A Block-chain based mechanism for securely storing data on cloud and IOT

PRIYANKA MISHRA, GANESAN R.
Computer Science Engineering
Vellore Institute of Technology
Chennai, Tamil Nadu
INDIA

Abstract: - The burgeoning paradigm of cloud computing has made a number of tools available to researchers. It is a cutting-edge technology that keeps revolutionizing many sectors in every imaginable method. It is a promising technology that gives users and researchers new perspectives, development, and many amazing factors. The integration of cloud and block-chain technology and internet of things (IOT). The benefits both service providers and customers by enabling the use of resources that can be authenticated while protecting anonymity. This joining method is distinct and environmentally. This cooperative method sheds light on the different paths or facets of computers that can solve issues other than security-related ones. The primary problem at the moment is cloud security. For service providers, it's critical to protect client privacy and avoid data loss. Using client data privacy solutions, the current review study focused on block-chain with combination of IOT and data security. In order to strengthen security and expand the power or utility of cloud systems, a comprehensive examination is also carried out. Block-chain technology has the ability to increase speed and anonymity while providing numerous advantages to cloud-based and IOT based applications.

Key-Words: - Cloud computing; Security, Block-chain, data security, IOT

Received: March 17, 2024. Revised: August 21, 2024. Accepted: September 19, 2024. Published: October 30, 2024.

1 Introduction

Users and service providers are able to distribute their resources in a wider range of ways thanks to the burgeoning technology of cloud computing. These factors impacted the decision of the researchers to give more of their thoughts and opinions to this particular field [1]. currently, when it comes to security, the safety of data, apps, services, and infrastructure comes first. The high level of scalability and capacity of cloud computing to provide data service requirements at low cost and with little effort is another advantage. This technology enables users to construct apps fast using a practical and user-defined tool. This approach could result in the application's blending by creating appropriate computing technology tools [2]. the tool, which is unique to the project and travels from beginning to end, provides end-user guidance. The "advanced side of cloud technology" refers to the area where application migration, data security, and information flow have all converged or when other technologies are employed to retreat applications [3]. The two primary purposes of the numerous tools developed using cloud computing technology must be focused on: tool development and client data protection. Numerous apps were developed as a result of the increasing demand for cloud services among users, which encouraged people to think more about new discoveries and encouraged them to repurpose outdated technology. Users and service providers both gain from this technology, which piques people's curiosity. The cloud's mechanism attracts customers primarily due to its high scalability, low cost, and minimal work [4].

Cloud computing has boosted the speed and flexibility of software evolution, but on the other hand, safety concerns have grown. Those that access information in the cloud could come under a variety of attacks [5]. The majority of those who worked for cloud service providers were accustomed to connecting with the authentication process in order to get customer information. Any insider finding out a user's login information found it difficult using block-chain technology [6]. When a user has been authenticated, a revolutionary technique called distributed ledger-based authentication stops insiders from accessing that user's data. Personal identity cards and signatures were provided to both insiders and outsiders as part of the authentication procedure, making it easy for service providers to recognise these insiders. In order to view the cloud's database, users have to authenticate first [7].

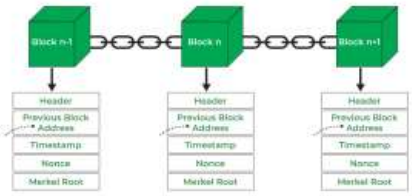

Figure 1 - Structure and Links between Block-chain Nodes

Because of its enormous demand, cloud computing has become a vital technology for meeting architecture and data service requirements at cheap cost with little effort and a high degree of flexibility, and is consequently widely employed in many sectors of the software business.[8]. Despite the rapid growth in cloud computing adoption, issues with information security are still being worked out. There were still some issues with information security that needed to be resolved that in some ways hampered the development of cloud computing. Block-chain has emerged as a crucial security solution at the moment, especially in terms of nobility, authenticity, and confidentiality [9]. This study discussed the various security characteristics of cloud computing and block-chain technology and investigated how block-chain technology might be utilized to enhance cloud computing security. Users of the cloud or clients made resource requests to cloud service providers. Clients were provided cloud storage services by this third-party provider of the cloud. The duty of delivering was delegated to Attribute Authority and third-Party auditor [10]. Personal data about users was at grave danger of being taken, assaulted, or leaked, yet there were no choices available to remove the data from this dire situation. Because users were oblivious to the recipients of their information, transparency between users and providers should be required to maintain the security of all user information [11].

