e-ISSN 2320 –7876 www.ijfans.org
Vol.11,S. Iss.4, 2022
 UGC CARE Listed (Group -I) Journal

Study On Integration Of Blockchain And Big Data Challenges Cloud Computing

Anand Deepak George Donald*
*LNCT University Bhopal

***Corresponding Author:**Anand Deepak George Donald

*LNCT University Bhopal

Abstract

The blockchain technology is sweeping the globe. Blockchain has emerged as a disruptive technology for the future generation of multiple industrial applications because to its decentralised, transparent, and secure nature. Cloud of Things, which is possible by the marriage of cloud computing with the Internet of Things, is one of them. Considering the need for security and efficiency as a problem, this paper proposes a safe and efficient smart home design that combines blockchain and cloud computing technologies to provide a comprehensive solution. The decentralised nature of blockchain technology allows it to provide processing services and create transaction copies of obtained sensible user data from smart homes. Blockchain, a distributed ledger technology that provides an immutable log of transactions recorded on a distributed network, has lately gained popularity as the underlying technology of cryptocurrencies and is revolutionising data storage and processing in computer network systems. Blockchain is seen as a possible option for future data-driven networks (DDNs) to provide safe data storage, sharing, and analytics, user privacy protection, strong, trustworthy network governance, and decentralised routing and resource management..

Keywords:Integration, Blockchain, Big Data,Cloud , Computing

INTRODUCTION

Cloud computing has five distinct properties. On-demand self-service is when users may supply network storage capabilities on their own time. Broad network access provides service via a network that may be accessed using conventional procedures to promote many client platforms. Using a multi-tenant approach, resource pooling allocates the majority of its computing resources to service a large number of customers. When resources are owned, managed, and optimised via metering capabilities, it is referred to as measured service. Elastic scalability refers to the capacity to adjust IT resources as required to meet fluctuating demand. When an application, for example, requires extra servers, it may automatically grow to meet demand..

1) Security of Data

The majority of cloud providers maintain data protection by using security methods. However, data leaking does occur in rare instances. Previously, there was a data leakage problem in ICloud, where much of the data of celebrities was exposed to the public. It seems that maintaining data online in the cloud allows data access without the user's knowledge. The major issue that prevents businesses from utilising the cloud and its services is security..

2) Downtimes

Cloud services are typically always accessible, however some of them have planned timeouts. For the time being, they have put a halt to their services in order to perform routine maintenance. Some of the services are only available at certain times of the day.

3) Limited Control
Users of the cloud will have minimal control over their data. They have the most control over virtual computers in IaaS (Infrastructure as a Service), where they may configure them to meet their demands..[1]

Cloud Deployment Models
Public Cloud: The public cloud is a service that allows several clients to collaborate on servers that are owned and managed by providers. When obtained dynamically, the cloud infrastructure is available to the public and may be utilised by several businesses. These clouds are hosted and maintained by cloud companies. For a short-term extension, the cloud provider may host the client to reduce customer risk and expense. Examples include Microsoft Azure and Google App Engine..

Private Cloud: This is primarily developed to meet the needs of single customers, giving data ownership, security, and client-dedicated service. It is used to install customer-owned infrastructure and applications. When compared to a public cloud, it is more secure and cost-effective. In private clouds, security regulations and bandwidth limits are in place. Clients may optimise user access and limit the networks that can be utilised in the private cloud. The finest example of a private cloud is the Eucalyptus System..

Hybrid Cloud: It's the equivalent of combining two or more cloud deployment models. Hybrid cloud delivers on-demand assistance as well as externally delivered scalability. These are largely focused on private data centres, although they rely on public cloud services to provide computing. A well-built hybrid cloud may aid in the provision of security services, but the challenge is in efficiently implementing and managing such a system. A good example of a hybrid cloud is Amazon Web Services..[1]

Blockchain, CoT, and Integration Motivation
The background information of blockchain and CoT is initially introduced in this part. The rationale for combining these two technologies are then presented..

