Asian Journal of Computer Science and Technology
ISSN: 2249-0701 Vol.8 No.S3, 2019, pp. 76-80

Cloud Computing Security Using Cryptographic Algorithms

K. Srilakshmi[1] and P. Bhargavi[2]
[1]Research Scholar, [2]Assistant Professor, [1&2]Department of Computer Science,
Sri Padmavati Mahila Visva Vidyalayam, Tirupati, Andhra Pradesh, India
E-Mail: srilakshmi21kakarla@gmail.com, pbhargavi18@yahoo.co.in

Abstract **- Cloud computing is a new and fast emergent technology in field of computation and data storage as a service at very eye-catching facilities. It provides fast and well-organized on demand services for storage, network, software, and hardware through the Internet. Applications that run in the cloud can balance various elements comprising load balancing, bandwidth, security and size of data. Major problems to cloud adoption are data privacy and security, because the data owner and the service provider are not within the similar trusted domain. Safety issues are increasingly significant in lowest layer Infrastructure as a Service (IaaS) to higher Platform as a Service (PaaS).In this paper we present range of dissimilar techniques or security algorithms exploiting to uphold the secrecy and security of the cloud with cryptographic algorithms.**

Keywords: **Cloud Computing, Data Security Challenges, Cryptographic Algorithms**

1. INTRODUCTION

In the recent years, Information Technology services rise tremendously, thereby IT needs to expand its architecture and infrastructures to afford more services. As a result, IT service providers are faced with challenges of expanding infrastructures with minimum expenditure and less time in order to provide rising demands from the customers. To meet these business challenges, cloudcomputing architecture was developed. Cloud computing architecture is an environment ofIT resource for particular services which is outsourced to customers [1].

Cloud computing is not a new idea, however it is mounting in last two decades and it will have major service in the areas of servers, software, storage, and networking [2]. Cloud Service Provider (CSP) maintains database and applications for the users on a remote server and provides independence of accessing them from any place through a network. There are three major cloud service categories: Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and infrastructure-as-a-service (IaaS).

Infrastructure services provide an environment that allows enterprises to access their applications faster, with easier manageability, and minimum maintenance to meet their business demands. Most of the large companies have promoted their own cloud computing platforms and infrastructures for users to deploy their web applications on these platforms.

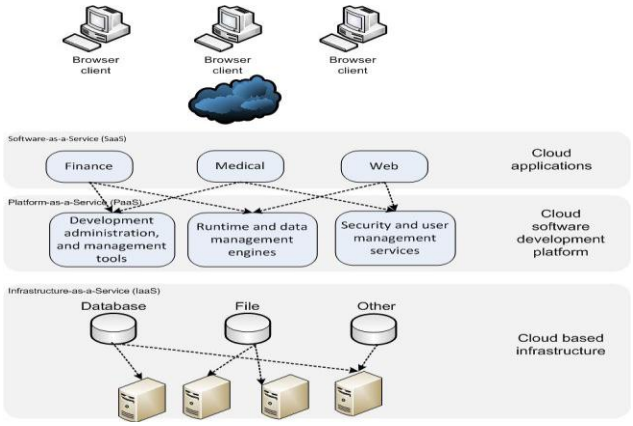

Fig. 1 Cloud Services Architecture [4]

Cyber crime's effects are felt throughout the Internet, and cloud computing is an enticing target for many reasons. Providers such as Google, Microsoft, and Amazon have the existing infrastructure to deflect and survive cyber-attacks, but not every cloud has such capability. If a cyber-criminal can identify the provider whose vulnerabilities are the easiest to exploit, then this entity becomes a highly visible target. If not all cloud providers supply adequate security measures, then these clouds will become high-priority targets for cyber criminals. By their architecture's inherent nature, clouds offer the opportunity for simultaneous attacks to numerous websites, and without proper security, hundreds of websites could be compromised through a single malicious activity.

