



A Review of Challenges of Cryptography Techniques in Cloud Computing

Ashish A. Patokar¹, Dr. V. M. Patil²

¹Assistant Professor, ²Head & Associate Professor

^{1,2}Department of Computer Science & Information Technology,
Shri Shivaji College, Akola, Maharashtra, INDIA.

Abstract: Cloud computing is a collection of IT Services offered through the Internet such as network, software and resources are supplied to a customer beyond a network. These Services are delivered by the third-party provider who owns the infrastructure. In Cloud Computing environment there is different collection of popular issue which includes issue of privacy, data security etc. In Cloud computing technology different cryptographic techniques are used such as DES, AES and RSA to insure that the security of data in cloud computing environment. In this paper Study the survey on review of challenges of security problems, of cryptography techniques over the cloud computing environment. Cryptography challenges include access control over the data lifecycle back and availability.

Keywords: Cloud Computing, Security Issues, Cryptography Techniques.

I. INTRODUCTION

Cloud Computing is the circulation – internet foundation support technology spared computing, this uses the internet and remote servers to sustain the application and information. Cloud Computing is defined as the collection of services or resources given by the internet to the users on their requirement by the cloud providers [1]. Cloud Computing contains several types of services such as IaaS, PaaS, SaaS and deployment model such as public, private and hybrid etc [2].

An Cryptography is the art and science of framing cryptosystem that is useful for supply information or data security. A cryptosystem is an implementation of cryptographic techniques. The components of cryptosystem such as plaintext, cipher text, encryption, decryption algorithm. Encryption is the process of converting plain text into cipher text and decryption is reverse of encryption that is process of converting cipher text into plain text [3]. Security of goals includes data security, data access, data confidentiality, denial of services, governance and privacy. The cryptography is combination of three types of algorithms.

- (a) DES Algorithm
- (b) AES Algorithm
- (c) RSA Algorithm

Challenges of cryptography include access control over the data lifecycle back and availability and data trust management. There is no 100% guarantee for security, cryptography can help significantly and have already need algorithms and protocols to secure over system.

II. LITERATURE REVIEW

Jaspreet Singh et al. (2015) in a Review on Cloud Computing Security Issues and Encryption Techniques [1] have described the security problem and encryption algorithm that provide security to the cloud data.

G K Patra et al.(2014) in a Securing Cloud Infrastructure for High Performance Scientific Computations Using Cryptographic Techniques [2] have focused on high performance cloud computing model can be introduced , cloud computing and its security challenges, security threats in cloud computing , techniques to ensure secured cloud HPC services.

Laurentiu BURDUSEL (2013) in New Cryptography Challengers in Cloud Computing Era [3] have focused on a review of new cryptographic techniques used for protecting the data from a remote storage and not only protected, but to be able to process remote encrypted data. Also described several types of services, data security issues in the cloud , homomorphic encryption and challenges.

Sashank Dara in Cryptography Challenges for Computational Privacy in Public Clouds [4] have focused on challenges with cryptographic techniques , cloud computing, delivery models such as SaaS, PaaS, IaaS, security and privacy of cloud, cryptographic techniques such as fully homomorphic encryption (FHE) , server aided secure multi party computation, functional encryption, instance hiding , superimposing encrypted data, hardware approaches and specialized operation, etc.

Shakeeba S. Khan (2015) in Security in Cloud Computing using Cryptographic Algorithms [5] have described cryptographic algorithm such as data encryption standard algorithm (DES), RSA algorithm described by how the message encrypted with the public key can only be decrypted using private key the process is discovered by using the block diagram of multilevel encryption.

Mayank Patwal et al. (2014) in A Survey of Cryptographic based Security Algorithms for Cloud Computing [6] have focused on fundamental characteristic cloud computing service model of cloud computing such as IaaS, SaaS, PaaS, deployment model of cloud computing data security in cloud computing security issues, security advantages and disadvantages in cloud environment, cryptographic algorithm such as RSA, DES, and AES algorithm, Digital signature.

Sharmila Rajasudhan et al. (2014) in A study on cryptographic methods in cloud storage [7] have discussed the opportunity for cryptography to address some of these security challenges, types of cloud environment such as public, private, and hybrid, advantages and security concerns, cryptographic cloud storage, cryptographic techniques identity based encryption, attribute base encryption. This paper describes various cryptographic techniques that can be used in cloud computing environment.

Rashmi Nigoti et al. (2013) in A Survey of Cryptographic Algorithms for Cloud Computing [8] have discussed how to protect data from unauthorized accessed, modification or denial of services etc. Also survey different security issue to cloud and different cryptographic algorithm to better security for the cloud.

S. Arul Oli et al. (2016) in Confidentiality Technique for Enhancing Data Security using Encryption and Obfuscation in Public Cloud Storage [9] have proposed the technique to enhance security level. This paper produces minimum time data size and service while uploading into the cloud storage.

