ZIBELINE INTERNATIONAL PUBLISHING

ISSN: 2616-5961 (Online)
CODEN: IMCSBZ

Information Management and Computer Science (IMCS)

DOI: http://doi.org/10.26480/imcs.02.2022.31.33

REVIEW ARTICLE

REVIEW OF CLOUD COMPUTING CRYPTOGRAPHY

Rajesh De, Ipseeta Nanda*

Faculty of Information Technology, Gopal Narayan Singh University, Jamuhar, Sasaram, Bihar-821305, India
Corresponding Author Email: ipseeta.nanda@gmail.com

ARTICLE DETAILS

Article History:

Received 10 September 2022
Revised 13 October 2022
Accepted 19 November 2022
Available online 22 November 2022

ABSTRACT

The delivery of computing services over the internet, as opposed to storing data on a local memory device or a proprietary disc drive, is known as cloud computing. Servers, storage, databases, networking, and software are some examples of computing services. The primary justification and major benefit of using the cloud are the user's ability to store data there and access it from any location at any time, as well as the low cost of all its services. Despite this, because the data stored in the cloud is not directly maintained by the customer, security has always been a major concern with cloud computing. The data owners are unlikely to be aware of the route their data is taking when they upload or store data using a cloud computing service. The user is unaware of whether or not a third party is gathering, processing, and accessing their information. Numerous cryptography algorithms have been proposed to address security concerns. This paper discussed different cryptography algorithms that are present in the previous work with a focus on the fundamentals of cloud computing.

KEYWORDS

Data, Cloud Computing, Security, and Cryptography.

1. INTRODUCTION

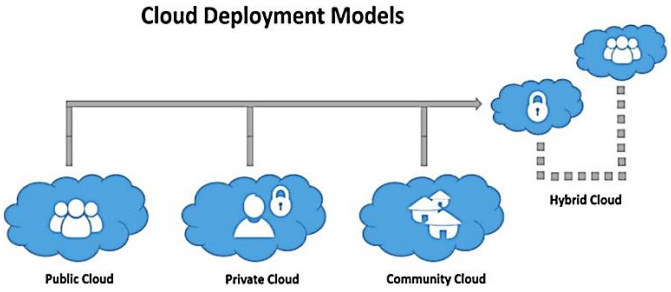
By rearranging various resources and providing them to clients in accordance with their needs, cloud computing offers a new way of providing services (Vouk, 2008). The cloud functions as a virtualized software programme. Additionally, it plays a crucial role in the upcoming generation of cellular networks and services. One of the most important cloud services is the ability to store data on the cloud, which significantly decreases the customers' storage load and gives them access to convenience. Utilizing the cloud permits the use of the utility by a character or business person online without the need to install any software (Wooley, 2011). The main advantages of cloud computing are its low cost, increased storage capacity, and flexibility. On the other hand, security and privacy issues are a major concern that are influencing the success of cloud computing (i.e. by using storing sensitive data on a third party's server in an unidentified location). Cloud safety includes the procedures and technology required to safeguard cloud computing services in favour of cloud computing. However, the solutions offered so far are ineffective and flawed, making them unworkable (Advin, 2020). Even though the risk of privacy leakage is much decreased, it is difficult to do auditing on information control when encrypted data is stored in the cloud. This particular challenge aims to bring together academics and industry professionals to discuss various facets of information security and cryptography in cloud computing (Subashini and Kavitha, 2011).

2. INTERNET OF THINGS

One of two methods is typically used to define cloud computing (Modi et al., 2013). depending on the deployment methodology or the service the cloud is providing (Winkler, 2011).

We can categorise cloud based on a deployment model as follows:

- public
- private
- hybrid
- community cloud



There are various cloud kinds accessible depending on the user or business need.

There are four different kinds of clouds.

2.1 Private Cloud

A private cloud is controlled by a third party or organisation and can only be accessed by one group or one organization (Mather et al., 2009). Larger enterprises or the government sectors frequently employ the private cloud because of its high levels of security and flexibility (Khan et al., 2012).