As cloud computing offers massive benefits, each and every organization are moving their data to the cloud. So there is a need to protect that data against unauthorized access, modification or denial of services etc. To secure the Cloud means secure the treatments (calculations) and storage (databases hosted by the Cloud provider). Security goals of data include three points namely: Availability Confidentiality, and Integrity. Confidentiality of data in the cloud is accomplished by cryptography [3]. Cryptography, in modern days is considered combination of three types of algorithms. They are (1) Symmetric-key algorithms (2) Asymmetric-key algorithms and (3) Hashing. Integrity of data is ensured by hashing algorithms.

Data cryptography is the state of art of scrambling the content of the data to make the data unreadable or meaningless during transmission or storage is termed

Encryption. The main aim of cryptography is to take care of data secure from invaders. The process of getting back the original data from encrypted data is Decryption, which restores the original data. To encrypt data at cloud storage both symmetric-key and asymmetric-key algorithms can be used. Cloud storage contains a large set of databases and for such a large database asymmetric-key algorithm's performance is slower when compared to symmetric-key algorithms [5].

In this paper, our focus is to do an extensive survey of various cryptographic algorithm that are providing data security in cloud services such as infrastructure-as-a-service (IaaS). The rest of the paper is framed in such a fashion, data security issues followed byfew data security models that include symmetric and asymmetric keycryptographic algorithms and comparison of security algorithms in the cloud services.

II. DATA SECURITY ISSUES

SysAdmin, Audit, Network, Security (SANS) defines Data security issues and methodologies which are deliberate to protect sensitive information or data from unauthorized access, disclosure, modification, or use. The form of the protected data or information can be electronic, printed, or other forms [4] [7]. Information security encompasses three fundamental security attributes namely confidentiality, availability and integrity [6]. The presence of these attributes characterizes secured information. Besides these, three fundamental attributes, non-repudiation and accountability complement the characteristic of secured information [4] [6]. The five issues of information security are shown in figure 2.
The five security issues are described as follows:

1. *Confidentiality:* This is concerned with protecting the sensitive information from the unauthorized or illegal disclosure [8].
2. *Integrity:* This is concerned with accuracy, completeness and validity of information in regards with business requirement and expectations [8].
3. *Availability:* This is concerned with information being operational and accessible whenever it is required by the business process now as well as in the future [4][8] [6]. Further, the information must be inaccessible to unauthorized users [6].

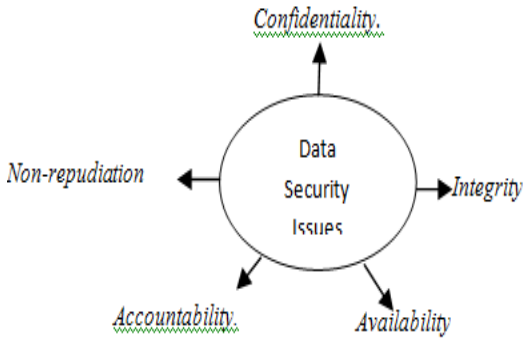

Fig. 2 Data Security Issues[4][6]

4. *Accountability:* This is concerns with keeping track of actions that are related to security actions and responsibilities [6].
5. *Non-Repudiation:* This is concerns with the ability to prevent users from denying the responsibility of the actions performed [6].

III. DATA SECURITY ALGORITHMS

Cloud services will become high-priority targets for cyber criminals due to its architecture's and have chance to simultaneous malicious parties, User's data must be made secure in the cloud using encryption. Data security supports all business issues such as full disk encryption, database encryption, file system encryption, distributed storage encryption and even row or column encryption.

Basically there are two types of encryption algorithms symmetric-key and asymmetric-key algorithms [5]. Private Key cryptography is also known as symmetric key cryptography. In symmetric Key algorithms, the longer the key length, the stronger the encryption. Also, although long key lengths provide more protection, they are more computationally intensive, and may strain the capabilities of computer processors. Here two symmetric key algorithms Data Encryption Standard (DES) & Advanced Encryption Standard (AES) and an Asymmetric key algorithm RSA are discussed.

