International Journal of Innovations in Engineering and Technology (IJIET)
http://dx.doi.org/10.21172/ijiet.161.01

A Survey on Data Security in Cloud Computing using Cryptography Algorithms

M. Kamal[1] , Dr. G. Ravi [2]
[1]*Research Scholar in Computer Science,*
[2] *Associate Professor & Head, Department of Computer Science,*
Jamal Mohamed College (Autonomous),
(Affiliated to Bharathidasan University)
Tiruchirappalli, Tamil Nadu, India

Abstract- Cloud computing has become the best solution to deliver a flexible, on-demand solution and a dynamic scalable computing infrastructure for many applications. Cloud computing also presents a significant technological trend, which is already evident. It is transforming the information technology processes and information technology market. This paper focuses on data security in cloud environment and it discusses about various cryptography algorithms. The challenges concerned with security are to enable two parties communicate confidentially, to ensure non-repudiation and to make sure that information can be protected against spoofing and forgeries. This paper presents an overview of data security techniques that are involved in strengthening the data security in cloud environment.
Keywords – Cloud Computing, Data security, DES, AES, BLOWFISH and RSA

I. INTRODUCTION

Cloud computing is a model for enabling convenient on demand network access to a shared pool of configurable computing resources.(e.g. networks, servers, storage application and services) that can be rapidly provisioned and released with minimum management effort or service provider interaction [1]. In the cloud computing there is no need to store data in the desktop or fixed location computer. Customers can store the data in a server and they can access the data in any remote location. Cloud computing provides a large amount of data can be easily stored in the cloud. The advantages of using cloud computing are: i) reduce hardware and maintenance cost ii) accessibility around the globe iii) flexibility and highly automated process.

Nowadays, most of the organizations are switch over to cloud environment. Cloud computing users can utilize the online services which are provided by Cloud providers. There are many cloud providers such as Yahoo, Amazon, Microsoft and Google who are all offering services like Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS).

A key concept in cloud computing is that the customers of cloud can reduce the expenditure on resources like hardware, software license and other services as they can get all these things from the cloud services provider [1]. In cloud computing, security is main role. Many security experts and researchers are working endlessly to address potential threats, vulnerabilities, potential reactions, and security risks in enterprise security cloud computing.

From processing and storing sensitive data on remote computers, privacy and security concerns are not met by the customer. [2] The cloud client can flexibly manage and control different privacy mechanisms with high data protection necessary to protect critical data. Cloud customers are provided with a minimal additional cost of data protection. The cloud security model should be user-centered and non-configurable.

Data security is a most significant issue faced by Cloud environment in the IT industry. In the cloud environment, data security is a serious problem because the data is deployed in different locations, even in the entire world. To ensure data security in a cloud environment, the following cryptography algorithms are discussed. Such as RSA, AES, DES and Blowfish algorithms are discussed in this paper.

BASIC TERMINOLOGY OF CRYPTOGRAPHY

1) Plain text - The unencrypted or understandable data is called the plain text.

2) Encryption - The process of changing over plain content into cipher content that cannot be read or understood by eavesdropper.
3) Cipher text - The message that can't be comprehended by anyone or aimless message. The other name for cipher text is scrambled or encoded data.
4) Decryption - A reversed process of encryption. In this method, cipher content is changed over into plain content.
5) Encryption algorithm - Algorithm converts message into a form that cannot be read or understood normally through various substitutions and transformations on plain text.
6) Secret key - The key which is an input to the algorithm is secret and it is independent of plain text.

This paper surveys different data security techniques and is organized as follows: Section II discusses the cloud service models. Section III discusses cloud computing deployment models. Section IV discusses the security issues in cloud computing. Section V discusses a brief overview of related work. Section VI concludes the paper.

II. CLOUD SERVICE MODELS

Software-as-a-Service (SaaS): This is a software delivery model that hosts third-party provider applications and makes them available to customers through a high-speed Internet connection.

Platform-as-a-Service (PaaS): This is a middle layer which gives organizations, organizations orCompanies have access to the resources they need to develop their own applications and deploy them and their customers within the company.

Infrastructure-as-a-Service (IaaS): Infrastructure is very important in all three service models, as it is a fundamental requirement for enterprises to launch their services on the Internet through a cloud platform and enable their services to customers and applications. They are consistent [3].On the basis of such considerations, the algorithm uses a different color image multiplied by the weighting coefficients of different ways to solve the visual distortion, and by embedding the watermark, wavelet coefficients of many ways, enhance the robustness of the watermark.

