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.2021.9.6.50
Article ID IRPS12060, Pages 225-228
www.ijircst.org

Encryption and Decryption Techniques in Cloud Computing

Pankaj Saraswat[1], and Swapnil Raj[2]

SOEIT, Sanskriti University, Mathura, Uttar Pradesh, India
Correspondence should be addressed to Pankaj Saraswat; pankajsaraswat.cse@sanskriti.edu.in

ABSTRACT-While big data applications in cloud computing are rapidly growing in popularity, privacy issues have increased dramatically. Encrypting data in real time is one of the most important issues during data processing and transfer. In order to reach an acceptable performance level, many modern applications forego data encryptions, which is incompatible with privacy concerns. This article covers several virtualized processes and analyses the cloud technology safety challenge and way to solve in brightness of cloud technology ideas and characteristics. Information confidentiality and dependability of services are major cybersecurity problems in internet applications. A singular monitoring platform will not address the cloud hosting privacy challenge; to defend the whole clouds infrastructure, a mix of old and new methods and technology must be employed in harmony. The author demonstrates the use of encoding and decoding techniques in aspects of the data confidentiality, computation time, and virtualized systems effectiveness. On top of this infrastructure, they may enable dynamically data storage functions on encoded information sections for inclusion, deleting, and updating, which we think will be future work for improvement.

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

I. INTRODUCTION

Virtualization has now grown a big problem in business and academics because to the rapid advancement of computers technologies and applications. Infrastructure has been influenced by a number of factors, include conventional information technologies, telecommunication technologies, and corporate culture. It is infrastructure and has a consumer-facing utilized for the purpose. The cloud provider provides a product to customers while ensuring growth and reliability. The customer is ignorant of the placement of the material in the public cloud since it is translucent to the software[1]. Your apps and information may be accessed from anywhere. A huge amount of consumers may access internet service. When the burden increases, the internet platform's capability may be increased by providing extra technology to better handle the increased demands. Internet services are provided on a need-to-know approach.

The cloud is made up of a huge quantity of raw material computers that are utilized to deliver extremely flexible and reliable on-demand applications. When customers demand additional services, the number of assets accessible to them in the public cloud is raised, then when they demand fewer, it is lowered. A compute, memory, and other services specification could well be the resources. Public cloud is being hailed as a major breakthrough in the information industry that will have a stronger impact on the progress of communication technologies in all aspects of mankind. The bulk of clouds computation system now comprises of trustworthy solutions delivered via data centers built on servers with various degrees of virtualisation technologies.

A. Cloud Data Encryption and Decryption

Cloud computing is maturing at a rapid pace, from early idea development to current real deployment. Many companies, particularly small and medium-sized businesses (SMBs), are rapidly discovering the benefits of placing their apps and data in the cloud. Adoption of cloud computing may result in increased efficiency and effectiveness in development and deployment, as well as cost savings in acquiring and maintaining infrastructure. "A design for terms of controlling, on-demand requirement infrastructure cloud computing is a model (e.g., connections, data centers, collection, software, and assistance) that can be arriving on time and published with limited communication or service provider communication," according to the Wikipedia definition of cloud containers. This computing infrastructure is made up of five core elements, 3 different types, and hybrid deployment patterns that foster reliability.