A. Symmetric Key Algorithms

1. Data Encryption Standard (DES)

DES [18] is one of the most widely accepted, publicly available cryptographic systems. It was developed by IBM in the 1970s but was later adopted by the National Institute of Standards and Technology (NIST), as Federal Information Processing Standard 46 (FIPS PUB 46).The Data Encryption Standard (DES) is a block Cipher which is designed to encrypt and decrypt blocks of data consisting of 64 bits by using a 64-bit key [10, 15].Fig2: RSA processing of Multiple Blocks [3]. Although the input key for DES is 64 bits long, the actual key used by DES is only 56 bits in length. The least significant (right-most) bit in each byte is a parity bit, and should be set so that there are always an odd number of 1s in every byte. These parity bits are ignored, so only the seven most significant bits of each byte are used, resulting in a key length of 56 bits. The algorithm goes through 16 iterations that interlace blocks of plaintext with values obtained from the key. The algorithm transforms 64-bit input in a series of steps into a 64-bit output. The same steps, with the same key are used for decryption. There are many attacks and methods recorded till now those exploit the weaknesses of DES, which made it an insecure block cipher. Despite the growing concerns about its vulnerability, DES is still widely used by financial services and other industries worldwide to protect sensitive on-line applications [17, 19]. The general structure of DES Encryption algorithm is shown in Fig. 3. The algorithm

processes with an initial permutation, sixteen rounds block cipher and a final permutation (i.e. reverse initial permutation).

2. Advanced Encryption Standard (AES)

AES is a block cipher with a block length of 128 bits. It allows three different key lengths: 128, 192, or 256 bits. In general 128 key lengths are considered in which encryption process consists of 10 rounds of processing. Except for the last round in each case, all other rounds are identical. 16-byte encryption key, in the form of 4-byte words is expanded into a key schedule consisting of 44 4-byte words. The 4 x 4 matrix of bytes made from 128-bit input block is referred to as the state array. Before any round-based processing for encryption can begin, input state is XORed with the first four words of the schedule. Fig. 4 shows AES encryption flow. For encryption, each round consists of the following four steps:

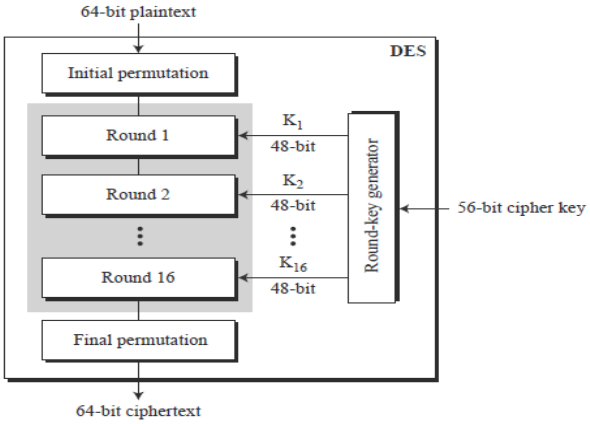

Fig. 3 General structure of DES

a. *Sub Bytes*: a non-linear substitution step where each byte is replaced with another according to a lookup table (S-box).
b. *Shift Rows*: a transposition step where each row of the state is shifted cyclically a certain number of times
c. *Mix Columns*: a mixing operation which operates on the columns of the state, combining the four bytes in each column.
d. *Add Round Key*: each byte of the state is combined with the round key; each round key is derived from the cipher key using a key schedule.

For the final round only three steps are performed: Sub Bytes, Shift Row and Add Round Key. Almost same steps are used in decryption, as in encryption, the order in which the steps are carried out is different.

