International Journal of Trend in Research and Development, Volume 9(5), ISSN: 2394-9333
www.ijtrd.com

Secured Storage of Text and Image in Cloud Environment Based on Triple Encryption Scheme

Gopal Prasad Sharma
Associate Professor, Purbanchal University School of Science & Technology (PUSAT), Purbanchal University, Biratnagar, Nepal

Abstract: Cloud computing is the current buzzword in the computer industry. It has a flexible infrastructure that enables it to provide excellent services. Client-server design is the basis of cloud computing. Cloud computing is a collection of servers and databases that store information. Cloud computing offers users a range of services that are stable, effective, and minimal. Data security is a big concern for cloud data because it is based on internet technology. Validity, integrity, data concealing, and accessibility are just a few of the issues. This paper proposed about the Secured Storage of Text and Image in Cloud Environment Based on Triple Encryption Scheme.

Keywords: *Cloud Computing, Triple Encryption Scheme, Securing text and Image*

I. INTRODUCTION

Cloud services models had evolved since 1950 when mainframe computers were first introduced. The automating phase began with numerous automatic controls on different electrical, mechanical, and computer devices. Personal computers were designed as mass-market customer electrical gadgets in the 1960s. Instead of a mainframe computer, a personal computer is an electronic device designed for individual users, where people share a huge computer depending on the time-sharing mechanism. Computer systems based on microprocessors are creating at a low cost. Cloud computing is a client-server design that intends to deliver decentralized applications among users and service providers [10]. It is a form of information technology that enables users to have unfettered access to these resources. Cloud computing is an emerging environment that comprises tens of thousands of servers. It is a World Wide Web on-demand business model that provides internet services. Cloud computing, according to NIST [21], is a well-suited approach for on-demand internet connectivity. Cloud computing distributes internet resources that can be delivered at an excellent velocity for a low cost. It's a novel process of obtaining IT services via the internet that utilizes dynamically scalable and usable materials [9,2,7]. NIST's cloud services paradigm is visualized in Fig 1 Three approaches are illustrated in the diagram. The first model describes the foundations of cloud computing.

The accompanying model depicts the fundamental cloud computing service models. The resulting model represents the fundamental cloud computing application scenarios.

The architecture of Cloud Computing

The architecture of cloud computing is comprise of essential components that split into three levels. A front, end platform, and a back end platform make up the components.

- Application layer
- Platform layer
- Infrastructure layer

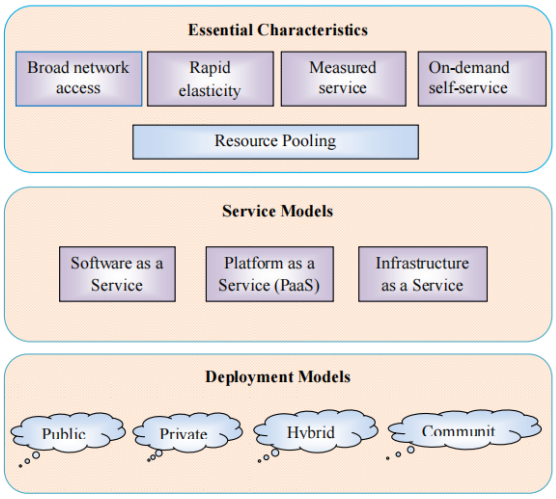

Figure 1 Cloud Computing Model

The software-as-a-service concept is used at an application level to supply computer services on demand. The platform-as-a-service architecture is used to access infrastructure as a service from the platform layer during runtime. Storage, computing, and communications networks are given on request under the Network level. Figure 2 depicts the cloud-computing architecture.