A. Blockchain and Cloud of Things
1) Blockchain: Blockchain is best known as the technology that powers the virtual currency Bitcoin, which was created in 2008 by a mysterious figure known only as Satoshi Nakamoto. In a word, the blockchain is a peer-to-peer network that serves as a public, trustworthy, and shared ledger. This new technology has lately been a hot subject among experts, with some arguing that it has the potential to revolutionise blockchain-based applications beyond Bitcoin.

Smart Contract
Szabo coined the term "smart contract" in 1994. Before the emergence of blockchain technology, smart contracts were not widely implemented due to a lack of a trustworthy execution environment. People are paying greater attention to smart contracts, which are a vital and essential aspect of distributed ledger technology, thanks to the fast growth of distributed ledger technology, particularly the large-scale deployment and use of blockchain.
Smart contracts are a kind of computer protocol that can execute, enforce, verify, and limit the execution of its instructions on its own. It enables transactions between untrusted or anonymous parties to be completed without the involvement of a trustworthy third party. These are traceable and irrevocable transactions. A smart contract is made up of four parts: value, address, function, and state. The transaction is accepted as input, the relevant code is run, and an output event is triggered; the state then changes based on the functional logic. The smart contract's contents, including circumstances that trigger contract execution, state transition rules, and liability for contract violation, are all agreed upon in advance by all parties. After that, the smart contract is distributed as a code on the blockchain. The smart contract will then be triggered and executed automatically once the requirements have been met..[3]

Big Data Challenges and Revolution in Smart Manufacturing

As industry evolved in the second decade of the new century, analytics' next-generation began to improve as well. Increased device complexity necessitated revolutions in manufacturing techniques; for example, we now design 3D devices rather than 2D, and novel devices such as FinFET were invented. The second phase was driven by new market forces that pushed for lower-power, quicker, and smaller devices. These gadgets make use of Internet of Things (IoT) technology. This method is used to set up devices that are linked over the Internet. Data gathering and analysis from many sources—feedback, production, enterprise, requests, and so on—improved the smart manufacturing decision-making process. Manufacturers and consumers supplied comments and points of view about the items throughout these developments, which helped the manufacturers enhance product quality, design, and other aspects. Big data analysis enables a manufacturer to uncover consumer preferences and product faults in real time, enhancing the predictive smart manufacturing potential of data-driven marketing..[2]

Blockchain-Based Frameworks for IoT Security and Privacy

As an alternate approach, researchers have been creating blockchain technology to solve the privacy and security problems in the IoT. , which discusses the deployment of different privacy-preserving techniques in blockchain-based IoT systems. Encryption, anonymization, private contracts, mixing, and differential privacy are examples of these tactics. The study's authors examine blockchain technology and applications for IoT systems, as well as how blockchain approaches may be used to solve security issues in IoT systems. The absence of a complete standard architecture, cloud server availability, capacity, manipulation susceptibility, and cost constraints are identified as key issues with the use of blockchain technology in IoT.

The Lightweight Scalable Blockchain (LSB) is introduced in order to improve IoT device privacy and security. With the blockchain-based framework implementation powered by devices with substantial compute capabilities, an overlay network is suggested to accomplish decentralisation and retain end-to-end security and anonymity..[4]

OBJECTIVES OF THE STUDY

1. To study on blockchain-based network architecture.
2. To study on big data challenges and revolution in smart manufacturing

IoT smart home challenges

***Security and privacy*:**The communication of real-world items poses significant trust, security, and privacy issues. The Internet of Things has already been subjected to several security concerns and assaults. Due to massive data transfers, adversaries such as man-in-the-middle (MitM) attacks and DoS/DDoS attacks may target vital data flows in the network. Data privacy difficulties and monitoring devices for phones and autos are among the numerous unique privacy challenges posed by the Internet of Things. Furthermore, speech recognition is being combined to actively transfer data to cloud storage for processing while listening to conversations..

