International Journal of Innovative Research in Computer Science & Technology (IJIRCST)
ISSN: 2347-5552, Volume-9, Issue-6, November 2021
https://doi.org/10.55524/ijircst.2021.9.6.32
Article ID IRPS12042, Pages 139-143
www.ijircst.org

An Overview on the Study of Data Encryption and Decryption in Cloud Computing

Swapnil Raj[1], and Mrinal Paliwal[2]

[1,2] SOEIT, Sanskriti University, Mathura, Uttar Pradesh, India
Correspondence should be addressed to Swapnil Raj; swapnil.cse@sanskriti.edu.in

ABSTRACT- While big data technologies in cloud computing are rapidly growing in popularity, privacy issues have increased dramatically. Encrypting data in real-time is one of the greatest important issues throughout data acquisition and transfer. In order to reach an acceptable performance level, many modern applications forego data encryptions, which is unsuitable with privacy issues. In light of cloud computing concepts and features, this article examines various cloud computing systems and analyzes the cloud computing security problem and solution. Data privacy but instead service availability are major security problems in cloud computing. A single security solution will not address the cloud computing security challenge; to defend the whole cloud computing system, a mix of old and new technologies and procedures must be employed in harmony. The author demonstrates the use of encryption and decryption algorithms in terms of data confidentiality, great computational efficiency, and cloud-based system effectiveness. On top of this architecture, they may enable dynamic block-level actions on data encryption blocks for insertion, removal, including update, which we believe will be future work for enhancement.

KEYWORDS- Cloud Computing, Decryption, Encryption, Privacy, Security.

I. INTRODUCTION

Cloud computing has become a significant issue in business and academics because to the fast advancement of computers technology as well as software. The Cloud computing has been influenced by a number of factors, including conventional computer technology, communication technologies, and corporate culture. It is network-based and has a consumer-facing service structure. The cloud computing system provides a service to customers while ensuring scalability and reliability[1]. The user is ignorant of the location of the resources in the cloud systems since it is apparent to the applications. Your apps and data may be accessed from anywhere. A huge number of users may share cloud resources. When the workload increases, the cloud system's capacity may be increased by adding additional hardware to better handle the increased demand. Cloud resources are provided on a need-to-know basis.

The cloud is made up of a huge number of commodity-grade computers that are utilized to provide highly scalable and reliable on-demand services. When users need more resources, the amount of resources accessible to them in the cloud system is raised, and when they require fewer, it is reduced. A computer, storage, or other service specification may be the resource. Cloud computing is being hailed as a major breakthrough in the information industry that will have a greater influence on the developments of information technologies for societal gain The majority of cloud computing infrastructure today consists of dependable services offered through data centers constructed on servers that use varying levels of virtualization technology.

A. Decryption and Encryption of Cloud Data

From early concept to present implementation, cloud computing is evolving at a fast rate. Many organizations, especially the little as well as moderate businesses (SMBs), are quickly realizing the advantages of storing their applications and data in the clouds. Cloud computing adoption may lead to increased efficiency and productivity in development and implementation, as well as cost savings in terms of acquiring and maintaining infrastructure.

"The definition of cloud computing is "an architecture for providing simple, on-demand network access to a shared pool of programmable computing resources that can be promptly provided and released with minimum administration effort or service provider contact." This cloud architecture promotes availability by combining five important qualities, three service types, and four deployment methodologies. Community cloud, private cloud, hybrid cloud, as well as public cloud are the four deployment options.

B. Management of Cloud Computing with their Own Encryption

In cloud computing, data is stored and computed on a vast number of computers distributed over the internet, rather than on a single computer and server. The duty for cloud encryption is moved from the individual computer and private data center to a bigger computing center that is shared by all users as well as dispersed across the internet. It assembles applications from loosely connected services, with one service failing without affecting the others. The front end as well as the back end are the two sections of the cloud computing system. They converse with one another over the internet[2]. The user who uses the encryption offered by the back end, which is the system's cloud component, is referred to as the front end.

Cloud encryption refers to the transmission of computer resources from a place other than the user's own. All computer hardware, software, encryption resources, and services, such as resource utilization and administration, are entirely shared. Cloud encryption services are widely available and may be used on a broad range of devices, including desktop computers and mobile phones. Virtualization enables several operating systems to coexist on a single physical computer while sharing hardware resources. One or more hosts may serve a virtual server, while a single host can handle several virtual servers. The loss of host encryption will have no impact on virtual servers if the environment is correctly setup. To make maintenance easier, hosts may be deleted and replaced at any time. The encryption systems for cloud-based virtual servers is readily scalable, and if managers determine that the resources supporting a virtual server are overworked in the real world, they may modify the number of resources provided to that virtual server. A multitude of technologies, such as parallel computing, grid computing, as well as other computer technologies, have aided cloud computing.

