Empowering Cloud Security System with Block chain Technology

Muhammad Amjad[1], Muhammad Zonain[2], Muhammad Akhter[3]

[1]University of Management and Technology (UMT), Lahore, 53000, Pakistan
[2]Bahauddin Zakria University (BZU), Multan, 66000, Pakistan
[3]National College of Business and Economics, Lahore (Multan Campus), 66000, Pakistan
[*]Corresponding Author: Muhammad Amjad. Email: v31324@umt.edu.pk

Abstract: Cloud computing (CC) empowers companies to minimize the entire costs by subcontracting their mandatory facilities. Consequently, it delivers a new task of information safety involving consistency, honesty, and privacy since of subcontracting. Cloud protection is creating a vital discriminator and viable advantage among cloud services. Today, One of the most popular innovations that can address security issues with cloud computing is the usage of Blockchain (BC). BC is a decentralized data management technology that offers data integrity, protection, and anonymity without the involvement of a third party. This research shows a BC-based security system for cloud computing and provides solutions in order to address security concerns. The proposed blockchain-based approach may be applied to prevent data leakage, remove the single point of failure, and create IoT trust relationships.

Keywords: Blockchain technology (BCT); cloud computing; cloud security system

1 Introduction

Blockchain Technology (BCT) is highly valued by many stakeholders, including government, real estate, infrastructure, finance, and healthcare sectors. Blockchain-based systems are based on a dispersed, combined, and fault-lenient ledger framework accessible to all network members but not under any network member's control. As a result, the blockchain network's service is not dependent on a centralized, reliable third party. BC may also be employed to increase community welfare and give consumers access to sustainable energy. Additionally, each blockchain network user has a copy of every previous transaction, granting network members access to data and confirming the process's high accessibility. BC is essentially a streamlined method of payment verification. A blockchain has taken the place of the server, eliminating the need for a centralized authority. Additionally, the adherents who mutually uphold the transaction records and eventually check the transactions using peer-to-peer connections have made transactions simpler due to blockchain [1].

On the other side, the cloud structure uses a model to offer on-request log on to a collective pool of programmable sources that may be quickly provisioned and issued with no preservation requirements. A group of network-enabled services known as "cloud computing" provide adaptable, affordable, and frequently personalized computing infrastructures that are widely accessible. Numerous organizations and researchers have identified the framework for cloud computing. The core and the management stack are the two components that make up the entire structure. The core stack consists of infrastructure, platforms, and applications. The setup layer comprises tangible and online networking, processing, and storage facilities. The platform layer, which can be divided into numerous sub-layers, is the most intricate part of the system. Task arranging and/or operation forwarding, for instance, are the responsibilities of a computing framework. Infinite caching and storage are possible with a storage sub-layer. The application server and other components provide on-demand operation or adaptive administration to logically assist the same fundamental function as earlier, preventing any features from becoming the system's bottleneck.

It depends upon the basic components and sources. The app will enable large-scale distributed transfers and big data processing. Across web services or other interfaces, all layers offer external services. CC capacity is standard with that of numerous techniques. The basic idea of CC is to expand the cloud's capability in order to reduce the processing load on the customer. The ultimate goal is to improve the customer interface to serve as an input structure for the robust computing resources of cloud computation [2].

Multiple issues about confidentiality and safety arise because of the unique architectural features of cloud computing. Customers' control over their data is diminished when it is sent to the cloud. Additionally, because subscribers lack the actual information, basic information safety is not feasible. Therefore, issues with security and privacy must be resolved. Blockchain technologies would be advantageous for cloud services with a strong partiality for data derivation assurance and support cloud inspecting. The most current study found that safety issues are the highly annoying cloud computing issues. A reliable encryption method to ensure a protected data storing method, stringent access controls, and a reliable and effective collection of user information are all features that the cloud is designed to have. BCT has concerned great interest in clarity, safety, and devolution [3].

2 Literature Review

Many researchers have previously worked on BC-based security systems for cloud computing. This section highlights some of their works.

Sharma et al. highlighted that the use of blockchain for secure cloud storage could be discovered in this research [4]. Between 2010 and 2019, they thoroughly analyzed BCT and cloud computation for cloud storage safety.