B. Asymmetric Key Algorithms

The public key cryptography is a cryptography technique used two different keys, first one for encryption (public key) and the other one for decryption (private key). The public key known to everyone and private key only known by the owner. The public key cryptography has a very good system of verification, such that even a single character change will cause verification to fail. The Asymmetric encryption do not have key distribution problem but slow compare to the symmetric encryption because they use huge amount of power for their process [11]. Different asymmetric algorithms used like RAS, Diffie Hellman (DH), Elliptic Curve Cryptosystem (ECC), Digital Signature Algorithm (DSA) and El Gamal. The best algorithms in asymmetric are RSA and Diffie Hellman [11] [12].

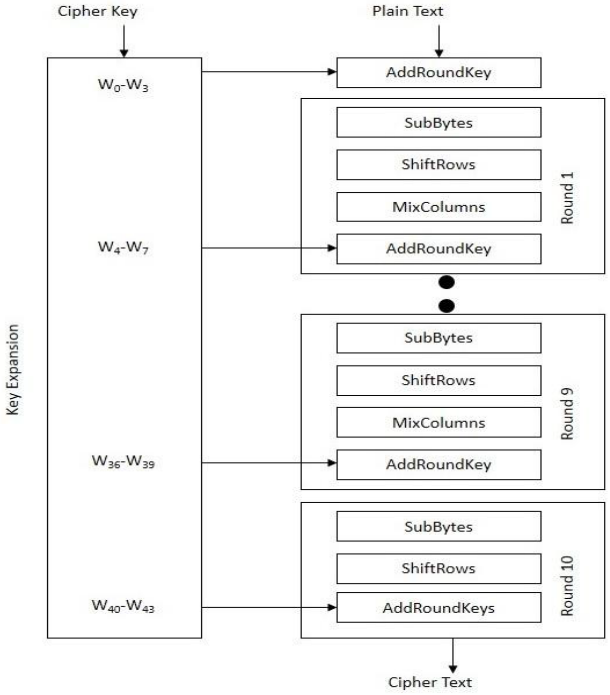

Fig. 4 AES Encryption flow [15].

1. RSA Algorithm

User data is encrypted first and then it is stored in the Cloud. When required, user places a request for the data for the Cloud provider; Cloud provider authenticates the user and delivers the data. RSA is a block cipher, in which every message is mapped to an integer. RSA consists of Public-Key and Private-Key. In our Cloud environment, Public-Key is known to all, whereas Private-Key is known only to the user who originally owns the data. Thus, encryption is done by the Cloud service provider and decryption is done by the Cloud user or consumer. Once the data is encrypted with the Public-Key, it can be decrypted with the corresponding Private-Key only.

Algorithm: [15]

a. SELECT two large prime number x and y.
b. Compute z=x*y the computed z is made public.
c. Now compute f(n)=(x-1)*(y-1).
d. Choose a random number 'e' as the public in the range 1<e<f(n) such that GCD(e,f(n))=1.
e. Find private key d such that $d=e^{-1} \bmod f(n)$, where d and f(n) are mutually prime.

Encryption:

a. Consider the user that needs to send x message to b in secured manner using rsa algorithm.
b. Now e is b's public key. Since e is public, a is allowed access to e.
c. For encryption the message m of a whitch is in the range 0<M<N< IS converted to cipher.
d. Where the cipher text $c=M^e$ mod n

Decryption:

a. Now the cipher text c is sent to b and a.
b. User b calculate the message with its private key β, where

IV. CLOUD SECURITY USING CRYPTOGRAPHY ALGORITHMS

Tim Mather *et al.,* discussed many algorithms in his book among which AES is not caring only about the security, even it also improving the performance of setting like hardware implementation. It is faster and stronger than DES. A performance evaluation reveals that going from 128 bits key to 192 bits key causes increase in power and time consumption by 8%- and 256-bits key causes an increase of 16% [10]. So for the use of industry-standard high grade, Advanced Encryption Standard (AES) symmetric encryption algorithm with key length of 128-bits is most preferable.