Shrif El-etriby (2012) in Modern Encryption techniques for Cloud Computing [10] have focused on data storage security in cloud and desktop cryptography algorithms are implemented using Java cryptographic extensions (JCE). Also present evolution of eight encryption techniques namely RC4, RC6, MARS, AES, DES, 3DES, Two-Fish, and Blow-Fish etc.

Manpreet Kaur et al. (2013) in Implementing Encryption Algorithms to Enhance Data Security of Cloud in Cloud Computing [11] have discussed security algorithm such as RSA, DES, AES and Blow-Fish algorithms, architecture cipher cloud. This paper suggests selective encryption techniques, which almost gives the data confidentiality just like private cloud models.

Saurin Khedia et al. (2014) in A Review on Hybrid Techniques of Security In Cloud Computing [12] have focused on comprehensively survey the various existing hybrid security techniques of cloud computing such as SaaS, PaaS, IaaS, deployment model of cloud computing such as public private, and hybrid cloud. Also these paper present different hybrid security techniques for cloud computing with wide variety of application of cloud computing, security solution are mainly privacy aware and data owner centric.

Rakhi Emelaya et al. (2015) in A Survey: Secure Data Storage Techniques in Cloud Computing [13] have described Optimized blowfish homomorphism encryption with SHA-2 for key generation to make encryption more authentic. In this paper survey the RSA, RC4, KP-ABE, AES and Blowfish algorithms to enhance the performance and encryption and decryption time.

Geethu Thomas et al. in Cloud computing security using encryption technique [14] have proposed security issues and some of its solution are explained and are concentrating mainly on public cloud security issue and there solution. Security issues can be categorized as Abuse and nefarious use of cloud computing, in secure application programming interfaces, malicious insiders.

Harpreet Singh et al. (2014) in Securing Data Storage on Public Cloud by Encryption Based 2-Way Authentication [15] have implement private and public cloud. This paper proposed new architecture for cloud data storage in which the private cloud should store only the organizations sensitive structure information and the public cloud should store the actual data in cipher text form by using newly design encryption algorithm.

Akshay D. Kapse et al. (2014) in Secure and Efficient search Techniques in cloud computing[16] have focuses on review of various methodologies which helps user for secured storage and efficient access to the data and secure and efficient system have been proposed to reduce the burden of the system thus to decrease complexity and to improve performance of overall system.

Shyam Nandan Kumar (2015) in Review on Network Security and Cryptography[17] have discussed on the state of the art for a broad range of cryptographic algorithms that are used in Networking applications. This paper also focuses on types of security attacks, security attacks, security services, network security model, cryptographic algorithms, message authentication code, network and internet security, firewalls and its characteristics, types of firewalls etc.

III. CRYPTOGRAPHIC TECHNIQUES

1. DES
2. AES
3. RSA

1. DES Data Encryption Standard:

Data Encryption standard (DES) is developed by IBM for the US government. DES is most widely used block cipher in world. DES is a symmetric- Key block cipher published as FIPS-6 in the federal register in January 1977 by NIST as a standard. DES takes a 64-bit cipher text and creates 64- plaintext at the decryption site and

56 bit cipher key is used for both encryption and decryption [5]. The encryption process is made of two permutations, which we call initial and final permutation, and sixteen Feistel rounds [8]. DES is a block cipher, as shown in Figure

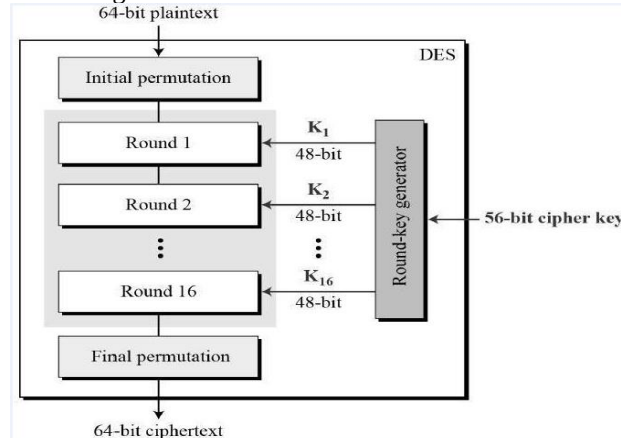


Figure 1: Encryption with DES

Each round uses a different 48-bit round key generated the cipher key algorithm as shown in Fig. The function F is made up of four section:

- Expansion P-box
- A whitener (that-adds key)
- A group of S-boxes
- A straight P-box.