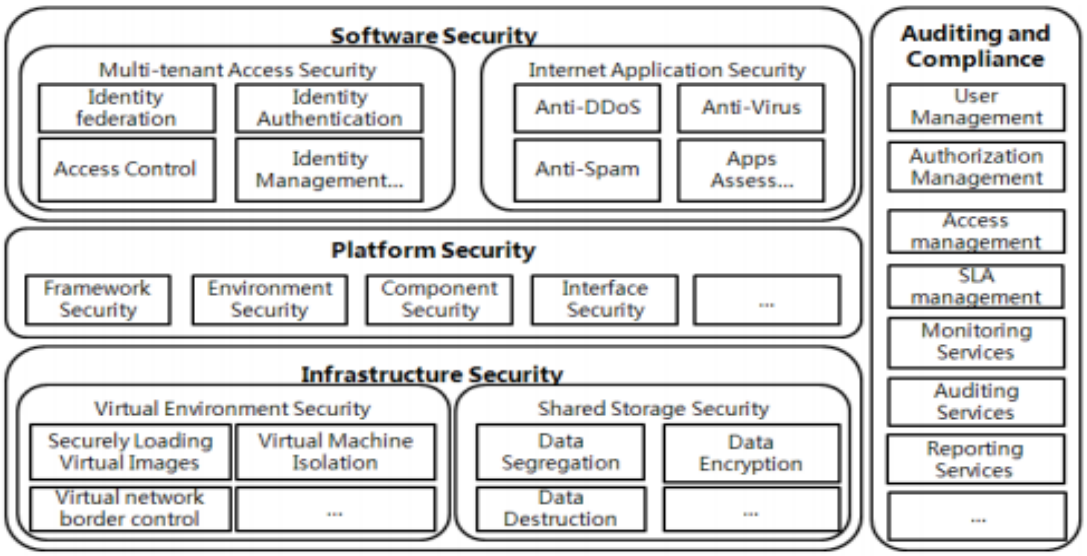

Figure 1: Hierarchy of Cloud Computing Data Distribution and Management of Each Segment

B. Cloud Computing Management with Their Own Encryption

The data storage and computation are not in the local computer and server, but rather in a large number of computers spread over the internet in cloud computing. The cloud encryption shifts duties from the personal computer and private data centre to a bigger computing centre that is shared with all users as well as disseminated through the internet. It constructs applications from loosely connected services, and a failure of one service does not impact other services. There are two parts to the cloud computing system: the front end and the back end. They communicate with one another over the internet. The front end is the user who uses the encryption supplied by the back end, which is the system's cloud portion. Based on how it is portrayed in computer network diagrams, the cloud is a metaphor for the Internet and an abstraction for the sophisticated infrastructure it hides[2]. A virtual server can be served by one or more hosts, and a single host can support several virtual servers. If the environment is properly configured, the loss of a host encryption will have no effect on virtual servers. To accommodate maintenance, hosts can be withdrawn and reintroduced practically at whim.

An entity that offers cloud services to the public or a major industrial business owns the cloud system infrastructures. The cloud computing is an internet-based service with a complex security system. Cloud computing services are virtualization information centers that aren't secured by a firewalls, and the phone company makes capabilities available to customers on request it through Online. Cloud technology architectures are extensively standardized and standardized, and they may help with software management. It offers huge scalability and can serve more apps to a big number of consumers. The cloud is fault resistant, extremely dependable, and capable of providing exceptional service quality. Encryption enables flexibility, in which capital and operating expenditures for resources are incurred only when they are required. Cloud computing is an on-demand service that provides computer capabilities as required. Many devices, including desktops, laptops, PDAs, and mobile phones, can access the service. In cloud platform, the customer utilizes the offered programs and does not handle or administer the connection, server's memory, or applications. It is easy to use and accessible from everywhere, and it may help reduce the amount. It makes a commercial application available as a services that may be viewed by a web computer or client-based roles entry and distribution constraints. The programme is hosted by the service provider, so the customer does not need to install, administer, or purchase hardware for it. They only need to connect and utilise it. Flickr, Google Docs, Amazon, and Cloud Drive are all instances of SaaS [3]. Customers install and administer their programs on the web computation environment using infrastructure as a services, but they really do not handle machines or memory and instead receive a computer environment or infrastructure as a service. It offers a framework for customizing, building, evaluating, and delivering custom business products. It allows installation process without any of the expense and difficulty of acquiring and maintaining fundamental computing levels, and it renders raw equipment accessible to customers via the Web, although it usually comes with a pre-installed and maintained version of windows from the Clouds provider[4]. When adding users or when the program's needs change, the application can be modified. There are several cloud computing platforms available on the market. GFS (Google File Infrastructure), Bigtable and Map Reduce are all part of the Google computing system[5].

C. MapReduce Along with Other Encryption Algorithms

The MapReduce programming mode is a distributing programming style that can reduce the complexity program in computing. Map Reduce is a programming style as well as an effective parallel job scheduling paradigm[5]. Bigtable is a large-scale, dispersed information server that maintains information in a tables that is segmented into many sections. The nodes stores a small tablet that is made

up of several sections. Integrated clustered task scheduler, GFS, and the chubby distribution repository services are all used by Bigtable. Microsoft Azure is a category of clouds processing services that programmers may build using the Window Microsoft computer system. On a public cloud, a web service, a PC, or an information center, a programmer may build an applications. Instead of supporting a particular type of application, the system offers general-purpose computing. Amazon offers the EC2 (Elastic Compute Cloud) and S3 services (Simple Storage Service). EC2 can deliver a variety of services that would otherwise be unavailable on a virtual machine. The user may select a virtual machine based on their needs, upload it to S3, and then call the machine interface to complete the operation. Hadoop is a distributed computing system that is free source and supplied by Apache. Many network stations, like Amazon and Facebook, utilise it to build systems. MapReduce and HDFS are the Hadoop cores (Hadoop Distributed File System). MapReduce is capable of task decomposition and result integration. The HDFS is a distributed file system that provides the foundation for file storage in storage nodes. Job and task trackers are included in MapReduce.