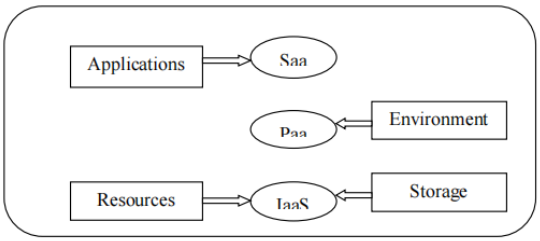

Figure 2 Cloud Computing Service Architecture

Cloud Computing Services

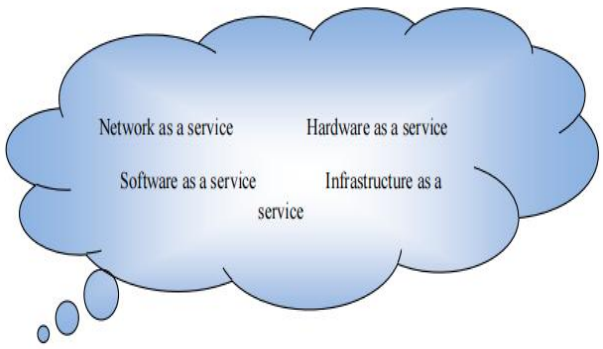

Figure 3 Cloud Computing Services

Cloud computing is an emerging framework that provides users with apps, resources, storage, and protection. Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) are three primary cloud technology services. The cloud computing infrastructure also offers other services [5]. In fig.3, the cloud computing services are depicted.

Advantages of Cloud Computing

The objective of cloud technology is to share resources as well as provide low-cost solutions. Many network operators are now utilizing this technique to distribute information more conveniently. For mail service providers, Gmail, email, and internet records management are suitable examples. In the internet and online engineering, cloud computing applications are feasible.

Cloud technology enables users to work in a more expensive, quicker, adaptable, and efficient setting. Some technologies are operating behind the cloud technology to preserve this. They are,

- Virtualization
- Service-Oriented Architecture (SOA)
- Grid compute
- Utility compute

The key benefits of cloud computing include the creation of healthy information infrastructure and greater flexibility, effectiveness, stability, and user-friendliness.

Virtualization technologies are also used to allow several organizations to share a shared resource, for example. When a cloud user requests help, the cloud gives the funding source a local identity and delivers a pointer to it. The cloud consumer can use and customize the service because of the artificial isolation among some of the multiple tenants. Utilizing Service Oriented Architecture, cloud users could use the applications over the internet (SOA). As a consequence, data can be an exchange between application programs without impacting services. Grid computing is a form of distributed computation that allows a group of machines from numerous places to work together on a common goal. Grid computing breaks complex tasks into smaller tasks, which will then be share across the CPUs accessible in the grid. The pay-per-use model underpins the utility computing platform. The computing information is shared as a demand-based, regulated service. Cloud computing, grid computing, and IT applications all employ the utility computing approach. Cloud technology has a lot of potential for productivity improvement while reducing prices. As a result, many businesses have adopted modern technology, but it also presents a lot of security threats and challenges. Cloud storage has numerous advantages. They are as follows,

- On-demand self-service
- Pay per use
- People can use the web to access services.
- Application may be used modified at any time.
- Rapid sharing of resources and flexibility
- Access to a vast network
- It provides load balancing, which enables cloud computing to be more reliable.

Deployment Models

Cloud storage has four service models, each of which is dependent on the cloud user.

The cloud consumer could be one collective of people. They are,

- Private cloud
- Public cloud
- Community cloud
- Hybrid cloud

A single user can utilize the private network to acquire cloud storage from a private enterprise. VMware, for instance, provides cloud customers with the private sector. The public cloud renders programs accessible to cloud customers via the internet. The finest public cloud provider is Google Cloud Platform. A more excellent range of companies shares the cloud environment resources out of the same community or group. The hybrid cloud offers the features of both private and public clouds.

Risks in Cloud Computing

In the contemporary and corporate world, information security is crucial. Sensitive information, including banking transactions, health records, and personal data, is exchanged between the cloud service and the cloud user via cloud computing. This information is kept in the business provider's area When migrating from a traditional computing model to a public cloud [12] [3]. Some of the significant compliance and security problems that providers and consumers alike face before migration. They are,

- Accountability
- Ownership
- Multi-tenant environment
- Geographical location

Cloud computing can address these problems when the user moves from a single cloud to multiclouds. The security of sensitive information poses a great threat to an attacker. Cloud computing has many advantages, but at the same time, it compromises security challenges and poses risks [16].

Fundamentals of Cryptography

The origins of computer security are the starting of the history of data security.

The necessity to protect hardware, software, and specific locations from external threads is a component of computer security.

Multi-level security mechanisms were used to secure mainframe computers and the integrity of data. To safeguard the network and data, an organization must use the essential multi-level security protocols. Physical security, personal protection, operational security, communications security, network monitoring, and data security are the five types of security.

Physical security is concerned with the protection of physical assets as well as unwanted accessibility or misuse. Personal protection refers to safeguarding groups or people of humans who have been allowed access to the organization. Operational and communications safety are focused on protecting a wide range of activities and communications networks. To safeguard network connections and information assets, networks information securities are utilized. An element of a building's security strategy for safe communications is the security of information.