The authors of this study [5] provide a detailed overview of several approaches for using blockchain technologies to address issues with data honesty in cloud computation. They also found that BC focuses on several issues, including security issues with cloud data storing, as it was constant, dispersed, affordable, clear, and valuable to work. They solved the problem of secure cloud data storage capacity with blockchain implementation.

Another work by Gai et al. covered integrating BCT with already-in-use infrastructure technologies to enable cloud datacenter reengineering. They roughly addressed three technical dimensions in their research. In this study, safety was a crucial technical concern, and security systems and searchable encrypted data were examined. Eventually, they considered the achievement of cloud data centers that supported or participated in BCT from both a software and hardware perspective. They started by examining the methodology and analyzing Blockchain-as-a-Service (BaaS), a developing blockchain service model relevant to the cloud.

In this research [6] present that Blockchain technologies are being used to address some problems with cloud computing. By offering a protocol for securely utilizing and removing the blockchain, their research concentrated on the way to deliver security. They found that efficiency assessments are frequently vital in terms of extra safety because of the way that a sizable amount of information was dispersed.

The Proof of Work (PoW)-based BC model used BC was discussed by [7]. Their study goal to provide a thorough overview of BCT's quickly gaining popularity. Before going on to a PoW-based BC model that resolves the Function-as-a-Service conundrum, they discussed various secrecy matters and exactly how they might be focused in cloud computing.

Another study by [8] looked at the potential impact of three new paradigms on cloud computing systems: BC, the Internet of things, and artificial intelligence. They also attracted international specialists to examine the recent state and upcoming instructions of cloud computing and identified several technologies that were powering these paradigms. In order to investigate the impact of new paradigms and technologies on the development of cloud computing, they also suggested a theoretical model for cloud computing.

Most of the approaches have been used while employing and constructing several smart as well as intelligent frameworks like machine learning approaches [9-12] Fuzzy Inference systems [13-15], Particle Swarm Optimization (PSO) [16], Fusion based approaches [17],cloud computing [18-20] and security systems algorithms [21] that may provide assistance in designing emerging solutions for the rising challenges in designing smart cloud-based monitoring management systems.

3 Proposed Methodology

Smart cities leverage technology to enhance the quality of life for residents and create more sustainable, efficient, and livable urban environments. In a smart city, IoT devices and sensors are used to collect and analyze data in real-time, enabling city administrators to make data-driven decisions and optimize city services. This data is then stored in large-scale data storage solutions and processed by cloud computing facilities for efficient service provision. One of the main challenges in implementing smart city services is ensuring the security and privacy of the data collected and processed. Blockchain technology offers a secure and transparent solution for the management of data in a decentralized manner. This allows for the creation of a secure, tamper-proof ledger that can be used to store sensitive information, such as financial transactions, without the risk of data tampering or theft.

BCoT is a combination of blockchain technology and cloud computing that aims to address the challenges faced by smart cities. By integrating blockchain technology into cloud computing, BCoT provides a secure and efficient platform for the management of data and the delivery of smart city services. It allows for the creation of decentralized, distributed networks that can be used to store and process data securely and efficiently. One of the key benefits of BCoT is that it enables the creation of a secure, decentralized infrastructure that can be used to support smart city services. For example, BCoT can be used to provide secure, decentralized data storage and processing for smart city applications, such as energy management systems, traffic management systems, and waste management systems.

Another benefit of BCoT is that it provides a secure and transparent platform for the management of financial transactions. For example, BCoT can be used to create decentralized financial systems that allow for the secure transfer of funds between individuals and organizations without the need for intermediaries. In conclusion, the integration of blockchain technology and cloud computing through BCoT offers a promising solution for addressing the challenges faced by smart cities. By providing a secure, decentralized, and efficient platform for the management of data and the delivery of smart city services, BCoT has the potential to revolutionize the way that cities are managed and operated.