Quick Response Code	Access this article online	
	Website: www.theimcs.org	**DOI:** 10.26480/imcs.02.2022.31.33

Cite the Article: Rajesh De, Ipseeta Nanda (2022). Review of Cloud Computing Cryptography. *Information Management and Computer Science, 5(2): 31-33.*

2.2 Public Cloud

Any user with an internet connection and the desire to pay for their usage can access a public cloud, where the files are hosted by a third party.Amazon, the Windows Azure Service Platform, and sales force are three examples.

2.3 Community Cloud

Two or more organisations with comparable cloud requirements will be able to access a community cloud (Vijaya et al., 20160.

2.4 A Hybrid Cloud

A Hybrid Cloud is one that combines two or more clouds (public, private, and community)

Depending on a service the cloud model provides, we could be talking about:

- IaaS (Infrastructure-as-a-Service)
- PaaS (Platform-as-a-Service)
- SaaS (Software-as-a-Service)
- or, testing-as-a-service, storage, databases, information, processes, applications, integration, security, and management

The cloud provider issuer will provide the customer more or less control over their cloud, depending on how much the buyer wants to use the gap and resources connected to the cloud (Yahya et al., 2014). For instance, the need for a cloud depends on whether it will be used for personal or business purposes, or both. There are three types of cloud computing: platform as a service (PaaS), infrastructure as a service (IaaS), and software as a service (SaaS) (PaaS).

2.5 SaaS

often known as cloud software services, stands for software as a service. SaaS is managed via theassistance of hiring a third party. Saas is most frequently used in business due to the fact that it doesn't require the installation of the programme on the client computer before it can be used; instead, it runs directly through the web browser. GoToMeeting and Google Apps are a couple of typical instances of Saas.

2.6 Infrastructure as a Service (IaaS)

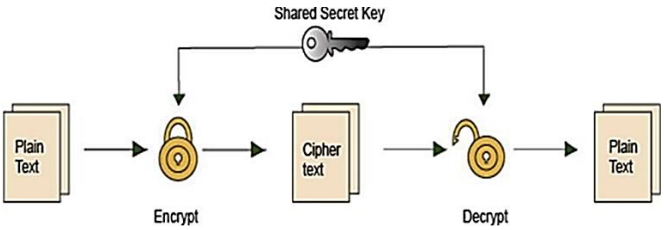
IaaS offers a variety of computer resources, hardware, software, and workshop tools on demand. Customers of IaaS can access the provider with the proper credentials by using the internet. IaaS examples are Amazon, three Tera, and Go Grid.

2.7 Platform as a Service (PaaS)

PaaS platforms perform significantly better than code as a Service setups. A PaaS supplier grants subscribers access to the conditions they need to develop and run programmes on top of the platform. J2EE, Ruby, and LAMP are among the instances of PaaS that are available .

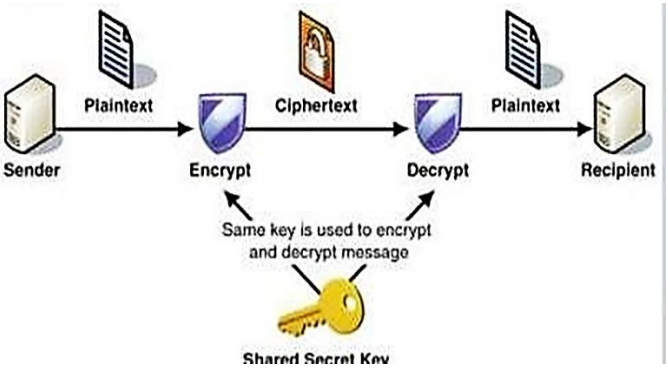
3. Cryptography

Information is protected from unauthorised parties via cryptography by being changed into an unintelligible form (Vankireddy et al., 2015). The primary goal of cryptography is to protect data from outside parties while achieving security in the areas of confidentiality, integrity, and availability. The major goal of cryptography is to protect the privacy of data stored in the cloud. The following categories of algorithms include I symmetric key-based algorithms and (ii) asymmetric key-based algorithms, also known as public-key sets of rules. Data cryptography encrypts information such as text and media to render it incomprehensible, meaningless, and invisible during transmission and storage. This process is known as encryption. Decryption is the alternative technique for recovering the original records from encrypted records. Both symmetric and asymmetric keys can be used to encrypt data stored on the cloud, but considering that the majority of databases and information are stored there Asymmetric key- based storage is slower than symmetric key- based storage.



