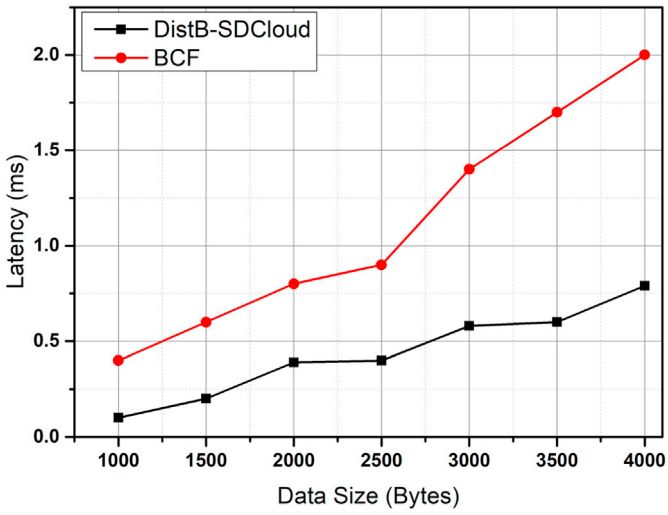

Fig. 15. Latency vs. data size (Bytes).

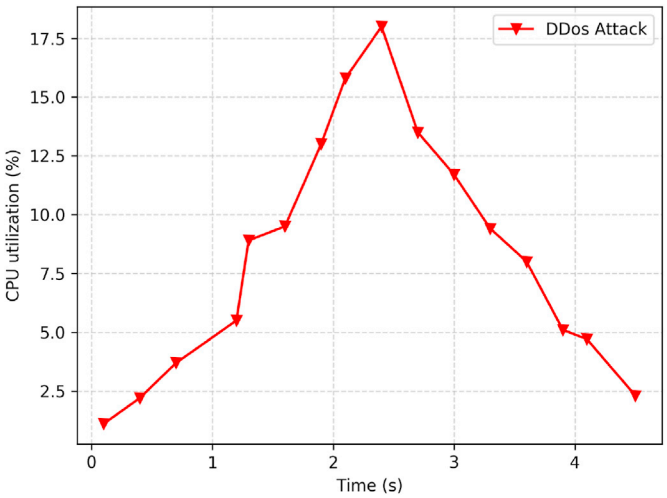

Fig. 16. CPU utilization during DDoS attacks.

5. Future scopes

5.1. Artificial Intelligence (AI) deployment in the smart IIoT

Smart IIoT is intended for use in intelligent factory applications, especially in predictive procedures and doing maintenance remotely [34]. AI constituents the models that could be used for predictive services. The deployment ofAI can transform the IIoT into a more powerful technology. Different manufacturing companies employ Industrial IoT with AI to make decisions during production. AI methodscan process the data of industry and draw a suitable conclusion to accelerate the operation of diligence. Recently, smart production systems are being developed with Machine Learning (ML) models.

5.2. AI in SDN-IoT networks

The functionality of an SDN is to programmatically control a system; thus AI and MLmodels could be deployed to the controllers from which various decisions could be made. The flow management of different SDN-based IoT networks using AI for cloud can be realized. This technology is also used in the field of 5G enabled by SDN, and Network Virtualization [63]. The scalability of the systems based on these technologies is another concerning issue. In this case, AI can also play a role. Moreover, SDN-IoT networks could be smart and self-propelled with the help of AI methods.

5.3. AI with blockchain

It is hard to find any research area where AI does not contribute. Most systems are being automated with the applications of AI. Since BC can work with the security and confidentiality of data, it could be combined with AI to built smarter systems with better security. They can provide solutions to contemporary problems such as medical issues, business revolution, and e-learning. Conceptual modeling in governance is also being encountered with the analysis of AI and BC. Another prominent field where these technologies can be used is digital marketing.

5.4. Smart IIoT security decentralized approach

Industry 4.0 applications [64] providesvarious services–IoT, SDN, BC, and so on— for security, privacy, and confidentiality purposes. Moreover, IIoT will be another advanced component in the IoT network. These technological approaches are not centralized; thus there is no interruption from a third party. The entire system remains safe from intruders, and applications data will be secure in the future developed system.

5.5. Security and privacy issues in IoT-AI

Privacy and security are some of the most popular areas of IoT research. AI is an advanced technology that can detect a security breaches automatically in smart cities and smart healthcare systems based on IoT networks. Identifying and resolving different intruders using AI models can lead a system to a successful real-life application. Some researchers have started to apply AI to 6G network security issues. The difficulties and opportunities, for example, are discussed in [65] and [66].