Grid computing tries to tackle the problem of encryption and resource storage assignment, whereas cloud computing wants to share processing, storing, as well as application resources. Grid computing, unlike cloud computing, does not employ virtualization and gives each company complete control over its own resources. The program does not require any computer or storage capabilities, and it is not distributed over the cloud. Cloud computing could be able to give the resource as well as the server. Encryption is classified as private cloud, cloud hosting, or hybrid cloud depending on the service object. A hybrid cloud is made up of two or more clouds connected by standard or customized technologies. Hybrid clouds provide together the best features of both public and private clouds in one convenient package. The firm has established a private cloud, so safety is straightforward to implement. Private clouds are virtualized cloud data centers located behind a firewall that are devoted to a single system[3]. The term "private cloud" refers to an organization's or other entity's internal data centers that are not accessible to the general public. The three cloud service paradigms are SaaS (Software as a Service), PaaS (Platforms as a Service), and IaaS (Infrastructures as a Service)[4].

C. Other Encryption Algorithms for Map Reduce

The MapReduce programming method is a distributed programming approach that may simplify cloud computing programming. Map and Reduce activities make up the MapReduce operation, with the Map utilizing the Key as well as Values to generate new Keys and Values[5].

The Key and Value styles are combined in the Reduce operation. MapReduce is both a programming language and a method for scheduling simultaneous jobs. To organize data, the programmer may offer their own Map and Reduce methods [7]. Big table is a distributed database management system that stores data in the table that is partitioned into numerous rows on a vast scale. A tiny tablet with numerous rows is stored in the node. Big table uses distributed cluster job scheduling, and thus the Chubby distributed locker service. Developers may use the Windows Azure operating system to create a cloud computing platform called Windows Azure. A developer may create an application on a remote server, a web server, a PC, or a data centre.

Apache Hadoop is a distributed computing system that is free and open-source. Several network stations, like Amazon and Facebook, utilize it to build systems. MapReduce and HDFS are the two major components of Hadoop. MapReduce allows for task decomposition as well as result integration. HDFS is a distributed file system that acts as a backbone for file storage in storage nodes. Task as well as job trackers are available in MapReduce.

D. Cloud Encryption Security Difficulty

Because the cloud system is linked to the internet, security flaws uncovered on the internet may also be detected in the cloud system. The cloud system is comparable to a traditional PC system, and it has the ability to address a wide range of new and unique security challenges. Security and privacy are the two most pressing problems with cloud computing. Traditional security issues such as security holes, viruses, and hack attempts may put the cloud system at risk, resulting in more catastrophic outcomes, due to the nature of cloud computing. Hackers and other malevolent intruders have the potential to get access to cloud accounts as well as steal important information. In the cloud center, data and business applications are kept, and the cloud system must protect the resource effectively. Cloud computing is the outcome of extensive use of virtualization, service-oriented architecture, and utility computing. It consists of software, platforms, and services that are supplied through the internet. If the systems fail, quick resource recovery is also a concern.

Cloud systems hide the intricacies of service deployment technology and administration. The user has limited control over how data is handled and cannot ensure data security on his or her own. The cloud system manages the storage and operation of data resources, as well as network transformation. The user places a high value on critical data resources and privacy data. The cloud must offer the user with a data control mechanism. The data security audit might be conducted using a cloud system. Data is sent to any approved location where it is required, in a format that can be read by any authorized software, by any authorized user, and on any authorized device. Only approved users are permitted to make changes to the data, and only authorized users are permitted to see it.

E. Strategies as well as Methodology of Encryption

Without authorization, data saved in the cloud system might be stolen and changed. Before the data is saved in the cloud system, it's conceivable that it will be encrypted. However, if the data collection is huge, additional time and computational resources will be required. Confidential data will be considered as such outside of the company, and other persons will have access to it. In the cloud, traditional approaches may secure user data privacy and security to some extent. Encryption, a secure authentication system, and an access control scheme are among the technologies used. The decoding complexity is determined by the encryption technology used. The two types of encryption systems are symmetric key encryption systems and asymmetric key encryption systems. Asymmetric keys are secure, but they take a long time to encode and decode. The security authentication method employs a broad range of technology technologies.

It includes directory security control as well as network access control. Users who can connect to a cloud system include cloud providers, operation and maintenance staff, and consumers. Client data must not be unlawfully stolen or utilized by others cloud computing businesses, which is a main concern. Data storage and backup, as well as data category management depending on the degree of data protection, are handled by personnel in charge of operations and maintenance.