III. CLOUD COMPUTING DEPLOYMENT MODELS

Public Cloud: Cloud services are easy to install and are free of charge or free of charge, applications, hardware and bandwidth are provided by the service provider, and they are scalable and can only access the services the user is interested in [4].

Private Cloud: As its name implies, its services and infrastructure are owned and maintained by only one company. The services are available at the proper authentication and the customer's data security is prioritized [1].

Community Cloud: Cloud resources are shared by an organization here, which is of common interest to every participant who is part of a community and whose needs are similar [1].
Hybrid Cloud: A combination of two or more cloud deployment models (public, private, community) that enables cloud application portability, multi-tenant, and resource sharing [4].

IV. SECURITY ISSUES IN CLOUD COMPUTING

There are many security issues are arises during the data transfer between service providers and customers. Such as Multi- tenancy, Elasticity, Insider attacks, Outsider attacks, Loss of control, Malware Injection, Flooding Attack Problem and Data Loss.

Techniques to Secure the Data in Cloud:

The following techniques are used to protect data in the cloud environment.

a. Authentication and Identity

b. Data Encryption

c. Information integrity and Privacy

d. Availability of Information

e. Secure Information Management

f. Malware-injection attack solution.

g. Flooding Attack Solution

DATA SECURITY

Data security continues to be an important issue in information technology. In the cloud computing environment, this becomes especially acute because data is located in different locations, even across all worlds. Data security and privacy protection are two key factors of a user's concerns about cloud technology. While many technologies on cloud computing are explored by both academics and businesses, data security and privacy protection are becoming increasingly important for the future development of cloud computing technology in government, industry and business.

Data security and privacy security issues are relevant to both hardware and software in the cloud architecture. This review is a review of different security techniques and challenges from software and hardware features for cloud data protection and aims to improve data security and privacy protection for a trusted cloud environment. In this study, we perform a comparative research analysis of existing research work on data protection and privacy protection techniques used in cloud computing.

Cloud has a security problem in terms of data segmentation, data theft, unauthorized access, obscure ownership and data protection, data loss conditions. [5]

DATA SECURITY FRAMEWORK

Security is a key concern for accessing data in the cloud. Security protects data from being lost, destroyed or altered. [6]

1) Protecting data: Cloud providers can protect data from an external user by creating security keys, such as a private key.

2) Building Blocks: Mathematical and Cryptographic Principles Building blocks of server security

3) Integrity of data: The user can verify the integrity of the integrity policies when uploading the data.

4) Access Data: Data can be accessed safely due to encryption and encryption techniques.

5) Authentication: Authentication allows only authorized users to access data in the cloud.

V. RELATED WORKS

The paper is mostly related to works in security of the user’s data. Some of the works are listed below.

Sarita Kumari [7] proposed techniques of cryptography encryption and compression. The goal is to improve privacy, probity, confirmation through the process of encryption and decryption during access. The proposed work also includes compression to condense the size of data in order to save space. Methods like lossy and lossless are used for compressing the data.

Shivani Sharma et al. [8] developed RSA algorithm for secure data transmission.RSA algorithm includes a public key and a private key. In RSA, an intruder can successfully constitute a chosen plain text attack against the crypto system. The property of RSA is, the product of two cipher texts is identical to the encryption of the outcome of respective plain text.

Yashaswini J [9] proposed a key distribution for symmetric key cryptography. The objective is to improve the key distribution and provide the different approaches used in distribution of keys. Many authentication and key distribution protocols are used. The server can easily recognize the authorized client by checking the legality of the key.

Manali Naik et al. [10] proposed substitution method for Cryptography. The author used creative cryptographic substitution method to produce a stronger cipher. The main focus is on the substitution of characters, numbers, and special blocks with color blocks.

Network security with cryptography proposed by Prof. Mukund et al. [11] suggested the Principles of Cryptography, types of Cryptosystem and algorithm for encryption and decryption.

Mansoor Ebrahim et al. [12] present a comprehensive comparative scrutiny of different existing algorithms based on certain parameters. The parameters incorporate architecture, Security, scalability, memory usage, restrictions and flexibility that are important for secure communication.

Dr.Sandeep Tayal [13] et al. designed different strategies which are utilized as a part of Cryptography for Network security reason. This also proposed, information hiding a procedure utilizing AES calculation. The paper gives a comparative study of various encryption algorithms on the basis of their ability to secure and shield data against attacks.

This list is used to allocate resources to users on request. Cloud secure federation occurs when a customer uses different services from different clouds; it must maintain its security requirements implemented by cloud providers. User identification, authentication and authentication will solve single-sign federation problems. Table 1 shows a comparison of different cryptography algorithms.