***Scalability and access control*:**Scalability is regarded to be one of the primary issues encountered by the middleware architecture since IoT enables a large number of devices that connect and interact with one another. As a result, in order to work properly in a small and big IoT environment, a trustworthy middleware is essential to control the number of devices and efficiently address scaling difficulties. Users may have access to the resources of the IoT system via access control. The system confronts access control issues due to a growth in the number of devices as well as resource demand, as well as poor bandwidth between devices and the Internet. Furthermore, due to the large number of resources and topics, the access control mechanism should be expandable in terms of structure, size, and users..

***Availability and reliability*:**To administer and monitor the IoT infrastructure in a self-manageable manner, dynamic and adaptable features are necessary. This will provide a long-term answer to the dynamic and robust connection's availability and dependability. Many experts believe that IoT availability is directly tied to dependability requirements. The IoT system must not only provide the application with the appropriate degree of performance, but it must also be flexible enough to maintain the acceptable level of availability..

***Confidentiality and integrity*:**Confidentiality refers to the safeguarding of information, particularly when it is communicated through a public network. It protects consumers' privacy and keeps their personal information secure. To achieve high anonymity, confidentiality requires effective cryptography and key management. Despite the existence of various solutions, there are still assaults on secrecy that disclose routing information and data transmission. In a smart home setting plagued by integrity challenges, integrity guarantees that no data is tampered with. An attacker may alter observed data while it is being stored in a node or travelling via the network. [5]

Security and privacy issues in CPSS

CPSS are more vulnerable to targeted assaults due to their more complicated systems and diverse networks. Cyberspace, physical space, and social space are all included in the CPSS. Multiple connection sources, such as GPS in social space, location data from a user's portable device, or user authentication information in cyberspace, might be used by malicious users to attack CPSS. A malevolent attacker might eavesdrop on the sensitive information if acceptable security and privacy protections are absent. Security flaws have been discovered in an increasing number of cyber physical systems, including the electronic grid, smart transportation systems, and medical systems. Many attacks arise as a consequence of these weaknesses, causing serious concerns about security and privacy in terms of integrity, availability, and authenticity in CPSS. The following are some examples of attacks:

Eavesdropping: CPS are especially prone to traffic analysis eavesdropping, as well as capturing monitoring data conveyed in the sensor network acquired throughout the monitoring process. The privacy of patients' personal health status data sent to the system is likewise jeopardised by eavesdropping attacks.

Attacks on keys that have been compromised: In reality, even if the procedure is complicated and resource-intensive, an attacker may get a key. An adversary, for example, may seize a sensor and use reverse engineering to figure out the internal key. An attacker may fool a genuine sensor node into matching a key with another sensor by impersonating one.

DoS attack: A CPS occurs when sensing, processing, and communication technologies are embedded in a physical system. An attacker may establish the following scenario after gaining access to the CPS network: Overload the controller or the whole sensor network with traffic until it shuts down due to an overload. Inappropriate data provided to the controller or system network causes incorrect shutdown or service behaviour. Block traffic in order to prevent authorised system components from accessing network resources.

Methodology for detecting MCA

MCA is essential in the area of data analysis since it uses a feature extraction approach to extract features from genuine and authentic data. The geometric correlation between network traffic functions is extracted using this method. 25 As indicated in Figure 1, the whole detection procedure is divided into three steps.

Step 1: At first, fundamental features are created in a predetermined interval from admittance traffic.

Step 2: MCA used the triangular area generating module to distinguish the co-relationship between two distinct characteristics.

Step 3: Data analysis and decision-making based on the training and testing phases.