There are countless applications for using these technologies to improve the security and intelligence of a system. Besides cloud computing, the combination might provide numerous benefits in various industries ranging from smart cities and healthcare to business and privacy.

6. Conclusion

Lately, the demand for cloud computing services has been rapidly increasing, with the number of customers in the innovative IIoT environment increasing dramatically. However, cloud computing faces several threats, problems, and challenges–security, including privacy, compliance, compatibility, control, and reliability. To address these threats, researchers have proposed several tips and techniques; however, the security of these services faces several challenges that remain an open research question. In this article, we propose the "DistB-SDCloud" architecture to enhance the security and confidentiality of cloud computing approaches using smart IIoT applications. We used a distributed BC approach integrated into an SDN-IIoT architecture to improve the security, privacy, stability, reliability, flourishing accessibility, and confidentiality of the cloud computing, which benefits users of IIoT services. As part of our future research, we intend to effectively implement this architectural approach in diverse applications such as the Fog and Edge computing environments. The proposed system paradigm will then be more reliant on SDN, smart IIoT, and BC technologies.

Declaration of competing interest

None.

Acknowledgment

The authors extend their appreciation to Researchers Supporting Project number (RSP2023R34), King Saud University, Riyadh, Saudi Arabia.

References

[1] S.E. Shukri, R. Al-Sayyed, A. Hudaib, S. Mirjalili, Enhanced multi-verse optimizer for task scheduling in cloud computing environments, Expert Syst. Appl. 168 (2021), 114230.
[2] A. Rahman, M. Rahman, D. Kundu, M.R. Karim, S.S. Band, M. Sookhak, Study on iot for sars-cov-2 with healthcare: present and future perspective, Math. Biosci. Eng. 18 (6) (2021) 9697–9726.
[3] M.S. Hossain, G. Muhammad, Emotion-aware connected healthcare big data towards 5g, IEEE Internet Things J 5 (4) (2018) 2399–2406.
[4] D. Meshane, A.K. Sangaiah, M.S. Hossain, G. Muhammad, J. Wang, Blockchain-empowered cloud architecture based on secret sharing for smart city, IEEE Internet Things J. 7 (7) (2020) 6143–6149.
[5] G. Muhammad, M.S. Hossain, Deep learning-based edge-centric covid-19 like pandemic screening and diagnosis system within b5g framework using blockchain, IEEE Network 35 (2) (2021) 74–81.
[6] G. Rathee, S. Garg, G. Kaddoum, B.J. Choi, Decision-making model for securing iot devices in smart industries, IEEE Trans. Ind. Inf. 17 (6) (2020) 4270–4278.
[7] A. Rahman, M.J. Islam, M. Saikat Islam Khan, S. Kabir, A.I. Pritom, M. Razaul Karim, Block-sdotcloud: enhancing security of cloud storage through blockchain-based sdn in iot network, in: 2020 2nd International Conference on Sustainable Technologies for Industry 4.0 (STI), 2020, pp. 1–6, https://doi.org/10.1109/STI50764.2020.9350419.
[8] T. Soo Fun, A. Samsudin, Recent technologies, security countermeasure and ongoing challenges of industrial internet of things (iiot): a survey, Sensors 21 (19) (2021) 6647.
[9] L. Peng, W. Feng, Z. Yan, et al., Privacy preservation in permissionless blockchain: a survey, Digital Communicat. Networks 7 (3) (2021) 295–307.
[10] M.J. Islam, A. Rahman, S. Kabir, M.R. Karim, U.K. Acharjee, M.K. Nasir, S.S. Band, M. Sookhak, S. Wu, Blockchain-sdn-based energy-aware and distributed secure architecture for iot in smart cities, IEEE Internet Things J. 9 (5) (2022) 3850–3864, https://doi.org/10.1109/JIOT.2021.3100797.
[11] A. Rahman, U. Sara, D. Kundu, S. Islam, M.J. Islam, M. Hasan, Z. Rahman, M.K. Nasir, Distb-sdoindustry: enhancing security in industry 4.0 services based on distributed blockchain through software defined networking-iot enabled architecture, Int. J. Adv. Comput. Sci. Appl. 11 (9) (2020) 674–681.
[12] R. Sahay, W. Meng, C.D. Jensen, The application of software defined networking on securing computer networks: a survey, J. Netw. Comput. Appl. 131 (2019) 89–108.
[13] S. Shin, L. Xu, S. Hong, G. Gu, Enhancing network security through software defined networking (sdn), in: 2016 25th International Conference on Computer Communication and Networks (ICCCN), IEEE, 2016, pp. 1–9.