Parameters /Algorithms	**DES**	**AES**	**BLOWFISH**	**RSA**
Key size	56 bits	128, 192, 256 bits	32 - 448 bits	1024 Bits
Block Size	64 bits	128 bits	64 bits	Variants
Introducer	IBM 75	Rijmna Joan	Bruce Schneier	Ron Rivest, Adi Shamir, and Leonard Adleman
Data encryption capacity	Encrypt average amount of data	Encrypt large amount of data	Encrypt average amount of data	Encrypt small amount of data
Memory usage	High RAM needed	Low RAM usage	Execute in less than 8 KB	Highest Memory usage
Execution Time	Faster	Faster	Lesser time to execute	Require maximum time
Security	Security applied to both providers and user	Secure for both provider and user.	Secure for both providers and user/client side	Secure for user only

Table 1: Comparison of different Cryptography algorithms

The above table discusses various cryptographic algorithms that are used to secure the data in the cloud storage. DES is the most basic cryptographic algorithm to implement. AES algorithm is the next step beyond DES algorithm. Blowfish algorithm takes least memory required & minimum time need to execute the algorithm. RSA is the asymmetric algorithm that can be used to ensure confidentiality while sharing data.

VI. CONCLUSION

In this paper, cryptography algorithms are provided to make cloud data safer and more vulnerable to security issues, competitions and evaluations between RSA, AES, DES and Blowfish algorithms are used to find a better security mechanism. The parameters concerned key size, block size, memory usage and execution time. It has been used in cloud computing to protect cloud data and to minimize invaders. It also helps to develop new encryption algorithms that strengthen the security further either by using symmetric or asymmetric techniques.

REFERENCES

[1] Sean Carlin and Kevin Curran, " Cloud Computing Security", International Journal of Ambient Computing and Intelligence, 3(1), 14-19, January-March 2011.
[2] Wassim Itani, Ayman Kayssi and Ali Chehab, "Privacy as a Service: Privacy-Aware Data Storage and Processing in Cloud Computing Architectures," Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, 2009.
[3] Mohamed A.AlZain, Eric Pardede, Ben Soh and James A. Thom, "Cloud Computing Security From Single to Multi-Clouds," 45th Hawaii International Conference on System Sciences, 2012.
[4] Cong Wang, Kui Ren, Jin Li and Wenjing Lou, "Toward Publicly Auditable Secure Cloud Data Storage Services," IEEE Network, July/August 2010.
[5] Lifei Wei, Haojin Zhu, Zhenfu Cao, Xiaolei Dong, Weiwei ia, Yunlu chen and Athenasios V.Vasilakos, "Security and privacy for storage and computation in cloud computing", Information Sciences, 258(2014) 371-386.
[6] Mohammed, E.M, Ambelkadar, H.S, "Enhanced Data Security Model on Cloud Computing," 8th International Conference on IEEE publication 2012.
[7] Sarita Kumari, "A Research Paper on Cryptography Encryption and Compression Techniques", International Journal of Engineering and computer Security", Vol: 06, Iss: 04, April 2017.
[8] Shivani Sharma, Yash Gupta, "Study on Cryptography and Techniques", International Journal of Scientific Research in Computer Science, Engineering and Information Technology, Vol: 02, Iss: 01, 2017.
[9] Yashaswini J, "Key distribution for Symmetric Key Cryptography: Review", International Journal of Innovative Research in Computer and Communication Engineering, Vol: 3, Iss: 5, May 2015.
[10] Manali Naik, Pushpanjali Tungare, Pooja Kamble, Shirish Sabnis, "Color Cryptography using Substitution method", International Research Journal of Engineering and Technology, Vol: 03,Iss: 03, 2016.
[11] Prof.Mukund R.Joshi, Renuka Avinash Karkade, "Network security with Cryptography", International Journal of Computer Science and Mobile Computing, Vol: 04, Iss: 1, Jan 2015, pg 201-204.
[12] Mansoor Ebrahim, Shujaat Khan, Umer Bin, "Symmetric algorithm Survey : A Comparative Analysis ", International Journal of computer applications, Vol: 61-No.20, Jan 2013.
[13] Dr.Sandeep Tayal, Dr.Nipin Gupta, Dr.Pankaj Gupta, Deepak Goyal, Monika Goyal, "A Review paper on Network Security and Cryptography", Advances in Computational Sciences and Technology, Vol : 10, Pg: 763-770, 2017.