Cryptography is a mathematical and statistical data security technique used in computer engineering. Cryptography is a combination of three terms,

- Cryptography
- Cryptology
- Cryptanalysis

Sometimes, the three terms are used indiscriminately. Cryptology is the research of communicating across unsecured networks and the security concerns that come as a result. Cryptography is a method of creating an overall cryptography network. Cryptanalysis seems to be the act of decoding a cryptographic system. The term coding concept is used to describe cryptography. It is focused onsymbolic code meanings input feature symbols as output signals. The coding theories explain how to connect via various channels, safeguard data from spillage, and assure that the signal conveyed is accurate even when there are no secure pathways.

II. LITERATURE REVIEW

Joseph Carl Robnett Licklider developed cloud computing in the year 1960. People and information can be interconnected from anything at any time using the cloud services approach.

Users can store their files on the storage capacity offered by the CompuServe organization.

The theory of web-based storing was introduced, and it is now extensively used in the commercial world. Amazon launched its cloud storage service AWS S3 in 2006, and it has since been recognized and adopted by service suppliers. SmugMug, Dropbox, and Pinterest are the three most popular services. In the year 2005, Box successfully supplied digital file sharing and the company's management services.

The fundamental purpose of cloud technology is to allow cloud users to use most of the cloud's capabilities at a low cost. Cloud consumers can use the products even if they are inexperienced with cloud computing or technologies [1]. Cloud technology relies heavily on virtualization as a critical enabling technology. For computational tasks, virtualized devices are utilized instead of actual computing devices. Infrastructure usage was raised to allow faster virtual operations and services. Automic technology is used to give services to cloud users mechanically. This automation decreases employment costs, increases productivity, and lessens the risk of making mistakes. Cloud computing involves SOA (Service Oriented Architecture) to solve multiple business concerns. Although some costly models, cloud computing addressed the grid computing's QoS (Quality of service) and stability issues. The "Pay As You Go" system, which determines prices for services used by customers, has become popular. The figures are based on computing time, data transfer, storage capabilities, and application activities. Consumers can spend for what they are using rather than paying upfront or on a month-to-month subscription model for all of these measures [14, 13, 8].In cloud computing, Yellamma et al. describe a model for making data storage and safety employing the RSA cryptosystem [17]. The author concentrated on issues concerning cloud services and virtual environment safety.In addition, the author explains cloud security agencies, key distribution, encrypting, and decryption in the cloud. According to the author, conventional hosting systems have limited capacity and usage. However, the present business tendency requires boundless solutions and data processing.

As a consequence, cloud storage has grown in popularity. It allows developers to build an environment, as well as resource allocation and reallocation on need. According to the authors, cloud computing enables cloud customers to share capabilities "as a service" and provides data centres to transfer their information globally. The researcher used the RSA technique to encrypt the information and then used the decryption algorithm when the permitted users required the data. Ashutosh et al. established a method [4] designed to offer total data protection throughout the cloud computing procedure.

To secure vital information from unauthorised access, a variety of mechanisms and techniques are employed. The proposed model is divided into four phases, as per the author. The procedure of enrolling a cloud user with a cloud provider is the first stage. The information is store in cloud data storage in the second stage. On critical data retrieval operations, the third stage is user authentication.

The authenticated public cloud retrieves information from cloud infrastructure in the fourth and final phase. The recovered data is confirmed, and all security methods are being used to ensure that the information is only accessible by permitted cloud services. According to the Brown et al. approach, information privacy and authenticity are primary security considerations for user data [6]. New techniques for data hiding and data protection can be acquired by the cloud provider [15]. All of these methods rely on the centralised dissemination of cloud data. They used a duplicate distribution strategy in their proposed system, in which retrieving requires at least a threshold amount of bits of data from the entire distribution range. Finally, the author mentioned that the SCMCS concept is used in cloud technology for multi-cloud storage. This method is used to disperse info that is financially based. This assures a high level of security and availability for the customer.

Because of its advantages, the number of cloud users is increasing every day. It is a supplier of on-demand internet platforms for a range of organizations. Storage capacity is a critical requirement for organizations. The cloud offers a high level of storage space for data.

Every day, the volumes of information stored in cloud computing increase. The necessity to secure images and text in the cloud stimulated the improvement of cryptography, which permits cloud consumers to protect their data.