[14] J. Du, C. Jiang, A. Benslimane, S. Guo, Y. Ren, Sdn-based Resource Allocation in Edge and Cloud Computing Systems: an Evolutionary Stackelberg Differential Game Approach, IEEE/ACM Transactions on Networking 30 (4) (2022) 1613–1628.
[15] R. Chaudhary, G.S. Aujla, S. Garg, N. Kumar, J.J. Rodrigues, Sdn-enabled multi-attribute-based secure communication for smart grid in iiot environment, IEEE Trans. Ind. Inf. 14 (6) (2018) 2629–2640.
[16] I. Bedhief, L. Foschini, P. Bellavista, M. Kassar, T. Aguili, Toward self-adaptive software defined fog networking architecture for iiot and industry 4.0, in: 2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), IEEE, 2019, pp. 1–5.
[17] A. Abdelaziz, A.T. Fong, A. Gani, U. Garba, S. Khan, A. Akhunzada, H. Talebian, K.-K.R. Choo, Distributed controller clustering in software defined networks, PLoS One 12 (4) (2017) 1–19.
[18] D. Chourishi, A. Miri, M. Milić, S. Ismaeel, Role-based multiple controllers for load balancing and security in sdn, in: 2015 IEEE Canada International Humanitarian Technology Conference (IHTC2015), IEEE, 2015, pp. 1–4.
[19] G. Muhammad, F. Alshehri, F. Karray, et al., A comprehensive survey on multimodal medical signals fusion for smart healthcare systems, Inf. Fusion 76 (2021) 355–375.
[20] L. Tan, K. Yu, N. Shi, C. Yang, W. Wei, H. Lu, Towards Secure and Privacy-Preserving Data Sharing for Covid-19 Medical Records: A Blockchain-Empowered Approach, IEEE Transactions on Network Science and Engineering 9 (1) (2022) 271–281.
[21] H. Altaheri, G. Muhammad, M. Alsulaiman, et al., Deep Learning Techniques for Classification of Electroencephalogram (Eeg) Motor Imagery (Mi), Signals: A Review, Neural Computing and Applications, doi:10.1007/s00521-021-06352-5.
[22] H. Yang, B. Bao, C. Li, Q. Yao, A. Yu, J. Zhang, Y. Ji, Blockchain-enabled tripartite anonymous identification trusted service provisioning in industrial iot, IEEE Internet Things J. 9 (3) (2022) 2419–2431, https://doi.org/10.1109/JIOT.2021.3097440.
[23] J. Wang, B. Wei, J. Zhang, X. Yu, P.K. Sharma, An optimized transaction verification method for trustworthy blockchain-enabled iiot, Ad Hoc Netw. 119 (2021), 102526.
[24] W. Feng, Y. Li, X. Yang, Z. Yan, L. Chen, Blockchain-based data transmission control for tactical data link, Digital Communicat. Networks 7 (3) (2021) 285–294.
[25] J.B. Awotunde, C. Chakraborty, A.E. Adeniyi, Intrusion detection in industrial internet of things network-based on deep learning model with rule-based feature selection, Wireless Communications and Mobile Computing, 2021, 7154587.
[26] W.-C. Chien, C.-F. Lai, M. Hossain, G. Muhammad, Heterogeneous space and terrestrial integrated networks for iot: architecture and challenges, IEEE Network 33 (1) (2019) 15–21.
[27] T. Koens, E. Poll, What blockchain alternative do you need?, in: Data Privacy Management, Cryptocurrencies and Blockchain Technology Springer, 2018, pp. 113–129.
[28] 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 Commun. Surv. Tutorial. 24 (1) (2022) 88–122, https://doi.org/10.1109/COMST.2022.3141490.
[29] S. Khezr, A. Yassine, R. Benlamri, M.S. Hossain, An edge intelligent blockchain-based reputation system for iiot data ecosystem, IEEE Trans. Ind. Inf. 18 (11) (2022) 8346–8355, https://doi.org/10.1109/TII.2022.3174065.
[30] S.A. Latif, F.B.X. Wen, C. Iwendi, F.W. Li-li, S.M. Mohsin, Z. Han, S.S. Band, Ai-empowered, blockchain and sdn integrated security architecture for iot network of cyber physical systems, Comput. Commun. 181 (2022) 274–283.
[31] F. Firouzi, B. Farahani, A. Marinšek, The convergence and interplay of edge, fog, and cloud in the ai-driven internet of things (iot), Inf. Syst. 107 (2022), 101840.
[32] H. Altaheri, G. Muhammad, M. Alsulaiman, Physics-Informed Attention temporal convolutional network for EEG-based motor imagery classification, IEEE Trans. Ind. Inf. 19 (2) (2022), https://doi.org/10.1109/TII.2022.3197419.
[33] Y. Cao, X. Ren, C. Qiu, X. Wang, Hierarchical reinforcement learning for blockchain-assisted software defined industrial energy market, IEEE Trans. Ind. Inf. 18 (9) (2022) 6100–6108, https://doi.org/10.1109/TII.2022.3140878.
[34] L. Bu, Y. Zhang, H. Liu, X. Yuan, J. Guo, S. Han, An iiot-driven and ai-enabled framework for smart manufacturing system based on three-terminal collaborative platform, Adv. Eng. Inf. 50 (2021), 101370.
[35] A. Rahman, C. Chakraborty, A. Anwar, M. Karim, M. Islam, D. Kundu, Z. Rahman, S.S. Band, et al., Sdn–iot Empowered Intelligent Framework for Industry 4.0