Every area benefits greatly from the Internet of Things (IoT). With more functions, it is almost employed in every industry. Key security components are extremely important and must be protected because it is utilized everywhere. Block-chain is a brand-new technology that can be used to formulate these ideas. This technology is heavily utilized without the usage of a third party in order to have secure transactions between diverse objects.

2 Block-Chain Technology

When it came to using the proper Cloud services, consumers may increase confidence and ensure the safety of their data by implementing the developing and innovative technology known as blockchain. Comparing block-chain security to that of centralised databases, it may be more effective. A cryptographic hash function was employed to continuously link and authenticates records using a block's prior block, allowing block-chain to keep track of their history [12]. A distributed ledger that could record transactions and prevent harm was a Block-chain. A block-chain is often managed through a peer-to-peer network and built to prevent unauthorized tampering. Block-chain technology can offer security on par with central database data storage. [13]. Aspects of management could be used to stop attacks and damages to data storage. As a result of the Block-chain's open attribute, data could also be made transparent when applied to a situation where data disclosure is necessary [14]. Due to its effectiveness, availability, and widespread use, cloud computing has been adopted by numerous industrial sectors [15]. Block-chain improved system performance by removing numerous tools' restrictions from existing technologies [16]. A public key surrounding the unique identity of the block-chain technology, and the owner of the private key was transferred to the deserving user. The user reviews assisted with the public key's verification on behalf of the block-chain identity [17]. The Block-chain application resisted changing the existing information. The idea of an assumed arbitrary party for the verification process is eliminated. In scattered systems, where a distributed ledger and network's node-supported stage lacked a centralised controller, it also operated as node-to-node. The Block-chain technique was built on a decentralised, circulating approach, which has several advantages over specially designed authentication procedures. It was especially useful for tracking the prior records and actions of the specific user [18].

2.1 Structure of block-chain

The essential information, including the timestamp and current hash, was typically contained in a block in a block-chain. Primarily based on lists provided by sources such as data records of, for instance, financial transactions, contacts, clearances, or transaction [19]. A transaction was hashed to code after it was finished, and it was then broadcast to other nodes. Due to the large number of transaction records that were included in each node block as well as the final hash to the block header, block-chain made use of a number of creative applications to reduce the data transmission and processing unit resources. The timestamp displays the time that the block was generated. The three main subcategories of additional information were block signature, user-defined data, and nonce values [20].

2.2 Aspects of block-chain technologies

- The successful and effective operation of a blockchain system was required. Consequently,

the system's architecture was more profoundly impacted by the full potential of the block-chain technology. The block chain network has the following non-functional traits.

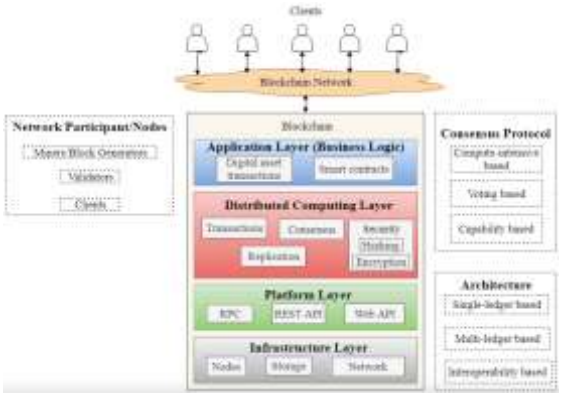

Figure 2 - Different Layers of Blockchain Nodes (Inspired From [26])

- The compatible node behaviour in the block-chain allows for the use and exchange of data at the time of a transaction. Block-chain performance improves as more nodes process data concurrently.
- Scalability refers to the capacity of the block-chain to add and remove new nodes. The three variables were mostly taken into account in terms of scalability: - Transactional Distribution Processing Rate, Size Manageability versus Latency:
- The block-chain network's resilience to failures at any node
- Every node in the network may observe the transactions made on the block chain, and the information was protected using cryptographic methods.