Map Reduce is a programming technique that Google has successfully utilised to handle large data volumes. A map function pulls intelligence from raw data, while a reduce function collects the data generated by map based on specified guidelines. MapReduce requires a distributed file system as well as an engine capable of distributing, coordinating, monitoring, and gathering results. The virtualization technique is used to implement the cloud server. The user can access the cloud server for the cloud system from any location and from any terminal. Users are unconcerned with the specific implementation or location of the cloud server. The virtualization is the cloud system's charter, and the application does not require hardware platform details. The cloud system may create applications in many locations or on various hardware.

D. Cloud encryption Security Problem

The cloud system operates on the internet, and the security issues that exist on the internet may also be discovered in the cloud system. The cloud system is not unlike the standard system in the PC, and it may address various unique and novel security issues. Security and privacy are the two most serious issues regarding cloud computing. Because of the properties of cloud computing, conventional security issues such as security flaws, viruses, and hack attacks can potentially pose risks to the cloud system and lead to more catastrophic outcomes. Hackers and malevolent intruders may get access to cloud accounts and steal critical data from cloud services. The data and business applications are kept in the cloud centre, and the resource must be properly protected by the cloud system. Cloud computing is a technical development resulting from the broad use of virtualization, service-oriented architecture, and utility computing. It consists of applications, platforms, and services delivered through the Internet. If the systems fail, quick recovery of the resources is also a challenge.

Cloud systems conceal the specifics of service deployment technology and administration. The user has no influence over the course of dealing with data, and the user cannot ensure data security on their own. The cloud system is also addressed in terms of data resource storage and operation, as well as network transformation. The cloud must provide the user with a data control system. The data security audit may also be implemented in a cloud system. Data is being moved to any allowed location where it is required, in a format that any authorised application, by any authorised user, on any authorised device, may utilise.

E. Strategies and Methodology of Encryption

However, if the data size is very huge, additional time and computational resources will be required. Confidential data will be considered as such outside of the firm, and other persons will be able to access the data. To some extent, traditional approaches can safeguard user data privacy and security in the cloud environment. Encryption, a security authentication method, and an access control policy are examples of these technologies. The reliability of the difficulty of decryption is dependent on the encryption technique.

Data collection isolate, external storing, backup and restoration, and information long-term preservation are the most important aspects of cloud technology store protection. Ownership of material is handed to cloud based businesses once it is uploaded to the internet. Many immoral businesses may get client confidentiality by deceptive methods that are more comfortable to the customers. The cloud provider can transfer client data from one server to another while the user is unaware of the location of the data storage. Data storage and manipulation are associated with cloud centre resources in a cloud system[7].

It is challenging to provide complete transparency in cloud computing services supplied to clients. Customers are unaware of internal cloud computing procedures and data storage location information. Customers have no idea what condition data will encounter if an accident occurs. In order to completely assure the security of client data, customers should have the authority to supervise and audit cloud computing services. Malicious programmes must be identified as soon as possible. Damage to the system must be rectified as soon as possible [8].

Data flow in the cloud system and the status of the cloud computing system should be monitored in real time. Service disruptions and system failures caused by hackers must be addressed. The cloud computing platform's disaster recovery mechanism, which comprises critical system backup and data disaster recovery, must be implemented. The emergency response system, as well as emergency response skills, must be developed and strengthened for emergency cases. The availability, privacy, and integrity of user information must be safeguarded [9].

Isolation and protection of the user system and data must be addressed. Data encryption and VPN technologies can be used to safeguard network data transfer security. User data must be managed and maintained in a secure and efficient manner. Data backup is critical, and a data security recovery method is also required [10]. SOA promotes interoperability across multiple systems, and programming languages serve as the foundation for integrating applications on diverse platforms via a

communication protocol. Many security measures are built into the web service.