A Triple Encryption Scheme

Many companies are moving to the cloud every day as a result of various advancements. Cloud computing, on either hand, confronts more significant challenges, hazards, and threats in terms of information security. In a cloud context, safeguarding sensitive data is a difficult task.

Combining these two or more methods, such as DNA cryptography and Morse pattern, is recommended for increased security. DNA cryptography using the Morse pattern is hard to emulate, rendering it more challenging for an attacker to acquire the essential information.

Morse Pattern

The Global Morse Code is a method of text messaging between transmission and reception. In the field of telephony, Samuel F.B. Morse developed it. This code transforms the actual document into "dots" and "dashes," which are non-English spontaneous languages. The ISO prosigns, Latin alphabet, Arabic numerals, Latin letters, and punctuation are stored in Morse. A separate cluster of dashes and dots represents words or a number. The dot is the fundamental measure of time in telegraphy coding transmission, and the period of the dash is

three times as much as the dot. Three dots represent the spacing among letters, and 7 dots indicate the division of words. The real benefit of the Morse code would be that it accelerates communication because the duration of a specific personality is inversely proportional to the frequency of recurrence. The letter E is the most widely utilized alphabetic letter in English and has the smallest code dot (single dot).

Differential Attack

The differential attack is an attempt of cryptanalysis that is most frequently used on block ciphers.

The technique is designed to make modest, undetectable changes in clear text to view the actual document. This would result in differences in data input and output. As a result, the attacker will be unable to establish a meaningful connection between the actual and encrypted data in terms of collapsed data. Because DNA-based Triple encrypting is hard to determine the private encryption stages behind the technique, using a new DNA sequence and modified Morse code.

Error Detection and Correction

Error detection methods are used in communications to find problems during transmitting.

When electronic information is exchange over an imperfect communication connection, an error happens. Noise is present on channels of communication as a consequence of channel noise.

In most instances, errors were made during data transfer from the origin to the destination. To identify mistakes in the transmission, error-detecting techniques have been created. The error-correcting procedures are used to repair the error and enable the data to be reformatted without mistakes.

Noise Detection

The amount of noise or interaction in all communication channels is caused by various sources such as electrical impulses, external communications, and deterioration. The parity checking is used in telecommunications to identify issues. The noise detection method is being used to identify problems that occurred during file transfer. Suppose the error detection algorithm determines that the transmitted information has been destroyed owing to noise. In that case, this will send out a message to the sender asking that the data be repeated. The parity check can be used for mistake correcting.

Image Cryptography

Ccryptography is a technique of how original data is encoded and decoded. Enciphering is the method of changing basic information into ciphertext, which is known as encryption. A cryptographic system, often called a cipher, is a scheme like this. Authentication, security systems, and integrity of data are all security services offered by cryptography. The image compression procedure utilizes image cryptography. Moni Naor and Adi Shamir developed one of the most acceptable image cryptography methods in 1994. There are three kinds of cryptography technologies. They are,

- The type of processes used only for transforming clear text to ciphertext
- The number of variables utilized
- The image analysis method

Steganography

Steganography is the method of hiding a text, picture, or sound inside another image or sound. Steganography is a mixture of the Greek words steganos&graphein. "Covered or protected" is the definition of steganos, and "writing" is the definition of graphein. Steganography relates to the procedure of concealing a hidden message or information within another image or text. Textual steganography, images steganography, and auditory steganography are examples of steganography. Steganography differentiates from cryptography in that, although cryptography is the technique of safeguarding only the content of messages. Steganography protects both the content of news and the knowledge that it is being sent. Steganography is categorized into two kinds: language steganography and technical steganography. The linguistic technique hides the information within text that is just not visible to the unaided observer.

There are 2 kinds of it. It's a mixture of semagrams and image steganography. Semagrams are signs and signals which are used to conceal information. The semagrams were split into two groups. Text and image semagrams are the two main types of semagrams. Physical things are utilize to express a statement in a visual semagram. Text semagrams are also used to alter the font size and style to change the look of the text. The technique of hiding information in a digital image is known as feature steganography.

The original image is considered the cover image, whereas the embedding image is referred to as the stego. The features of image steganography are,

- Transparency
- Robustness
- Capacity

To disguise the secret message, technological steganography uses unique gadgets, equipment, and scientific methods. To keep communications hidden, invisible inks, microdots, and computer-based technologies are use.