Applications during Covid-19 Pandemic, Cluster Comput. 25 (4) (2021) 2351–2368.
[36] M.A. Rahman, M.S. Hossain, M.S. Islam, N.A. Alrajeh, G. Muhammad, Secure and provenance enhanced internet of health things framework: a blockchain managed federated learning approach, IEEE Access 8 (2020) 205071–205087.
[37] E.T. Michailidis, S.M. Potirakis, A.G. Kanatas, Ai-inspired non-terrestrial networks for iiot: review on enabling technologies and applications, IoT 1 (1) (2020) 21–48.
[38] D.C. Nguyen, P.N. Pathirana, M. Ding, A. Seneviratne, Integration of Blockchain and Cloud of Things: Architecture, Applications and Challenges, IEEE Communications Surveys & Tutorials 22 (4) (2020) 2521–2549.
[39] P. Wei, D. Wang, Y. Zhao, S.K.S. Tyagi, N. Kumar, Blockchain data-based cloud data integrity protection mechanism, Future Generat. Comput. Syst. 102 (2020) 902–911.
[40] C. Yang, L. Tan, N. Shi, B. Xu, Y. Cao, K. Yu, Authprivacychain: a blockchain-based access control framework with privacy protection in cloud, IEEE Access 8 (2020) 70604–70615.
[41] H. Xu, P.V. Klaine, O. Onireti, B. Cao, M. Imran, L. Zhang, Blockchain-enabled resource management and sharing for 6g communications, Digital Communicat. Networks 6 (3) (2020) 261–269.
[42] M. Hasan, A. Rahman, M.J. Islam, Distb-cvs: a distributed secure blockchain based online certificate verification system from Bangladesh perspective, in: 2020 2nd International Conference on Advanced Information and Communication Technology (ICAICT), 2020, pp. 460–465, https://doi.org/10.1109/ICAICT51780.2020.9333523.
[43] A. Rahman, M.J. Islam, F.A. Sunny, M.K. Nasir, Distblocksdn: a distributed secure blockchain based sdn-iot architecture with nfv implementation for smart cities, in: 2019 2nd International Conference on Innovation in Engineering and Technology (ICIET), 2019, pp. 1–6, https://doi.org/10.1109/ICIET48527.2019.9290627.
[44] S. Singh, I.-H. Ra, W. Meng, M. Kaur, G.H. Cho, Sh-blockcc: a secure and efficient internet of things smart home architecture based on cloud computing and blockchain technology, Int. J. Distributed Sens. Netw. 15 (4) (2019), 1550147719844159.
[45] H.L. Cech, M. Großmann, U.R. Krieger, A fog computing architecture to share sensor data by means of blockchain functionality, in: 2019 IEEE International Conference on Fog Computing (ICFC), IEEE, 2019, pp. 31–40.
[46] S. Tuli, R. Mahmud, S. Tuli, R. Buyya, Fogbus: a blockchain-based lightweight framework for edge and fog computing, J. Syst. Software 154 (2019) 22–36.
[47] G. Deep, R. Mohana, A. Nayyar, P. Sanjeevikumar, E. Hossain, Authentication protocol for cloud databases using blockchain mechanism, Sensors 19 (20) (2019) 4444.
[48] Z. Li, A.V. Barenji, G.Q. Huang, Toward a blockchain cloud manufacturing system as a peer to peer distributed network platform, Robot. Comput. Integrated Manuf. 54 (2018) 133–144.
[49] E. Gaetani, L. Aniello, R. Baldoni, F. Lombardi, A. Margheri, V. Sassone, in: Blockchain-based Database to Ensure Data Integrity in Cloud Computing Environments, ITASEC, 2017, pp. 146–155.