F. Advantages of Data Encryption

To maintain control over data in the cloud, encryption and robust key management are more vital to the company in order to address security concerns. The advantages of encryption in the cloud environment are as follows[11]:

- Encryption ensures the privacy of the organization's data while it is being sent, used, and stored.
- Encryption Aids Cloud Multi-Tenancy with Security The data controller may prohibit the cloud providers from obtaining information by protecting it in the web and holding the encrypted message.
- If a breaches happens and unique material is exposed, the breached party is obligated to contact all individuals who are impacted.
- In a virtual infrastructure, cryptography guarantees that storage systems are safe from a rogue entity.
- Encrypted may help customers with confidential or regulatory information earn more money by enabling the cloud - based data owners to sell the information, to keep the key, giving cloud service providers a competitive advantage.

II. DISCUSSION

Because the clouds technology model incorporates more data, especially subscriber knowledge, data cannot be erased or taken. A hackers may concentrate their attempts on obtaining data in a public computer since it may be essential to a client. The new system must be more closely guarded than the previous one. The company makes use of cloud computing and stores data there. People who are not employed by the company can view data. If a company wants to store sensitive information in the cloud, it must believe in cloud computing. Governance and security are important components of cloud computing, regardless of whether the cloud system is behind a firewall or not. Cloud technology cybersecurity is a critical issue in clouds computing evolution. The traditional protection method is inadequate to completely secure the cloud environment. The cloud services implementation has no boundary lines and is extremely movable, which could lead to a slew of innovative protection issues. Cybersecurity, customer data personal private, cloud services platforms trustworthiness, and public cloud administrative are the key surveillance issues.

In this paper, we present an efficient data encrypted decode approach for securing outsourcing important information in a clouds processing. To minimize space and computational expenses, data controllers may integrate the benefits of file partitioning with encrypting technology. A person or organization is frequently formed to authenticate allowed users for accessibility to information from online storage, easing the load on the data controller. We demonstrate the usefulness of encoding and decoding in confidentiality, processing efficiency, and online backup system usefulness. Designers may also propose future work on dynamic block level operations for insertion, removal, and update of encrypted data blocks.

III. CONCLUSION

The most effective method of safeguarding data transfer over the Internet is data encryption. This research develops and implements a cloud-based data security approach to address these issues, as well as a secure cloud computing system. It resolves the unpredictability of clouds computation data transit to offer users with a secure cloud infrastructure. The trial validates the reliability and efficiency of the distributed technology secure communication 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. By using the advantages of splitting files, data owners may utilize data krypton to reduce storage and computing overheads. In terms of encryption and decryption techniques, our data security, computing performance, and efficiency of the cloud storage system are shown.

REFERENCES

[1]. Dash SK, Sahoo JP, Mohapatra S, Pati SP. Sensor-Cloud: Assimilation of wireless sensor network and the cloud. Lect Notes Inst Comput Sci Soc Telecommun Eng LNICST. 2012;84(PART 1):455–64.

[2]. Parhi M, Pattanayak BK, Patra MR. A Multi-agent-Based Framework for Cloud Service Description and Discovery Using Ontology. Adv Intell Syst Comput. 2015;308 AISC(VOLUME 1):337–48.

[3]. Software MR-J of S and, 2013 undefined. Cloud computing security: The scientific challenge, and a survey of solutions. Elsevier. 2013;86:2263–8.

[4]. Bastia A, Parhi M, Pattanayak BK, Patra MR. Service Composition Using Efficient Multi-agents in Cloud Computing Environment. In: Advances in Intelligent Systems and Computing. 2015.

[5]. Lai J, Deng R, Guan C, on JW-IT, 2013 undefined. Attribute-based encryption with verifiable outsourced decryption. ieeexplore.ieee.org. 2013;8(8):1343.

[6]. Ahamed F, … SS-C of the, 2013 undefined. Cloud computing: Security and reliability issues. ibimapublishing.com. 2013;2013:12.

[7]. Chen Y, Paxson V, California RK-U of, No BR, 2010 undefined. What's new about cloud computing security. Citeseer. 2010;

[8]. Aggarwal N, Tyagi P, Dubey BP, Pilli ES. Cloud Computing: Data Storage Security Analysis and its Challenges. Int J Comput Appl. 2013;70(24):975–8887.

[9]. Moghaddam F, … OK-2013 I 2nd, 2013 undefined. A comparative study of applying real-time encryption in cloud computing environments. ieeexplore.ieee.org. 2013;

[10]. Zhao Y, Ou K, Zeng W, Song W. Research on cloud storage architecture and key technologies. ACM Int Conf Proceeding Ser. 2009;403:1044–8.

[11]. Furht B. Cloud Computing Fundamentals. Handb Cloud Comput. 2010;3–19.