Storage location, Data storage isolation, data recovery, as well as data long-term survival are the most important aspects of cloud computing storage security. Control of data is ceded to cloud computing firms once it is stored in the cloud. Some unethical businesses may get client privacy information via deceptive methods that are more convenient for the customer. While the user is ignorant of the location of the data storage, the cloud provider may move client data from one server to another. In a cloud system, cloud center resources are linked with data storage and manipulation. Despite the facts that the cloud provider is in charge of the police, monitoring as well as audits have become a significant issue for them.

It is necessary to address the isolation and security of the user system and data. To protect network data transmission security, data encryption and VPN technologies may be employed[7]. The key distribution system and user data encryption management must be properly developed. User data must be managed and maintained in a secure and efficient manner. A data backup, as well as a data security recovery solution, are both required. The cloud service may be compared to a web service, and the security mechanism of a service-oriented architecture can be utilized as a model. Programming languages serve as the foundation for connecting applications across platforms through a communication protocol, and SOA facilitates cross-system interoperability. The web service includes security features like as WS-Security, WS-Trust, WS-Authorization, WS-Reliability, as well as WS-Secure Conversation.

F. Benefits of Data Encryption

- The advantages of encryption in the cloud environment are listed below:
- Encryption ensures that an organization's data is kept private while being sent, used, or retained.
- If a data breach occurs as well as personal information is compromised, the breached party must notify all affected persons.
- In a cloud setting, encryption ensures that data backups are protected from unauthorized access.
- Encryption may increase income opportunities for clients with sensitive or regulated data by allowing the cloud data owner to keep the key, giving cloud service providers a competitive edge.

II. LITERATURE REVIEW

G. Naga Srikanth et al. discussed a review on security of cloud computing[9]. Cloud computing was created to offer services to consumers and individuals while lowering costs. Cloud computing enhances an organization's performance by using minimal resources and management assistance, as well as a shared network, valuable bandwidth, cost-effective software and hardware, and limited service provider interactions. The use of cloud computing in a business infrastructure raises serious security issues. For a successful cloud computing implementation in a company, proper planning and understanding of emerging risks, threats, vulnerabilities, and possible solutions are essential. Cloud security is fast becoming a distinguishing feature and competitive advantage for cloud providers. This article discusses the many types of clouds, security issues at the cloud and network level, and an encryption approach.

Miss Pulatsya Kanasagara et al. discussed a review on the Data encryptions technique in cloud computing[10]. Customers have the illusion of utilizing limitless computer resources that are accessible on demand from anywhere and at any time. Secure data transfer is provided via cloud computing. Data security has become a major issue due to the need to ensure different attributes such as integrity, confidentiality, and authentication. Cryptography methods such as AES, DES, RSA, Blowfish, RC5, 3DES, and Diffie-Hellman play an important role in securing data in network-based applications. This article compares and contrasts different security algorithms that are currently accessible.

Sanjoli Singla et al. discussed cloud data security[11]. Cloud computing has been envisioned as the next-generation architecture for the IT company. In cloud computing, application software and databases are shifting to centralized huge data centers. This method brings a plethora of new challenges that aren't completely understood. Security and privacy concerns, on the other hand, are substantial hurdles to mainstream cloud use. The most pressing concern in cloud computing is providing security to end users in order to protect files and data from unauthorized access. Any technology's main purpose is to prevent unauthorized intruders from accessing your cloud files or data. We've come up with a design and architecture that can let users encrypt and decrypt files at the user level, ensuring data security both at rest and in transit. The author utilized the Rijndael Encryption Algorithm in conjunction with EAP-CHAP in this study.

III. DISCUSSION

Because the cloud computing system incorporates more data, including user-specific information, data cannot be erased or taken. A hacker may concentrate their efforts on obtaining data in a cloud system since it may be essential to a user. The new system must be protected even more than the old one. Cloud computing is used by the firm, and data is stored there. Non-employees may have access to the company's information. If a business wants to keep sensitive data on the cloud, it must trust in the technology. Whether the cloud system is behind a firewall or not, governance and security are critical components of cloud computing. Cloud computing security is a critical issue in cloud computing's evolution. The traditional security method is inadequate to completely secure the cloud system. The cloud computing application has no limits and is very mobile, which might lead to a slew of new security issues. Data security, user data privacy protection, cloud computing platform dependability, and cloud computing administration are the key security issues.

To improve licencing, certification, quarantine, and other areas of data management, cloud computing should provide effective user access control. The cloud provider system in cloud computing has a large number of users who respond dynamically to changing service demands. Users have no idea where their information is stored or which servers are handling it. Because of the cloud system's flexibility and scalability, the user has no idea which network is giving the data. The user cannot be confident that the cloud maintains data privacy in a secure manner. The cloud system may install the cloud center in many locations, and data can be stored in numerous cloud nodes. Security management must be able to satisfy the legal risk since different locations have different laws. More legal protection is required for cloud computing services.