3.1 Equilateral Key

Symmetric key cryptography is a type of encryption technique where messages are encrypted and decrypted using the same secret. Such a kind of information encoding has historically been widely utilised to assist secret communication. Nowadays, symmetric key algorithms are widely employed in many laptop architectures to improve data security. A separate key that is shared by two or more individuals is the foundation of symmetric encryption systems. The so-called "plaintext" is encrypted and decrypted using the same key (which represents the message or piece of information that is being encoded) (Swapnila et al., 2012). The process of encrypting involves passing a plaintext (input) through a cypher, an encryption method that produces ciphertext (output). The best way to inspect or gain access to the data included in the ciphertext, if the encryption technique is strong enough, is by using the associated key to decrypt it. The conversion of the ciphertext back to plaintext is the essence of the decryption process. Private-key encryption and safe key encryption are other names for symmetric encryption. It makes use of a private key, which could be a word, a phrase, or a collection of random letters. It is combined with the plain text of a message to control the content in a certain way. The personal key used to cypher and decipher all of the messages should be understood by both the sender and the recipient. Although symmetric key systems are quicker and simpler than traditional systems, the sender and receiver key exchanged in a safe manner. the data encryption device, which is the most widely used symmetric-key cryptography structure (DES).



4. Employing The DES Method for Encryption and Decryption

4.1 Data Encryption Requirements

The classic block cypher is DES, an algorithm that converts a fixed-duration string of plaintext bits into a second bitstring of the same length through a series of intricate operations. When using DES, the block size is

64 bits. In addition to using a key to modify the transformation, DES also claims that only those who are aware of the actual encryption key may successfully decrypt data. The crucial bit supposedly has 64 bits, but the algorithm only uses 56 of them because they are the most useful. Eight bits are entirely utilised for parity verification before being lost. 56 bits are the

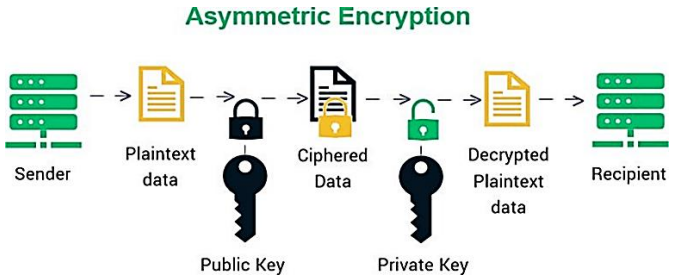
actual key period as a result. The key is typically communicated or stored as 8 bytes, each with a peculiar parity. The block is divided into two 32-bit halves and processed alternately before the main rounds; this crisscrossing is known as the Feistel scheme (Prateek and Singh, 2014). The only difference between decryption and encryption, according to the Feistel structure, is that while decrypting, the subkeys are used in the opposite sequence.

4.2 By Diffie Hellman

One of the oldest, real-world applications of public key exchange is the Diffie Hellman set of rules, which creates a shared secret key for data exchange that is confidential. ramification of authenticated protocols and serves as the foundation for a branch of cryptography (Mahim, 2018). In delivering Layer Safety's ephemeral modes, for instance, DH is employed to provide the best forward secrecy (also known as EDH or DHE depending on the cypher suite). The technique uses an exponentials module calculation to produce a key, making it secure.

4.3 Equal-sided key

The broad public key cryptography is a type of encryption that employs two keys: a primary one for encryption (the public key) and a backup key for decoding (private key). the final public key, which is known to everyone, and the owner's only private key. Even a single character alteration will result in a failure of the verification process, according to the general public key cryptography. Although asymmetric encryption does not have issues with key distribution, it is slower than symmetric encryption since it consumes so much energy.



5. RSA CRYPTOGRAPHY

The plaintext and ciphertext of the RSA algorithm are both integers between 0 and n-1 for some n. It employs exponentials and blocks of plaintext encryption using C = Me mod n, where C is the ciphertext and M is the plaintext. The plaintext is obtained in a similar manner by using M = Cd mod n, where d is the private key (Ahmed et al., 2016).