The block-chain network was designed to be reliable, and failure sites were identified.

2.3 Drawbacks

Block-chain technology, which is closely related to digital and virtual currency, was used by all users. However, there have been reports of other block chain security problems, including the following:

- A block-chain is a collection of sequentially connected, fundamentally formed blocks; it is possible for two separate peers to produce results during mining at the same time, which might cause a block-chain to split into two. If the peers in the Bitcoin network do not choose the block as the most recent block, the block will lose its significance and further mining would be useless. The network will follow Bitcoin peers that have more than a 50% chance of mining.
- One can create a number of forms for resolving security issues by using a versatile programming language and well-written scripts. Bitcoin contracts were applied to financial services, validation, and verification. A popular strategy that integrated the multiple-signature method was established on the framework of the script known as "multisignature."
- Bitcoin addressed the issue of using a public key's hash value after the public and private keys were encrypted. If the script holding the encryption of the public and private keys was left unlocked, it was not possible to unlock the script for bitcoin transactions. The script was unlocked by using the integrated personal key data that was saved in the bitcoin wallet. And suppose that this important data was lost, which would be very bad for bitcoin. As a result, protecting the Bitcoin wallet from hackers remained the top priority.
- The Bitcoin-related software had a severe bug that caused a problem. Even though the certified developer of the bitcoin documentation explicitly described all pertinent bitcoin activities as being extremely knowledgeable and efficient [21]

3 Blockchain Consensus Methods

A further issue for trust is anonymity, which is one of the expected block-chain advantages. It is impossible to completely guarantee the integrity of transactions that anonymous users add to a ledger. The answer is to double-check each transaction to make sure it is legitimate and not fraudulent, double-spending, or something else. Earlier than putting it into a block. A block's addition to the block chain is approved using consensus techniques. The fact that the majority of block-chain users share the same aim to preserve the integrity of the block-chain is advantageous to these consensus algorithms. In a block-chain system, transactions are properly stored on blocks and trust is built through a consensus technique. Therefore, consensus algorithms could be viewed as the basis of all transactions.

An agreed-upon set of rules is all that makes up a consensus method. The distributed nature of block-chain technology necessitates the use of a distributed consensus technique by all participants in order for the block-chain to be accepted in its current state. It is widely accepted on the block-

chain that owning more of a scarce resource gives you more control over how it is used.

If the security was breached or hacked by the attackers, an effective and trustworthy restoration of the e-wallet must be included. The settings necessary to administer and use an electronic wallet should be secure, as should the user transaction data recorded in the wallet. When the e-wallet was not in use, a technique should be needed to safely and effectively remove the remaining user information, and once that was done, the data should be discarded.

4 Necessities of Blockchain

Table 1: Necessities Of Blockchain for Modified the Design Pattern.

Need	Explanations
Scalability	Multiple million nodes that could scale up and down.
Trust	System helped to secure all the sensitive information of the users so user can trust easily on blockchain secure applications.
Resources	Users were not permitted to propose or plan in advance when using the services.
Cost	Multiple of applications, amount of services demanded varied costs based upon their usage.
Utility	The variable load should be used with careful tuning.
Performance	Depending on how many active applications are available on the system.
Reliability	Shared data in large quantities while simultaneously giving users the greatest services.

5 Policies of Blockchain Mechanisms

Prior to now, academics developed a number of user authentication control authority and multi-factor rules for complicated systems. The ledger-based authentication is a revolutionary peer-to-peer authentication policy was produced. A limited amount of insider mechanism research was found using the block-chain mechanism. By controlling the user and using the insider's data in the accessible approaches, the attacker has an advantage that may be avoided by keeping the insider's authentication information the same. If a third party is found to have violated the rules by providing authentication information, their motivation should be declared invalid. A distributed ledger-based authentication policy was implemented for the outsider with the use of block-chain technology, making it tough for them to get in. The strategical traits of insider and outsider threats were explained as threat structures became less complex as a result of the increasing efficiency brought about by the requirement for data security. Due to data transfer over the cloud, insider dangers are at their peak. Insider threat was seen to be particularly dangerous because it negatively impacted multiple significant corporations. Insider threats initiated by an attacker with strong access to the available data were the cause of all of this, which was transpiring. Additionally, because these attackers were familiar with the system design, it was simple for them to extract the important data records or establish a straightforward access point for a third party. The increased data transit over the cloud may lead to an increase in insider attacks, posing more risks. Therefore, around a third of users thought that an insider might hurt someone more than an outsider. A new set of security controls was put in place to guard against insider assaults. To safeguard and defend data from inside attackers, a number of apps were previously employed. However, this multifactor authentication led to simple password guessing, insider assaults and no session key computation by temporary device, making it easier for insiders to exploit. This agreement improves the usage of security by requiring the signature of a verified user from any of the group. One group user may invite an infinite number of people to join using their access credentials. The particular authority then provided them with a key that could be used by providing information such as their name, service, and the time [22].