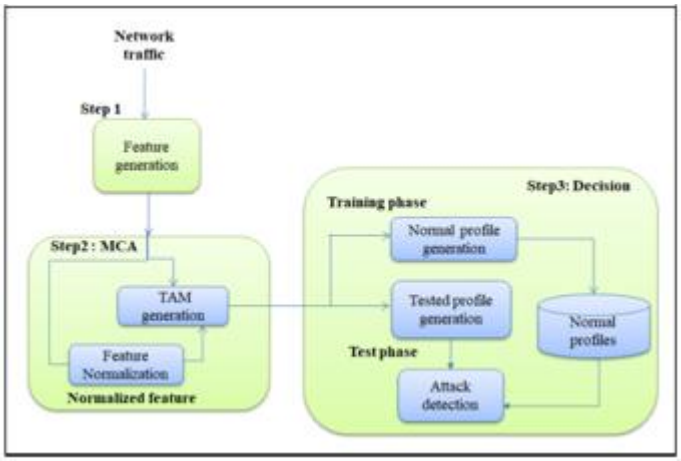

Figure 1. MCA detection approach.

Existing Works on Blockchain-based Network Architecture.
Many academics have looked at incorporating blockchain technology into other network designs. Reference proposes a paradigm for a next-generation blockchain network (NGBN) based on peer-to-peer interactions. The blockchain network layer (BNL) combines the physical and application layers into a unified networking layer that includes encryption, storage, traffic balancing, token management, and consensus to provide safe data transport with minimal latency. In addition, various studies have looked at ways to link blockchian with current frameworks like SDN and cloud computing to improve the network's design and functionality in order to deliver safe and decentralised services in common communication scenarios..

(1) Blockchain-based SDN architecture.
Weng et al. in Reference offer a secure blockchain-based SDN network architecture, which comprises of the data plane, blockchain plane, control plane, and application plane, to address security concerns in SDN. The control plane's blockchain plane enables resource-recording and resource-sharing functionality across numerous controllers. The blockchain records all application flows and network events connected with the corresponding network conditions as transactions. Multiple controllers in the underlying blockchain are in charge of recording network data from the application plane and data plane as transactions into the blockchain in the control plane. To ensure low latency and prevent temporary forks, Byzantine fault tolerance (BFT) protocols such as the Ripple network are used.

A distributed blockchain-based network architecture for optical networks, as well as two distributed multi-controller credible routing (MCR) schemes for software-defined data centre optical networks, are detailed in Reference. Data centres are connected to multi-domain elastic optical networks, which allocate compute, storage, and optical spectrum resources. Each data centre may accept trustful cross-domain lightpaths based on the blockchain network, and these domains are software-defined and modified by cooperating SDN controllers..
(2) Blockchain-based cloud computing architecture.
The device layer, fog layer, and cloud layer are proposed by Sharma et al. in Reference as a distributed blockchain-based cloud architecture at the network's edge. The device layer sends the filtered raw data to the SDN-enabled fog layer, where each SDN controller is responsible for network management and all SDN controllers are linked in a distributed way via a blockchain. When compute resources are inadequate, the fog nodes send processed data to the dispersed cloud and device layers, allowing them to access and offload computational chores to the cloud. A consensus protocol is presented to combine the benefits of both Proof of Work (PoW) and Proof of Stake (PoS) consensus mechanisms by using a 2-hop blockchain approach to increase the speed of computing, data transmission, and storage in the blockchain..

(3) Blockchain-based IoT architecture.

A blockchain-based multi-layer method for IoT is presented in Reference, which comprises of an edge layer and a high-level layer. The edge layer is a local area network that consists of a number of nodes and a central node that provide interfaces to the high-level layer for addressing, bidirectional data transmission, and participation in high-level layer activities. All nodes in the high-level layer are data-independent, with complete replica records being shared throughout the blockchain. They communicate with the edge layer over a common interface that is unaffected by the activity of the edge nodes..

(4) Blockchain-based VANET architecture.