CONCLUSION

The process begins with understanding cloud services layers, cloud computing services, and cloud technology types. Cloud computing enables businesses to find cloud resources anywhere at time and without limitation.

Sensitive data is sent and kept at a smaller price in the cloud infrastructure. However, the cloud's immensity is limited by its security problems. The security approaches and difficulties of cloud computing storage explored. The security measures are broken easily by the adversary with today's advanced software technology. A novel model has been proposing to improve the security of the cloud computing environment.

References

[1] A Venkatesh and Marrynal S Eastaff. "A Study of Data Storage Security Issues in Cloud Computing." *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, pp. 1741-1745, Vol. 3(1), 2018.

[2] Alicherry. M and Lakshman. T. V. "Network Aware Resources Allocation in Distributed Clouds." *In Proceedings of the IEEE International Conference on Computer Communications*, pp. 963-971, Vol. 4, 2012.

[3] Anthony Velte T, Toby Velte J and Robert Elsenpeter. "Cloud computing, A Practical Approach." *Mc-Graw-Hill publishing House*, New York, 2 nd edition, 2010.

[4] Ashutosh Kumar D. "Cloud-User Security Based on RSA and MD5 Algorithm for Resource Attestation and Sharing in Java Environment." *In Proceedings of IEEE CSI Sixth International Conference Software*

Engineering (CONSEG), DOI: 10.1109/CONSEG.2012.6349503, pp. 1-6, Vol. 5, 2012.

[5] AWS| Amazon Elastic Compute Cloud (EC2):http:aws.amazon.com/ec2/. Accessed on 10.7.2015.

[6] Browne. PS. "Data Privacy and Integrity: An Overview." *In Proceedings of the IEEE International Conference on Computer Communications*, New York, USA, pp. 619–24, Vol. 24, 2011.

[7] Buyya. R, Yeo. C. S, Venugopal. S, Broberg. J and Brandic. I. "Cloud Computing and Emerging IT Platforms: Vision, Hype and Reality for Delivering Computing as 5th Utility." *Future Generation Computer System*, pp. 599-616, Vol. 25(6), 2009.

[8] Che Jianhua, Yamin Duan, Tao Zhang and Jie Fan. "Study on the Security Models and Strategies of Cloud Computing." *In Procedia Engineering*, pp. 586-593, Vol. 23, 2011.

[9] Che. J, Duan. Y, Zhang. T and Fan. J. "Study on the Security Models and Strategies of Cloud Computing." *In Procedia Engineering*, China, pp. 586–93, Vol. 23, 2011.

[10] Hayes. B. "Cloud Computing." *Communications of the ACM Digital Library*, pp. 9-11. Vol. 51(7), 2008.

[11] Mell. P and T. Grance. "The NIST Definition of Cloud Computing." *NIST special publications* 800-145, pp. 1-7, Vol. 5(3), 2013.

[12] Paul. PK, Mrinal. K and Ghose. "Cloud computing: Possibilities, Challenges and Opportunities with Special Reference to its Emerging Need in the Academic and Working Area of Information Science." *In Procedia Engineering, India*, pp. 2222–2227, Vol. 38, 2012.

[13] Pedro Ramos Brandao. "The Importance of Authentication and Encryption in Cloud Computing Framework Security." *International Journal on Data Science and Technology*, pp. 1-5, Vol.4 (1), 2018.

[14] Prabal Verma, Aditya Gupta and Rakesh Singh Sambyal. "Security Issues and Challenges in Cloud Computing: A Review." *National Conference on Recent Advances in Computer science and IT (NCRACIT)*, pp.189-196, Vol.4 (1).

[15] Rajathi. A and Saravanan. N. "A Survey on Secure Storage in Cloud Computing." *Indian Journal of Science and Technology*, pp. 4396–401, Vol. 6(4), 2013.

[16] Sengupta. S, Kaulgud. V and Sharma. VS. "Cloud Computing Security-Trends and Research Directions." *In Proceedings of IEEE World Conference on Services*, USA. pp. 524–531, Vol. 4(5), 2011.

[17] Yellamma Pachipala, Challa Narasimham, Velagapudi Sreenivas. "Data Security in cloud using RSA." *In Proceedings of the IEEE Fourth International Conference on Computing Communications and Networking Technologies (ICCCNT)*, IEEE Catalog Number: ISBN: CFP1352J-POD 978-1-4799-3927-5, pp. 338-343, Vol. 4, 2013.