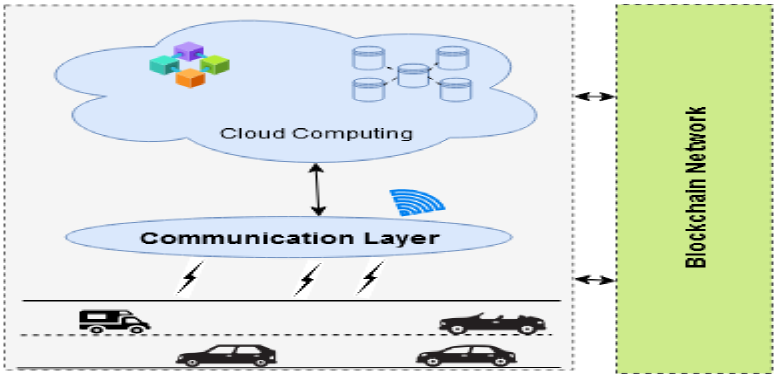

Figure 1: Proposed model

Figure 1 illustrates the use of BC in vehicular communication management to achieve high levels of security, such as user verification through agreements and data privacy through cryptography. The blockchain layer is utilized to code and attach vehicular data to units through a harmonizing process within the BC network. Furthermore, BC enables the creation of a secure peer-to-peer connection for seamless communication and shared trust in the exchange of information for service administration and value transfer.

This study proposes the integration of multiple clouds through the use of BC to establish a synchronizing system. The data from various sources can be efficiently linked across the clouds, providing secure service management, value transfer, and collective trust within the communication layer. BC is utilized to facilitate peer-to-peer connections between multiple cloud networks of vehicles with enhanced security levels.

4 Limitations & Future Recommendations

Despite its potential, blockchain is not a perfect technology and it is not suitable for all applications. One of its major limitations is the lack of public awareness about its benefits and how it can be used in practical applications. Additionally, there are issues with data integrity, key management, and scalability that must be addressed in order to ensure that blockchain-based applications can be used effectively. This research presents an innovative approach for overcoming these limitations by proposing a reputation computation model that is based on non-quantitative identifiers. This model provides a means for analyzing these identifiers, which are critical for building trust relationships in the Internet of Things (IoT) domain. The proposed model is implemented using blockchain technology and provides a secure and transparent method for managing and analyzing these non-quantitative identifiers.

The proposed model can play an important role in preventing data leakage, removing single points of failure, and creating trust relationships in the IoT. By utilizing blockchain technology, the model can provide a decentralized, trustless platform for managing and analyzing non-quantitative identifiers, thereby mitigating the limitations of blockchain technology. In the future, the proposed model has the potential to become a key component of IoT security and trust management.

5 Conclusion

This paper presents that incorporating blockchain technology into cloud security systems can greatly enhance the security and privacy of data collected and managed in the cloud. By using blockchain to create a secure, decentralized ledger, sensitive information can be stored and managed without the risk of data tampering or theft. Additionally, blockchain technology enables secure, peer-to-peer transactions and communication, ensuring that information is shared only with authorized parties.

The use of blockchain in cloud security systems has the potential to revolutionize the way that sensitive data is managed in the cloud. Through its decentralized nature, blockchain provides a secure and transparent platform for the management of information, making it ideal for use in cloud security systems. As such, the integration of blockchain technology into cloud security systems offers a promising solution for addressing the challenges of cloud security and protecting sensitive data in the cloud.

6 References

[1] Gong, J., Navimipour, N.J., 2022. An in-depth and systematic literature review on the blockchain-based approaches for cloud computing. Cluster Comput. 25, 383–400.

[2] Souri, A., Rahmani, A.M., Navimipour, N.J., Rezaei, R., 2020. A hybrid formal verification approach for QoS-aware multi-cloud service composition. Cluster Comput. 23, 2453–2470.

[3] Sharma, P., Jindal, R., Borah, M.D., 2021. Blockchain Technology for Cloud Storage. ACM Comput. Surv. 53, 1–32.

[4] Gai, K., Guo, J., Zhu, L., Yu, S., 2020. Blockchain Meets Cloud Computing: A Survey. IEEE Commun. Surv. Tutorials 22, 2009–2030.

[5] Chayal, N.M., Patel, N.P., 2021. Review of Machine Learning and Data Mining Methods to Predict Different Cyberattacks, Lecture Notes on Data Engineering and Communications Technologies.

[6] Murthy, C.V.N.U.B., Shri, M.L., 2020. A Survey on Integrating Cloud Computing with Blockchain. Int. Conf. Emerg. Trends Inf. Technol. Eng. ic-ETITE 2020 1–6.

[7] Prianga, S., Sagana, R., Sharon, E., 2018. Evolutionary Survey on Data Security in Cloud Computing Using Blockchain. 2018 IEEE Int. Conf. Syst. Comput. Autom. Networking, ICSCA 2018 1–6.