6 Threats and Attacks

The bulk of agreements were implemented in order to protect against internal and external adversaries in the cloud. The employees who served as cloud service providers typically had access to all user data on the cloud. These employees benefited most from data management by collaborating closely with cloud service providers. It was quite simple to recognize and keep tabs on these internal attackers after they had successfully completed the authentication process. By using the proper authentication, activities of the attacker who remained inside may be firstly tracked. For both insiders and outsiders, authentication has to be created and kept up-to-date. Following the

implementation of this authentication, only authorized users who had been authenticated were able to access the users' data in the cloud. Attackers have on occasion benefited from managing user data for specific applications. In the event of an insider threat, the employee's duty may be modified. After engaging in insider threat, the employee shouldn't permit changing the authentication information to alter the right tracking order. Authentication was required for all users of the cloud, including machines and everyday users For both internal and external attackers, using block-chain technology, a similar authentication approach should be utilized, making it difficult for them to replace the authenticated data that has been saved. Block-chain removes a lot of programme restrictions, which also enhances gadget performance. The block-chain needed an identifying system that could only be accessed with a private key and transmitted ownership to the specified user. The user's key note or impressions were used to verify the public key that was kept in the block-chain identifying system. This block-chain methodology, which uses a decentralized approach, has significant advantages over conventional authentication methods.

7 Secure Applications for Blockchain Transactions

The block-chain technology had a significant impact in the recently rapidly expanding sector of financial technology. The implementation of block-chain as a public ledger helped to avoid hacking during the exchange of trades for digital transactions. The block-chain software can operate smoothly with the help of transactions, which can also be encrypted in accordance with the law. All user information is kept safe in a central database because of the great security provided by block-chain. The only way to prevent any kind of database harm is by taking data storage and administration into account. When data disclosure was required, it was always possible because of the features of the block chain. Groups of data chunks could continue to be listed in a specific order using a technology known as "block-chain." Data storage security was crucial for the decentralized ledger. The block-chain contains many applications, including those for money and a programmable society. Block chains are categorized into three subcategories: private, public, and group. In the case of a private block-chain, it was shown that the nodes were still part of the organization and still a part of the underlying block-chain technology. Any number of nodes could join the network and examine data relating to other nodes simultaneously in the case of a public block-chain. The nodes must be allowed to communicate their node information while still being authorized in order to join the network in the consortium block-chain, though.

A framework that combines attribute-based encryption and block-chain was suggested in order to better understand how to manage access to storage data via the cloud. This solves the key management issues with customizable attribute-based encryption and makes it more flexible because only one specified user at a time could access the data and transfer the private key to user.

8 Advantages of Blockchain Technology

The fact that all of the data from the series was saved in scrambled form was one of the biggest benefits of employing block-chain technology. Block-chain technology is made up of many different architectural levels, some of which include the application, network, contract, data, consensus, and incentive layers. The majority of the definitions for the various application cases came from an application layer. The multiple methods, including data transmission and data verification, that were part of the network layer that made up block-chain technology were its key characteristic. The top application layer's programmable smart contract and various scripts were impounded by the contract layer. For the base data block and data encryption, there are data layer constraints. The consensus layer includes several different network fetching techniques. The distribution of mechanisms, issues with mechanisms, and block increment were all enforced through an incentive layer.

Block-chain technology was used to create a secure protection for the cloud data confederacy. The users could focus on their data requirements, and the cloud service providers could manage the secrecy operation.