2. AES Advanced Encryption standard:

The advanced encryption standard (AES) is a symmetric-key block cipher published by the National Institute of standards and Technology (NIST) in December 2001. NIST announced that a draft of the federal information processing standard (FIPS) was a variable for public review and comment. [5]. AES was published as FIPS 197 in the Federal Register in December 2001. The block size of AES encrypts data is 128, 192 or 256 bits. AES operates on a 4X4 column-major order matrix of bytes. The criterion for NIST for AES is falls on three areas such as security, cost and implementation [8].

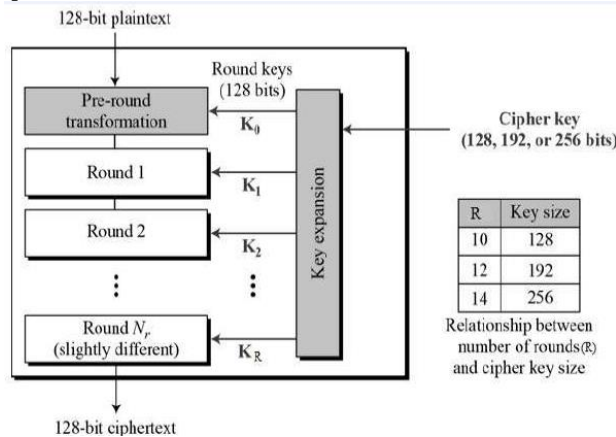


Figure 2: schematic of AES structure

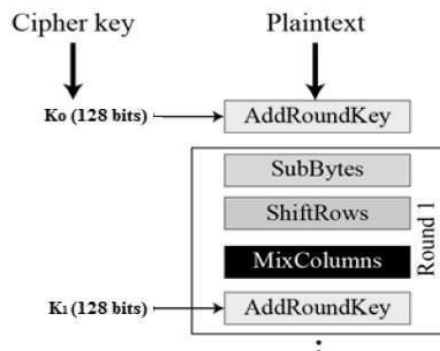


Figure 3: Encryption Process with AES

3. RSA

The system was invented by three scholars Ron rivest, adi Shamir, and len Adleman and hence, it is termed as RSA crypto system. RSA uses modular exponential for encryption and decryption. It depends on property of positive integers [5] [8].

RSA uses two exponents, a and b , where a is public and b is private, then an encryption

$$c = p^a \bmod n$$

And at decryption side

$$P = c^b \bmod n.$$

n is very large number, created during key generation process. The process is shown in fig.

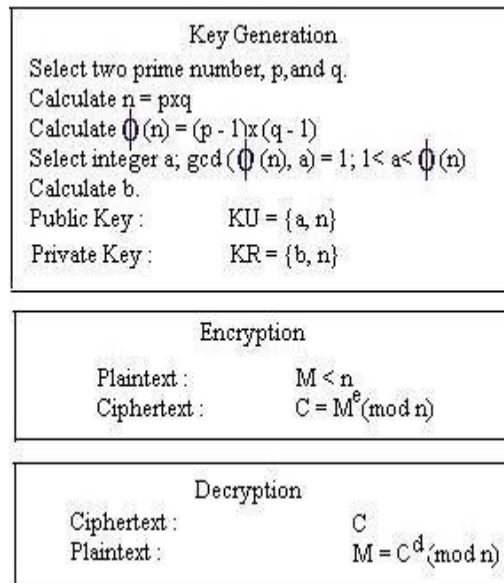


Figure 4: RSA algorithms [8]

IV. SECURITY ISSUE IN CRYPTOGRAPHIC TECHNIQUES

a) Data Integrity:

The data in the cloud floats reach from the actual data holder to the other side and end user, due to migration of data to cloud the service provider cannot maintain data integrity and safety. For the security of the data, cloud service providers should apply mechanisms to convince data truthfulness and define data set at the point [6].

b) Data access:

Data access is primarily informed to the security schemes that are given to the users while ensuring cloud data. The organization use the cloud provided by the provider to conducting its business process and the organization have notice polices to access the business data stored on cloud [1].

c) Data Confidentiality:

Data Confidentiality is the quality that data contents are not accessible to the illegal users. Users can supply their data and information on remote servers accessed through the internet, only authorized users can access the sensitive data while others not gain only information of the data. Cloud data services, data search, data computation, and data sharing utilize the data without the leakage of data [1].

d) Denial of service:

Denial of service is a discrete problem for cloud computing, attacker highjack the service and easily target the machine those which are connected outside the world of cloud and IP addresses [1].

e) Governance:

Cloud computing need suitable IT governance model to assure a secured computing environment and to carry with all relevant organizational information technology schemes. Organization require a set of capabilities that are important when effectively implementing and arranging cloud services, that include demand management, data security management risks and compliance management [8].

f) Privacy:

The providers accrued that all crucial data such as credit card number are encrypted and only authorized users can access to data in its entirety. Digital identities and credentials ought to be protected and the data that the provider produces about costumer's activity in cloud [6].