[50] P.K. Sharma, S. Singh, Y.-S. Jeong, J.H. Park, Distblocknet: a distributed blockchains-based secure sdn architecture for iot networks, IEEE Commun. Mag. 55 (9) (2017) 78–85.
[51] H.-C. Hsieh, C.-S. Lee, J.-L. Chen, Mobile edge computing platform with container-based virtualization technology for iot applications, Wireless Pers. Commun. 102 (1) (2018) 527–542.
[52] J.Q. Navid Rajabi, Sdiobot: a software-defined internet of blockchains of things model, international journal of internet of things, Int. J. Internet Things 8 (2019) 17–26.
[53] J.H. Park, J.H. Park, Blockchain security in cloud computing: use cases, challenges, and solutions, Symmetry 9 (8) (2017) 164.
[54] M. Rehman, N. Javaid, M. Awais, M. Imran, N. Naseer, Cloud based secure service providing for iots using blockchain, in: 2019 IEEE Global Communications Conference (GLOBECOM), IEEE, 2019, pp. 1–7.
[55] 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.
[56] A. Attkan, V. Ranga, Cyber-physical security for iot networks: a comprehensive review on traditional, blockchain and artificial intelligence based key-security, Complex Intell. Syst. 8 (2022) 3559–3591.
[57] A. Rahman, M.J. Islam, Z. Rahman, M.M. Reza, A. Anwar, M.P. Mahmud, M.K. Nasir, R.M. Noor, Distb-condo: distributed blockchain-based iot-sdn model for smart condominium, IEEE Access 8 (2020) 209594–209609.
[58] J. Medved, R. Varga, A. Tkacik, K. Gray, Opendaylight: towards a modeldriven sdn controller architecture, in: Proceeding of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks 2014, IEEE, 2014, pp. 1–6.
[59] A. Rahman, M.K. Nasir, Z. Rahman, A. Mosavi, S. Shahab, B. Minaei-Bidgoli, Distblockbuilding: a distributed blockchain-based sdn-iot network for smart building management, IEEE Access 8 (2020) 140008–140018.
[60] A. Rahman, M.J. Islam, A. Montieri, M.K. Nasir, M.M. Reza, S.S. Band, A. Pescape, M. Hasan, M. Sookhak, A. Mosavi, Smartblock-sdn: an optimized blockchain-sdn framework for resource management in iot, IEEE Access 9 (2021) 28361–28376.
[61] K.M. Shayshab Azad, N. Hossain, M.J. Islam, A. Rahman, S. Kabir, Preventive determination and avoidance of ddos attack with sdn over the iot networks, in: 2021 International Conference on Automation, Control and Mechatronics for Industry 4.0 (ACMI), 2021, pp. 1–6, https://doi.org/10.1109/ACMI53878.2021.9528133.
[62] A. Yazdinejad, R.M. Parizi, A. Dehghantanha, Q. Zhang, K.-K.R. Choo, An energy-efficient sdn controller architecture for iot networks with blockchain-based security, IEEE Transact. Serv. Comput. 13 (4) (2020) 625–638.
[63] B.-S. Lin, Toward an ai-enabled o-ran-based and sdn/nfv-driven 5g& iot network era, Netw. Commun. Technol. 6 (1) (2021) 6–15.
[64] L.D. Xu, E.L. Xu, L. Li, Industry 4.0: state of the art and future trends, Int. J. Prod. Res. 56 (8) (2018) 2941–2962.
[65] Y. Liu, Q. Lu, S. Chen, et al., Capability-based iot access control using blockchain, Digital Communicat. Networks 7 (4) (2021) 463–469.
[66] N. Ye, J. Yu, A. Wang, R. Zhang, Help from Space: Grant-free Massive Access for Satellite-Based Iot in the 6g Era, Digital Communications and Networks 2 (8) (2022) 215–224.