9 Solutions Using Blockchain Technology to Secure Data

Typically, data privacy meant that only the data owner should be able to access all of the necessary information that was stored securely in the cloud. A decentralized, exposed situation that resulted in considerable loss was created if all the necessary safe data was ever hacked. Numerous systems have been tried in the past to protect the users' private data in the cloud, but they have all shown to be inefficient and unreliable.

The block-chain brought about a model method for certifying insignificance. The development of a

suitable service that could produce well-built safety started when this new technology was put into a cloud environment. An electronic wallet that was used for security needs to be properly erased when employing block-chain technology; otherwise, there's a chance that the user's data will remain. The ledger and bitcoin procedures, as well as occasionally both, are part of the block-chain technology, which has led to a serious security problem. The introduction of an electronic wallet, however, was made to avoid problems of that nature and is now recognized as the best in mobile systems. The possibility of the security transaction emerged only when individual unification and the validity of time sequence in mobile systems emerged.

This authentication example normally does not give morals because it entailed hacking a private key to attack the block-chain and disclosing the key. Because the complete removal of an electronic wallet was not classified, data security was also interrupted. Because the electronic wallet's authentication process was left unattended, complete information security could not be generated. The unsecured dual verification used by the improved block-chain method failed to grant access or guarantee integrity. Furthermore, it typically didn't provide any residual data security when the deletion of the electronic wallet was still supported. However, when data was encrypted using a public key that allowed for the deletion of an electronic wallet, complete data security was made possible.

10 Examples of Block-Based Cloud Data Protection Technologies

10.1 Cloud data with privacy protection

Public key cryptography and access control lists were the two methods used to secure the private information in the cloud. Public key cryptography, which makes use of both public and private keys, is also known as asymmetric cryptography. In contrast to the public key, which was made available to everyone, the private key is usually very secret. Before selecting how to decrypt the data using a separate secret, asymmetric cryptography was mostly employed to finish the encryption process. The access control list, which also included how users could read the databanks, was made clearer with the help of a few guidelines. To view data saved in the cloud, any organization must have the appropriate access control authorization from the list. The data can then be encrypted using public key cryptography with the aid of service providers. The two strategies that were previously described were combined to show how to manage risk variables and stop losses.

10.2 Statistics for unified clouds

The consistency of the cloud data's accuracy was the cloud environment allows for the long-term storage of information. Data editions and public key encryption were used to ensure the data integrity that was promised. A keyless signature infrastructure encryption tool might be used by users in this asymmetric cryptography procedure to assign the data for any updates to the information that the signature verification method would find. These procedures involved periodically storing copies of all the data on the cloud, and then compiling all the data without any exchange via a polling procedure. In order to maintain stability, dependability, and consistency throughout the circuition of the data via smart contracts, the block-chain developed a node-to-node integrity confirmation. Keeping In order to show the oneness of the information, it was helpful to have a clear hub with a concordant structure that secured beliefs inside the nodes.

10.3 The ability to detect data

Cloud data detectability kept track of the originality of the data saved in the cloud to ensure its own private information and distinctive procedure. Information that resulted from processes like input and output was also found to be saved in the cloud environment.

The conventional detectability of information was caused by logging and auditing methods, which were connected to zero-knowledge proof. These methods allowed for the monitoring of changes in data flow across the cloud and the assurance of the accuracy of information sources.

11 Applications for Blockchain and Iot

Using gateway nodes, block-chain-based IoT applications can be created. These gateways act as an abstraction layer between IoT devices and older systems. Data can be exchanged between these gateways, and they can also verify blocks before submitting them to the block-chain network.

Security and privacy are the main drivers for implementing hybrid block-chain and IoT applications, among the numerous other advantages of merging block-chain with the Internet of Things. We can profit from the adoption of block-chain in IoT in all facets of our lives. Block-chain can be utilized in the Healthcare business, e- Governance etc. Example:

Enhances security: Real-time data is captured by IoT smart devices and stored in the cloud. The main difficulty with keeping data in the cloud is ensuring its privacy and security. In such a case, a patient's data is open to hackers, which could jeopardise his private health information. The information about the patient can subsequently be used to make phoney identification cards to buy drugs or even to submit false insurance claims. Due to the data's resistance to hacking and manipulation, block-chain technology can offer the necessary solution to the security problems IoT devices are experiencing.