The primary characteristics of RSA are that it may be used for key exchange, digital signatures, and encryption and decryption. The most popular asymmetric encryption algorithm is this one. When you encrypt with a private key, the only way to decrypt the cypher text is with the public key. When doing online banking or logging into a website, for example, SSL/TLS (secure sockets layer/transport layer security) is used to protect the information you transmit and obtain over the internet. The major challenge with the RSA technique is that if d is known, the text included in the cypher may be easily decoded.

6. CONCLUSION

The main objective is to securely store and retrieve information in the cloud that is not under the owner's control. Software architectures frequently have a few endpoints, usually more than one client, and one or more are surrender servers. These customer-server communications take place through unreliable networks. Communication occurs across open, public networks, such as the internet, or over private networks that could be hacked by outside attackers or nefarious insiders. Communications that travel over untrusted networks can be protected using cryptography. An enemy may attempt to carry out one of several main types of attacks on a community. Attackers can listen in on a community phase and try to look at sensitive records as they travel in passive attacks. Passive attacks can be conducted offline (where an attacker collects site visitors in real-time and views them later, possibly after spending some time decrypting them) or online (where an attacker reads traffic in real-time). This paper has provided a clear view on cloud computing and its security issues using cryptography methods. Active attacks include an attacker impersonating a customer or server, intercepting communications in transit, and viewing and/or altering the contents before passing them directly to their meant vacation spot (or dropping them completely).

REFERENCES

Advin, M., 2020. Cloud Performance Evaluation: Hybrid Load Balancing Model Based on Modified Particle Swarm Optimization and Improved Metaheuristic Firefly Algorithms June 2020 International Journal of Advanced Science and Technology 29(5):Pp. 12315-12331.

Ahmed, A., Madini,O., Alassafi, R, W., 2016. Data Security in Cloud Computing.

Khan, A. U., Oriol, M., Kiran, M., Jiang, M., and Djemame,K.,2012. Security risks and their management in cloud computing, 4th IEEE Int. Conf. Cloud Comput. Technol. Sci. Proc., Pp. 121–128.

Mahim, S., 2018. Secure file storage on cloud using cryptography, Mumbai, 03 | Mar

Mather, T., Kumaraswamy, S., and Latif, S.,2009. Cloud Security and Privacy, Pp. 299.

Modi, C., Patel, D., Borisaniya, B., Patel, A., and Rajarajan, M.,Supercomput, J., 2013. A survey on security issues and solutions at different layers of Cloud computing, vol. 63, no. 2, Pp. 561–592.

Prateek G. L. M., and Singh, I., 2014. Data Encryption and Decryption Algorithms using Key Rotations for Data Security in Cloud System', International Journal Of Engineering And Computer Science vol. 3, issue 4, Pp. 5215-5223, April

Subashini S. and Kavitha V.,2011. A survey on security issues in service delivery models of cloud computing, J. Netw. Comput. Appl., vol. 34, no. 1, Pp. 1–11, Jan.

Swapnila, S., Mirajkar, Santoshkumar, B.,2012. Enhance Security in Cloud Computing, International Journal of Advanced Research in Computer Science and Software Engineering,2014. 13Ashalatha R, A survey on security as a challenge in cloud computing, International Journal of Advanced Technology and Engineering Research (IJATER) National Conference on Emerging Trends in Technology.

Vankireddy, V., Sudheer, N., Lakshmi Tulasi, R., 2015. Enhancing Security and Privacy in Multi Cloud Computing Environment, International Journal of Computer Science and Information Technologies.

Vijaya, P., Neeraj, R., KrunalJha, AnkeetDalvi.,2016. Single Cloud Security Enhancement using key Sharing Algorithm, Recent and Innovation Trends in Computing and 2016Communication.

Vouk M. A., 2008. Cloud computing - Issues, research and implementations, Proc. Int. Conf. Inf. Technol. Interfaces, ITI, Pp. 31–40.

Winkler, V. J., 2011. Securing the Cloud, Cloud Comput. Secur. Tech. tactics. Elsevier

Wooley, P. S., 2011. Identifying Cloud Computing Security Risks, Contin. Educ., vol. 1277, no. February.

Yahya, F., Chang, V., Walters, J., Wills, and B.,2014. Security Challenges in Cloud Storage, Pp. 1– 6.