Gurpreet Singh *et al.,* did a study of survey on DES, 3DES, AES, RSA, Blowfish etc. According to the author, AES will have a key length of 128, 192 or 256 bits with corresponding number of rounds 10, 12 and 14 respectively. AES offers good security its high speed in comparison with DES, 3DES and RSA algorithms [17].

V. Biksham *et al.,* proposed high data security based on"somewhat" and "fully holomorphic" encryption methods. Cryptographic encryption algorithms provide high security to Cloud service providers (CSP) and cloud customers through. So, with minimal queries, data can access from the cloud servers through decryption. However, decryption of cipher text frequent may lead to the authenticationand integrity. Author developed holomorphic encryption to provide security to the encrypted data which enhance the performance of the cloud services [19].

Peidong Sha *et al.,* combined an RSA algorithm with pascal triangle theorem and inductive methods to proposed new encryption algorithm that meets homomorphic computation on cipher-texts. Thus proposed cryptography system satisfies homomorphic way of encryption in Cloud Computing [20].

Viney Pal Bansalv *et al.,* introduced a hybrid Cryptography system that combines RSA and Blowfish algorithm in which digital signature is necessary for customer authentication in cloud computing services. The proposed system utilizes the features of both asymmetric and symmetric cryptography. The FPGA device Virtex-4 is, used for implementation exploit Xilinx ISE 14.1 [21].

Adil Bouti *et al*., proposed algorithm to improve efficiency of utilization of cloud computing services that supports multiparty calculations by protecting its homomorphic properties. Author then exploited optimization blocks to efficient face recognition utilizing an Eigen face recognition algorithm [22].

In AES, the cipher and its inverse use different components which eliminate the likelihood for weak keys, which is an existing drawback of DES. The nonlinear characteristics of key generation eliminate the possibility of similar keys in AES. According to Sanchez-Avila, performance comparison amongst AES, DES and Triple DES shows that AES has a computer cost of the same order as required for Triple DES [13]. Another performance evaluation reveals that AES has an advantage over algorithms-3DES and DES in terms of execution time (in milliseconds) with different packet size and throughput (Megabyte/Sec) for encryption as well as decryption. RSA is the most widely used asymmetric encryption algorithm. When you encrypt with a private key, the cipher text can only have decrypted with the public key unlike symmetric key algorithms. The strength of RSA lies in that algorithm can be applicable for encryption/decryption, digital signature and for key exchange. Table I visualized the Features of DES, AES and RSA cryptography algorithms.

TABLE I FEATURES OF DES, AES AND RSA [17]

Parameters	DES	AES	RSA
Key Length	56	128, 192, or 256 bits	Depends on number of bits in the modulusn where n=p*q
Round(s)	16	10 -128 bit key,12 -192 bit key,14 -256 bit ke	1
Block Size	64bits	128 bits	variable
Cipher Type	Symmetric Block Cipher	Symmetric Block Cipher	Asymmetric Block Cipher
Speed	slow	Fast	Slowest
Security	Not good	Excellent	least

V. CONCLUSION

Cloud computing emerging in the recent years, but the main challenge is security. As cyber crimes and hacking step in to new developments, it becomes more and more cautious about data security. This challenge can meet to some extent with data encryption by the user before storing it in cloud. This paper discussed data security issue in the cloud and various cryptographic algorithms both symmetric and asymmetric key i.e., private and public key algorithm to restricts and to stop the attacks from malicious users.

REFERENCES

[1] K. Jeffery, and B. Neidecker-Lutz, "The Future of Cloud Computing Opportunities for European Cloud Computing Beyond 2010", *European Commission Information Society and Media,*. Nov. 2012.

[2] R. Barga, J. Bernabeu Auban, and D. Gannon, "Cloud computing architecture and application programming," *in Proc SIGACT News, 2009*, Vol. 40, No. 2, pp. 94-95.