It becomes difficult to combine several IoT devices since they each have a separate data transfer protocol and processing capability. This slows down the integration process and limits the usage of IoT in healthcare. Block-chain provides a solution for this, but due to IoT devices' low processing power, these cannot be connected to the Block-chain directly since substantial computer power is needed for connecting with Block-chain. These Internet of Things (IoT) smart gadgets must be connected to the block-chain through an intermediary. A cloud system with powerful computing capabilities that can gather data from sensors and send it to the block-chain which may serve as this intermediate system. A person will receive a distinctive ID tied to the Block-chain in the system driven by block-chain technology. He has the option to control who can access the data that smart gadgets have acquired. When there are several IoT devices, he can also decide which IoT devices' data should be given to the healthcare provider.

Better synchronisation of IoT device data with electronic medical records: Fitbits, health bands, watches, and blood glucose monitors are examples of IoT smart health wearables that keep track of a user's daily data and activities. These include tracking calories, steps, miles, heart rate, sleep quality, blood pressure, blood glucose levels, and other metrics. With the help of Blockchain technology, all of this everyday data from a user's smart health devices may be combined with the user's Electronic Health Records (EHRs). Doctors can view a patient's status in real-time because these gadgets collect the user's real-time data. Patients don't need to undergo every test when they visit the hospital because data is collected continuously. As a result, basic test costs will be lower and important time will be saved.

12 Implications for Secure Iot Deployments

Data security is a major issue for the IoT ecosystem. This technology is a prime target for hacking efforts due to the millions of connected devices. DDoS assaults, which are malicious campaigns that barrage targets with millions of requests, can affect a lot of Internet of Things (IoT) equipment. Before, this caused disruptions to both services and personal lives. Additionally, as IoT devices lack adequate security measures, they are a prime target for cybercriminals.

Because block-chain technology is decentralized, devices in the network are always linked to the block-chain network to take part in the consensus process. IoT devices are also susceptible to security breaches due to their constant connectivity. Scalability and dependability are crucial for IoT applications in the end.

By improving the security and productivity of IoT devices, block-chain technology can aid in overcoming these difficulties. IoT devices could disrupt crucial infrastructure because they lack authentication rules. Block-chain technology can be applied to guarantee the accuracy of sensor data, prohibiting the duplicate of harmful data. Block-chain enables for device unique identification in addition to data security. For the safety of IoT devices, this is essential.

13 Advantages of Blockchain Adoption In Iot

IoT device maintenance, data transport, and data management costs can be decreased by using a decentralized ledger to store data on IoT devices. This helps organizations safeguard the information.
Businesses can also do away with a central IoT gateway thanks to blockchain technology. The adoption of blockchain in IoT can speed up processes. Because of this, it works well for a variety of IoT applications. However, the decentralized nature of blockchain could provide a problem for IoT.

Most IoT platforms are built on hub-and-spoke or client-server designs, which depend on a centralized authority to carry out transactions. Because of this, IoT platform designers must make sure their systems are interoperable with blockchain networks. This might provide a substantial difficulty because it can be challenging to set up sensors so that they rely on centralized processing.

14 Issues of Blockchain and Internet of Things

Although IoT and block-chain may share certain objectives, there are still many obstacles to overcome. Block-chain does away with the necessity for centralized servers, but smart contracts' immutability is a drawback. They cannot be altered once they have been launched, making them bug-prone.

These weaknesses are frequently the focus of hackers. To successfully utilize block-chain for IoT, it will be essential to provide tools for reviewing smart contracts. Another element that makes adopting block-chain in IoT systems more difficult is the existing regulatory landscape. With IoT, there are numerous security concerns. The security of the transactions could be compromised due to a problem with the device sensors. Additionally, maintaining the integrity of IoT devices is essential to prevent outside interference. In spite of these obstacles, block-chain and IoT have made great progress towards finding solutions. Businesses will be able to integrate new IoT technologies with the least amount of security risk thanks to block-chain technology.