V. CHALLENGES OF CRYPTOGRAPHIC TECHNIQUES

- There is no better way to secure critical data than through cryptography - especially when that data is stored in the cloud. While no one can guarantee 100% security, cryptography can help significantly is that we already have the algorithms and protocols we need to secure our systems.
- "In the cloud, we don't have the richness of having actual, physical control over the storage of information, so the only way we can ensure that the information is protected is for it to be stored cryptographically, with us maintaining control of the cryptographic key."
- Challenges include access control over the data lifecycle back and availability.
- Cryptography for cloud data trust management.
- Cryptography for auditing on cloud data management.
- Cryptography for secure IOT data process at cloud.

VI. CONCLUSION

Cloud Computing is a collection of services offered by the internet to the client on their demand by cloud providers. Every organization is carrying its data to the cloud, that it uses the storage services provided by the cloud provider, so there is a need to secure that data to the unauthorized access by cloud computing can made secure using cryptographic techniques/ algorithms. This paper is largely based on security issue, security techniques and challenges of cryptographic techniques.

References

- [1] Jaspreet Singh, Sugandha Sharma, "Review on Cloud Computing Security Issues and Encryption Techniques", International Journal of Engineering Development and Research, Volume 3, Issue 2, ISSN: 2321-9939, 2015, pp 1051-1053.
- [2] G K Patra, Nilotpal Chakraborty, "Securing Cloud Infrastructure for High Performance Scientific Computations Using Cryptographic Techniques", International Journal of Advanced Computer Research (ISSN (print): 2249-7277 ISSN, Volume-4 Number-1 Issue-14 March-2014, pp 66-71.
- [3] Laurentiu BURDUSEL, "New Cryptography Challengers in Cloud Computing Era", Proceeding of the Romanian Academy, Volume 14, Number 1/2013, pp 72-77.
- [4] Sashank Dara, "Cryptography Challenges for Computational Privacy in Public Clouds".
- [5] Shakeeba S. Khan, Prof. R. R. Tuteja, "Security in Cloud Computing using Cryptographic Algorithms", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 3, Issue 1, January 015, pp 148-154.
- [6] Mayank Patwal and Tanushri Mittal, "A Survey of Cryptographic based Security Algorithms for Cloud Computing", HCTL Open Int. J. of Technology Innovations and Research HCTL Open IJTIR, Volume 8, March 2014 E-ISSN: 2321-1814, pp 1-17.
- [7] Sharmila Rajasudhan, Nallusamy R, "A Study on Cryptographic Methods in Cloud Storage", International Journal of Communications Technologies, Volume 02-No. 01, Issue:02, March 2014, pp 1-5.
- [8] Rashmi Nigoti, Manoj Jhuria, Dr. Shailendra Singh, "A Survey of Cryptographic Algorithms for Cloud Computing", International journal of Engineering Technologies in Computational and Applied Science(IJETCAS), 2013, pp 141-146.
- [9] S. Arul Oli, Dr. L. Arockiam, "Confidentiality Technique for Enhancing Data Security using Encryption and Obfuscation in Public Cloud Storage", International Journal of Advanced Research in Computer and Communication Engineering Vol. 5, Issue 2, February 2016, pp 431-435.
- [10] Shrif El-etriby, Eman M. Mohamed, "Modern Encryption techniques for Cloud Computing", ICCIT, 2012, pp 800-805.
- [11] Manpreet Kaur, Rajbir Singh, "Implementing Encryption Algorithms to Enhance Data Security of Cloud in Cloud Computing", International Journal of Computer Applications (0975 – 8887), Volume 70– No.18, May 2013, pp 16-21.
- [12] Saurin Khedia, Nishant Khatri, "A Review on Hybrid Techniques of Security In Cloud Computing", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 2, Issue 11, November 2014, pp 6389-6393.
- [13] Rakhi Emelaya, Dr. Sanjay Agrawal, "A Survey: Secure Data Storage Techniques in Cloud Computing", International Journal on Recent and Innovation Trends in Computing and Communication Volume:3, Issue: 9, IJRITCC, September 2015, pp 5376-5379.
- [14] Geethu Thomas, Prem Jose V, P. Afsar, "Cloud computing security using encryption technique", pp 1-7.
- [15] Harpreet Singh, Er. Gagandeep Singh, Er Madhu Bahl, "Securing Data Storage on Public Cloud by Encryption Based 2-Way Authentication", International Journal of Emerging Research in Management & Technology ISSN: 2278-9359 (Volume-3, Issue-7), July 2014, pp 87-92.
- [16] Akshay D. Kapse, Piyush K. Ingole, "Secure and Efficient search Techniques in cloud computing", 2014 Fourth International Conference on Communication systems and Network Technologies, pp 743-747.
- [17] Shyam Nandan Kumar, "Review on Network Security and Cryptography", International Transation of Electrical and Computer Engineers system, Vol. 3, No. 1, 2015, pp 1-11.