[3] Shakeeba S. Khan, and R.R. Tuteja, "Security in Cloud Computing using Cryptographic Algorithms" *International Journal of Innovative Research in Computer and Communication Engineering*, Vol. 3, No.1, pp.1-7, 2015.

[4] Nia Ramadianti Putri, Medard Charles and M. Ganga, "Enhancing Information Security in Cloud Computing Services using SLA Based Metrics", *M. Eng. thesis, School of Computing Blekinge Institute of Technology, Computer Science, Sweden, March, 2011*.

[5] Neha Jain and Gurpreet Kaur, "Implementing DES Algorithm in Cloud for Data Security" *VSRD International Journal of Computer science and Information Technology*, Vol. 2, No.4, pp. 316-321, 2012.

[6] J.H. Allen, S. Barnum, and R.J. Ellison, "Software Security Engineering: A Guide for Project Managers", *Addison Wesley Professional, 2008*.

[7] SANS (2010) home page on SANS Information Security resources. [Online]. Available:
[Online] Available at: http://www.sans.org/informationsecurity.php

[8] COBIT 4.1(2007) home page on IG Institutions [Online] Available at: https://www.saca.org/knowledgecenter/cobit/documents /COBIT4 .pdf.

[9] Tim Mather, Subra Kumaraswamy, and Shahed Latif, "Cloud Security and Privacy", *O'Reilly, 2009*.

[10] Elminaam, DiaaSalama Abdul, Hatem Mohamed Abdul Kader, and Mohie Mohamed Hadhoud, "Performance Evaluation of Symmetric Encryption Algorithms", *International Journal of Computer Science and Network Security*, Vol. 8, No.12, pp. 280-286, 2008.

[11] Aman Kumar, Sudesh Jakhar, and Sunil Makka, "Comparative Analysis between DES and RSA Algorithms", *International Journal of Advanced Research in Computer Science and Software Engineering*, Vol.2, No.7, pp. 66-71, July 2012.

[12] William Stalling, "Cryptography and Network Security: Principles and Practice", *6th ed., Pearson Education, 2014*.

[13] C. Sanchez-Avila and R. Sanchez Reillol, "The Rijndael block cipher (AES proposal): a comparison with DES", *in Proc., 35th IEEE International Carnahan Conference on Security Technology*, pp.134-138, 2001

[14] Abha Sachdev, and Mohit Bhansali, "Enhancing Cloud Computing Security using AES Algorithm", *International Journal of Computer Applications*, Vol. 67, No.9, pp.87-92, 2013.

[15] P. Suresh, *et al.*, "Secure Cloud Environment Using RSA Algorithm", *International Research Journal of Engineering and Technology*, Vol.03, No.2, pp.144-148, 2016.

[16] William Stallings, "Cryptography and Network Security: Principles and Practice", *5th ed. Prentice Hall, 2011*.

[17] Gurpreet Singh, and Supriya, "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security", *International Journal of Computer Applications*, Vol. 67, No.19, pp. 33-38, 2013.

[18] N. Ziong, tropsoft home page on DES [Online] Available at: http://www.tropsoft.com/strongenc/des., 2014.

[19] V. Biksham, and D. Vasumathi, "Query based computations on encrypted data through homomorphic encryption in CC security", *in Proc. IEEE International Conference on Electrical, Electronics, and Optimization Techniques*, pp. 34-37, 2016.

[20] Peidong Sha, and Zhixiang Zhu, "The Modification Of RSA Algorithm To Adapt Fully Homomorphic Encryption Algorithm In CC", *in Proc. IEEE International Conference on Cloud Computing and Intelligence Systems*, pp. 123-126, 2016.

[21] Viney Pal Bansal, and Sandeep Singh, "A Hybrid Data Encryption Technique using RSA and Blowfish for CC on FPGAs", *in Proc. IEEE International Conference on Recent Advances in Engineering & Computational Sciences*, pp. 57-60, 2015.