15 Smart Contracts

Since the Internet of Things relies on a sizable network to transfer data, privacy is another significant issue in this area. Privacy is therefore necessary to stop data from being stolen. Many researchers proposed various number of methods to address the issue of data privacy in the IoT sector, but this has an impact on the ability of IoT networks to grow because the solutions place a demand on the centralized network. Due to its decentralized structure, block-chain offers data privacy measures that allow to secure data from outsiders without raising concerns about expandability. Block-chain is used to store IoT data and make it temporarily available for use in transactions. Numerous researchers have proposed lightweight block-chain systems that enable the privacy. IoT hardware and block-chain technology are combined on a platform called the Inter-Planetary File System (IPFS), which offers solutions to IoT concerns about interoperability, security, and privacy. Filament provides hardware solutions for IoT device-to-device interactions in businesses leveraging block-chain.

16 Review Gap

Applications utilized in the cloud computing environment and block-chain technology have demonstrated one of the key effects on the user and cloud service provider. It also affects data owners who want to ensure the security of their data. The aforementioned discussion identified security issues and difficulty as two of the cloud's biggest negatives. It still has to cope with concerns like controlling data or information, preserving data stability, and sustaining data dependability in a cloud computing environment.

Block-chain is a crucial and secure tool for monitoring the data detectability via the cloud. However, by providing greater direction when service providers work together, cloud computing may grow more quickly in the future. The verification of data must be increasingly decentralized. This has a significant effect on data distribution, which calls for improvement.

17 Conclusions

The following can be concluded from the above discussions:

The primary emphasis of this study is the application of block-chain technology to analyze cloud data security in light of threats to the environment for cloud computing. Numerous tools are available right now to strengthen the confidentiality, discoverability, and dependability of cloud data. Despite the development of many applications, there are still a number of issues with block-chain that have not yet been solved, such as those relating to transaction security and software administration. It's important to confirm the privacy of user data while using block-chain technology. User data must be removed from the programme during extraction in order to do this. The future of smart technologies is block-chain and IoT. Adoption of block-chain in IoT has enormous promise for securing the domestic IoT ecosystem as well as opening the door to smart entertainment and other extensive applications. The third generation of the Internet will be reliable, safe, and effective thanks to block-chain technology, even though there are still certain integration challenges with the current IoT system to overcome.

References:

[1] Sarmah, S. S. Application of blockchain in cloud computing. International Journal of Innovative Technology and Exploring Engineering (IJITEE), vol. 8, 2019, pp. 4698-4704.