Zhang et al. introduce a security blockchain-based VANET with mobile edge computing in Reference for vehicular communication networks. The perception layer, edge computing layer, and service layer make up the architecture. The perception layer, which connects automobiles and roadside units (RSUs) through blockchain, ensures that sent data is secure. The edge computing layer, as well as the service layer, supply computational resources and cloud services. The perception layer's edge computing layer is in charge of managing a high number of transactions and other computation-intensive operations, while the service layer is in charge of data security recording, such as traffic violation history, traffic accident information, and so on..[6]

CONCLUSION

Cloud computing has expanded the smart-home area, allowing consumers to benefit from cloud providers. The efficient broker handled the end users' selection of energy-efficient service providers, while blockchain technology offers a peer-to-peer network in which untrustworthy nodes communicate with the efficient processing network. In a local smart home network and an overlay network, we employed blockchain technology's encryption and hashing algorithm to ensure secrecy and integrity. Authorization is accomplished via the use of a policy header and a shared key between the device and the miners, while availability is ensured by approved transactions between the device and the miners. The suggested method addresses IoT security issues such as framework privacy, authentication, heterogenicity, and adaptability, as well as network scalability, among others. Four current methods were compared to the suggested hybrid clustering technique. The simulations show that the suggested approach exceeds the competition in terms of network load, network coverage, and distances, among other performance measures. The suggested multi-layer blockchain-based framework's performance was assessed..

REFERENCES

- M. LAWANYA SHRI (2016) “Blockchain Based Cloud Computing: Architecture and Research Challenges”November 2020 IEEE Access 8 DOI:10.1109/ACCESS.2020.3036812
- Ruonan Wang (2017) “The Applications of Blockchain in Artificial Intelligence”Volume 2021 |Article ID 6126247 | https://doi.org/10.1155/2021/6126247
- Marco Picone (2018) “Integration of Blockchain, IoT and Machine Learning for Multistage Quality Control and Enhancing Security in Smart Manufacturing”doi: 10.3390/s21041467
- Fakhrul Alam (2015) “Multi-Layer Blockchain-Based Security Architecture for Internet of Things” Security Architecture for Internet of Things. Sensors 2021, 21, 772. https:// doi.org/10.3390/s21030772
- Saurabh Singh(2015) “SH-BlockCC: A secure and efficient Internet of things smart home architecture based on cloud computing and blockchain technology” First Published April 23, 2019 Research Articlehttps://doi.org/10.1177/1550147719844159
- ZEHUA WANG, (2015) “Blockchain-empowered Data-driven Networks: A Survey and Outlook”ACM Comput. Surv., Vol. 54, No. 3, Article 58, Publication date: April 2021. DOI: https://doi.org/10.1145/3446373

- Meng, Weizhi (2017) "SH-BlockCC: A secure and efficient Internet of things smart home architecture based on cloud computing and blockchain technology"International Journal of Distributed Sensor Networks, 15(4). https://doi.org/10.1177/1550147719844159
- L. Xie, Y. Ding, H. Yang, and X. Wang, "Blockchain-based secure and trustworthy internet of things in SDN-enabled 5G -vanets," IEEE Access, vol. 7, pp. 56 656–56 666, 2019.
- Z. Li, A. V. Barenji, and G. Q. Huang, "Toward a blockchain cloud manufacturing system as a peer to peer distributed network platform," Robotics and Computer-Integrated Manufacturing, vol. 54, pp. 133– 144, 2018.
- N. Mohamed, J. Al-Jaroodi, and S. Lazarova-Molnar, "Leveraging the capabilities of industry 4.0 for improving energy efficiency in smart factories," IEEE Access, vol. 7, pp. 18 008–18 020, 2019.
- A. Bahga and V. K. Madisetti, "Blockchain platform for industrial internet of things," Journal of Software Engineering and Applications, vol. 9, no. 10, p. 533, 2016.
- G. Perboli, S. Musso, and M. Rosano, "Blockchain in logistics and supply chain: A lean approach for designing real-world use cases," IEEE Access, vol. 6, pp. 62 018–62 028, 2018