[8] Gill, S.S., Tuli, Shreshth, Xu, M., Singh, I., Singh, K.V., Lindsay, D., Tuli, Shikhar, Smirnova, D., Singh, M., Jain, U., Pervaiz, H., Sehgal, B., Kaila, S.S., Misra, S., Aslanpour, M.S., Mehta, H., Stankovski, V., Garraghan, P., 2019. Transformative effects of IoT, Blockchain and Artificial Intelligence on cloud computing: Evolution, vision, trends and open challenges. Internet of Things (Netherlands) 8, 100118.

[9] Areej Fatima 1, M., Adnan Khan 1, Sagheer Abbas 1, M.W. 1, 2019. Evaluation of Planet Factors of Smart City through Multi-layer Fuzzy Logic (MFL) 11, 51–58.

[10] Ghazal, T.M., Noreen, S., Said, R.A., Khan, M.A., Siddiqui, S.Y., Abbas, S., Aftab, S., Ahmad, M., 2022. Energy demand forecasting using fused machine learning approaches. Intell. Autom. Soft Comput. 31, 539–553.

[11] Khan, M.F., Ghazal, T.M., Said, R.A., Fatima, A., Abbas, S., Khan, M. A., Issa, G.F., Ahmad, M., Khan, Muhammad Adnan, 2021. An iomt-enabled smart healthcare model to monitor elderly people using machine learning technique. Comput. Intell. Neurosci. 2021.

[12] Saleem, M., Abbas, S., Ghazal, T.M., Adnan Khan, M., Sahawneh, N., Ahmad, M., 2022. Smart cities: Fusion-based intelligent traffic congestion control system for vehicular networks using machine learning techniques. Egypt. Informatics J.

[13] Asadullah, M., Khan, M.A., Abbas, S., Alyas, T., Saleem, M.A., Fatima, A., 2020. Blind channel and data estimation using fuzzy logic empowered cognitive and social information-based particle swarm optimization (PSO). Int. J. Comput. Intell. Syst. 13, 400–408.

[14] Ihnaini, B., Khan, M. A., Khan, T.A., Abbas, S., Daoud, M.S., Ahmad, M., Khan, Muhammad Adnan, 2021. A Smart Healthcare Recommendation System for Multidisciplinary Diabetes Patients with Data Fusion Based on Deep Ensemble Learning. Comput. Intell. Neurosci. 2021.

[15] Saleem, M., Khan, M.A., Abbas, S., Asif, M., Hassan, M., Malik, J.A., 2019. Intelligent FSO Link for Communication in Natural Disasters empowered with Fuzzy Inference System. 1st Int. Conf. Electr. Commun. Comput. Eng. ICECCE 2019 1–6.

[16] Iqbal, K., Khan, M.A., Abbas, S., Hasan, Z., 2019. Time complexity analysis of GA-based variants uplink

MC-CDMA system. SN Appl. Sci. 1, 1–8.

[17] Ma, F., Sun, T., Liu, L., Jing, H., 2020. Detection and diagnosis of chronic kidney disease using deep learning-based heterogeneous modified artificial neural network. Futur. Gener. Comput. Syst. 111, 17–26.

[18] Bukhari, M.M., Ghazal, T.M., Abbas, S., Khan, M.A., Farooq, U., Wahbah, H., Ahmad, M., Adnan, K.M., 2022. An Intelligent Proposed Model for Task Offloading in Fog-Cloud Collaboration Using Logistics Regression. Comput. Intell. Neurosci. 2022.

[19] Naseer, I., 2022. Removal of the Noise And Blurriness using Global & Local Image Enhancement Equalization Techniques 1.

[20] Siddiqui, S.Y., Haider, A., Ghazal, T.M., Khan, M.A., Naseer, I., Abbas, S., Rahman, M., Khan, J.A., Ahmad, M., Hasan, M.K., Mohammed, A., Ateeq, K., 2021. IoMT Cloud-Based Intelligent Prediction of Breast Cancer Stages Empowered with Deep Learning. IEEE Access 9, 146478–146491.

[21] Saeed, S. (2023). A Customer-Centric View of E-Commerce Security and Privacy. Applied Sciences, 13(2), 1020.