[2] Dhananjay Yadav ,Aditi Shinde, Akash Nair, Yamini Patil, Sneha Kanchan "Enhancing data security in cloud using Blockchain," 2020, IEEE Access Journals
[3] Marwan Adnan Darwish, Eiad Yafi, Mohammad A. AI Ghamdi, Abdullah Almasri "Decentralizing Privacy implementation at cloud storage using Blockchain-based Hybrid algorithm", 2020 Springer Science.
[4] Azath Mubarakali "Healthcare services monitoring in cloud using secure and robust healthcare-based Blockchain approach," 2020 Springer Science.
[5] Mueen Uddin, Anjum Khalique, Awais Khan " Next Generation Blockchain virtualized cloud security solutions: Review and open challenges", 2020, IEEE Access Journals.
[6] Prof Saurabh Sharma, Dr, Ashish Mishra, Dr. Ajay Lala, Deeksha Singhai"Secure Cloud storage architecture for digital medical record in cloud enviornment using Blockchain",2020 Springer Science
[7] Meet Shah, Mohammedhasan Shaikh, Vishwajeet Mishra, Grinal Tuscano "Decentralized cloud storage using Blockchain", 2020 IEEE Access Journals
[8] Peng chang Wei, Dahu Wang, Yu Zhao, Sumarga Kumar Sah Tyagi, Neeraj Kumar "Blockchain data base cloud data integrity protection mechanism " 2020, ELSEVIER, Science Direct.
[9] Osama Alkadi, Nour Moustafa, Benjamin Turnbull," A Review of Intrusion detection and Blockchain applications in the cloud: Approaches, Challenges, and Solutions", 2020 IEEE Access Journals.
[10] Kake Gai, Jinnan Guo, Leihung Zhu"Blockchain meets Cloud Computing: A Survey", 2020 IEEE Access Journals.
[11] Nasrin Soharbi, Xun Yi, Zahir Tari, Ibrahim Khalil "Blockchain- based access control for cloud data ", 2020 ELSEVIER, Science Direct.
[12] Bharathi Murthy, M. Lawanya Shri, Siefedine Kadry, Sangsoon Lim, "Blockchain based Cloud computing: Architecture and Research challenges", 2020 IEEE Access Journals
[13] Pratima Sharma, Rajni Jindal, Malay Dutta Borah "Blockchain Technology for Cloud Storage: A Systematic Literature Reiew " 2020, ELSEVIER.
[14] Vivekanadam, B. (2020). Analysis of recent trend and applications in block chain technology. Journal of ISMAC, 2(04), 200-206.
[15] Gai, R., Du, X., Ma, S., Chen, N., & Gao, S. (2020, December). A summary of the research on the foundation and application of blockchain technology. In Journal of Physics: Conference Series (Vol. 1693, No. 1, p. 012025). IOP Publishing.
[16] Patil, A., Patil, S., Sharma, V., Rokade, S., & Sambare, G. B. (2021). Securing Cloud Based Data Storage using Blockchain. International Journal of Engineering Research and Technology (IJERT), 10(06), 517-521.
[17] Liang, J., Li, T., & Song, C. Application of Cloud Computing and Blockchain Technology in Intelligent Information Security. In 2021 IEEE International Conference on Emergency Science and Information Technology (ICESIT) 2021, pp. 819-823.
[18] Kollu, P. K. Blockchain Techniques for Secure Storage of Data in Cloud Environment. Turkish Journal of Computer and Mathematics Education (TURCOMAT), vol. 12, 2021, pp.1515-1522.
[19] Kaushal, R. K., Kumar, N., & Panda, S. N. Blockchain Technology, Its Applications and Open Research Challenges. In Journal of Physics: Conference Series. Vol. 1950, 2021, p. 012030.
[20] Kumar, R., & Tripathi, R. Scalable and secure access control policy for healthcare system using blockchain and enhanced Bell–LaPadula model. Journal of Ambient Intelligence and Humanized Computing. Vol. 12, 2021, pp. 2321-2338.
[21] Li, W., Wu, J., Cao, J., Chen, N., Zhang, Q., & Buyya, R. Blockchain-based trust management in cloud computing systems: a taxonomy, review and future directions. Journal of Cloud Computing. Vol. 10, 2021, pp. 1-34.
[22] Habib, G., Sharma, S., Ibrahim, S., Ahmad, I., Qureshi, S., & Ishfaq, M. Blockchain Technology: Benefits, Challenges, Applications, and Integration of Blockchain Technology with Cloud Computing. Future Internet Vol. 14, 2022, pp. 341.
[23] Khanna, A., Sah, A., Bolshev, V., Burgio, A., Panchenko, V., & Jasiński, M. (2022). Blockchain–Cloud Integration: A Survey. Sensors, Vol. 22, 2022, pp. 5238.
[24] Guo, H., & Yu, X. A Survey on Blockchain Technology and its security. Blockchain: Research and Applications. vol. 3, 2022, pp.100067.
[25] Ke, Z., & Badarch, T. (2022). Research on Information Security and Privacy Technology Based on Blockchain. American Journal of Computer Science and Technology. Vol. 5, 2022, pp. 49-55.

[26] Ismail, Leila, and Huned Materwala. 2019. "A Review of Blockchain Architecture and Consensus Protocols: Use Cases, Challenges, and Solutions" Symmetry 11, no. 10: 1198. https://doi.org/10.3390/sym11101198.

Contribution of Individual Authors to the Creation of a Scientific Article (Ghostwriting Policy)

Priyanka Mishra is responsible for study conception and design, data collection, analysis, and manuscript preparation

Ganesan R has implemented concept of study, analysis and manuscript preparation

Sources of Funding for Research Presented in a Scientific Article or Scientific Article Itself

No funding was received for conducting this study.

Conflict of Interest

The authors have no conflicts of interest to declare that are relevant to the content of this article.