In this research, the author presents a data encryption and decryption technique for securing outsourced sensitive data in a cloud computing environment. To minimize storage and processing expenses, data owners may combine the benefits of file partitioning with data encryption. A trusted third party is frequently formed to authenticate allowed users for access to data from cloud servers, easing the load on the data owner. We demonstrate the usefulness of encryption and decryption in terms of privacy, computational efficiency, and cloud storage system efficacy. Future work on dynamic block level operations for insertion, removal, and modification of encrypted data blocks may also be proposed by designers.

IV. CONCLUSION

The most effective method of safeguarding data transfer over the Internet is data encryption. To solve these concerns, this study proposes and executes a cloud-based data security strategy as well as a secure cloud computing system. It addresses the unpredictability of cloud computing data transport to offer users with a secure cloud computing platform. The experiment validates the security and efficiency of the cloud computing security transmission mechanism presented in this research. This research demonstrates cloud concepts and capabilities, including scalability, elasticity, independent platforms, cheap cost, and reliability. The cloud system's security concerns are investigated. Data encryption is rapidly evolving and has a lot of promise and potential. Many elements of information and service management are related to cloud computing. Data privacy is more important in the cloud computing environment than on a traditional network since data is more reliant on the network and server. Many consumers are wary about cloud computing customers' security and privacy, and they are hesitant to transfer data from their businesses or private data encryption systems to the cloud platform. Several challenges have plagued cloud computing, the most serious of which being security. To effectively address these challenges, the cloud computing provider will need to use a number of security measures as well as data encryption methods. Data owners may use data crypton to decrease storage and processing overheads by taking use of the benefits of splitting files. A trustworthy third party is introduced to check allowed users for access to the data from the cloud-server, reducing the strain on the data owner. Our data security, processing speed, and efficiency of the cloud storage system are shown using encryption and decryption algorithms. On top of this architecture, we can enable dynamic block level operations on encrypted data blocks for insertion, deletion, and update, which we believe will be future work for enhancement.

REFERENCES

[1] S. K. Dash, J. P. Sahoo, S. Mohapatra, and S. P. Pati, “Sensor-Cloud: Assimilation of wireless sensor network and the cloud,” Lect. Notes Inst. Comput. Sci. Soc. Telecommun. Eng. LNICST, vol. 84, no. PART 1, pp. 455–464, 2012, doi: 10.1007/978-3-642-27299-8_48.

[2] M. Parhi, B. K. Pattanayak, and M. R. Patra, “A Multi-agent-Based Framework for Cloud Service Description and Discovery Using Ontology,” Adv. Intell. Syst. Comput., vol. 308 AISC, no. VOLUME 1, pp. 337–348, 2015, doi: 10.1007/978-81-322-2012-1_35.

[3] M. R.-J. of S. and Software and undefined 2013, “Cloud computing security: The scientific challenge, and a survey of solutions,” Elsevier, vol. 86, pp. 2263–2268, 2013, doi: 10.1016/j.jss.2012.12.025.

[4] A. Bastia, M. Parhi, B. K. Pattanayak, and M. R. Patra, “Service Composition Using Efficient Multi-agents in Cloud Computing Environment,” Adv. Intell. Syst. Comput., vol. 308 AISC, no. VOLUME 1, pp. 357–370, 2015, doi: 10.1007/978-81-322-2012-1_37.

[5] F. Ahamed, … S. S.-C. of the, and undefined 2013, “Cloud computing: Security and reliability issues,” ibimapublishing.com, vol. 2013, p. 12, 2013, doi: 10.5171/2013.655710.

[6] D. L.-I. C. Computing and undefined 2017, “Cloud computing changes data integration forever: What’s needed right now,” ieeexplore.ieee.org.

[7] Y. Zhao, K. Ou, W. Zeng, and W. Song, “Research on cloud storage architecture and key technologies,” ACM Int. Conf. Proceeding Ser., vol. 403, pp. 1044–1048, 2009, doi: 10.1145/1655925.1656114.

[8] B. Furht, “Cloud Computing Fundamentals,” Handb. Cloud Comput., pp. 3–19, 2010, doi: 10.1007/978-1-4419-6524-0_1.

[9] G. N. Srikanth, “A Study on Cloud Computing Security with Encryption and Decryption Technique,” vol. 4, no. 34, pp. 1–5, 2016.

[10] P. Kanasagara, “A Review on Data Encryption Algorithm in Clould Computing,” Int. J. Adv. Res.

Innov. Ideas Educ., no. 5, pp. 569–576, 2017.

[11] S. Singla and J. Singh, “Cloud data security using authentication and encryption technique,” Int. J. Adv. Res. Comput. Eng. Technol., vol. 2, no. 7, pp. 2232–2235, 2013, [Online]. Available: http://ijarcet.org/wp-content/uploads/IJARCET-VOL-2-ISSUE-7-2232-2235.pdf.