A Survey: Exhaustive Study of Data Security Algorithms in Cloud Computing

[1]Shivam Gupta
DDIPG, PG Scholar

[2]Prof. Uday Chourasia
Assistant Professor

[3]Prof. Rajeev Pandey
Assistant Professor

[123]Department of Computer Science and Engineering, UIT-RGPV, Bhopal-462036, India

Abstract- Since a huge amount of data is being generated everyday on the internet and stored in cloud. Because of which information security is a biggest challenge. In order to provide data confidentiality to the user, cryptographic algorithms can be used. If we talk about reality, every user needs such an algorithm which is low cost and high performance. So in order to find such algorithm, an analysis is done so that we can gather some valuable information insights. This paper aims to study different papers based on cryptography and gathering information about widely used specific algorithms and also about all previous works and studies that has been done related to cryptography. This paper also compares all these papers to gather the best results so as to get the most suitable algorithm in cloud computing.

I. INTRODUCTION

The basic elements we have studied so far in cryptography moves around plain text and cipher text [1].Here Plain Text is that specific text that sender wants to send whereas Cipher Text is an encrypted form of the plain text. This plain form of text is converted using encryption algorithms into encrypted form, called as cipher text and this ciphered text gets converted into the plain form of text with the use of decryption algorithms.

These algorithms are classified into two types:

1. Secret or Symmetric Key Algorithm.
2. Public or Asymmetric Key Algorithm.

Symmetric Key Algorithm- These are also called as Secret Key Algorithm, where the sender and the receiver share a common key for encryption and decryption. This secret key should be secured by both sender and receiver. 3DES, AES, DES and Blowfish are some of the types of symmetric key algorithms [1].

a. Data Encryption Standard (DES):

This algorithm was developed by IBM (1977).

Key Length – 56 bits

Block Size – 64 bits

This Algorithm consists of a fiestal network which divides a block into two equal halves where the right half passes through a chain of S-Boxes and P-Boxes. After passing through this, cipher text is obtained by XOR operation [2].

Number of Rounds in DES- 19

DES is vulnerable to Brute Force Attacks. So later M-DES was proposed to improve Bit Error Rate (BER) which is used to occur due to avalanche effect. But M-DES is also vulnerable to some attacks like Man in Middle Attack.

b. 3DES:

3DES algorithm was introduced by IBM in 1978 in order to improve security.

Key Length- 56 bits

Block Size- 64 bits

3DES is same as DES but here each data block is undergone execution of algorithm three times on it. Just like DES, 3DES also vulnerable to Brute Force Attacks but comparatively 3DES is more secure than DES.

c. Advanced Encryption Standard (AES) :

National Institute of Standard and Technology, NIST developed AES.

Block Size- 128bits, 192bits and 256bits

Depending on the block sizes, AES-128, AES-192 and AES-256 uses 10 rounds, 12 rounds and 14 rounds respectively. These rounds, we talked about, consist of steps like substitution accompanied by functions like mixed columns, rows shift and round key addition.

AES is comparatively more secured than previously discussed ones. AES is known to have a strong avalanche effect.

AES algorithm is vulnerable to a combination of rectangle and boomerang attack with related key-differential but this attack can't break complete AES.

d. Blowfish :

Bruce Schneier developed blowfish encryption algorithm in 1993.

Key Length- Variable maximum up to 448 bits [2].

Block Size – 64 bits

Blowfish is executed in two phases, first is Key Expansion phase and second is Encryption phase. In key expansion phase, conversion of 448bit key into number of sub keys takes place, totalling 4168bytes whereas in encryption phase, 16 times iteration of a function takes place and then using XOR operations, the cipher text is obtained [1].

Password management systems are also based on Blowfish Algorithm.

Asymmetric Key Algorithms- These algorithms basically constitutes two types of keys, they are public and private key. So here for encryption, algorithm uses public key and meanwhile for decryption, it uses a private key. RSA is one such Asymmetric key algorithm [1].

a. Rivest Shamir Adlemen (RSA) :

Rivest, Shamir and Adlemen developed RSA in 1977.

RSA is an asymmetric algorithm, where sender's message gets encrypted with the use of a public key and at the receiver end the message gets decrypted by the private key.

RSA consist of some mathematical operations through which encryption and decryption keys are calculated that is E and D respectively.

Cipher text is calculated by formula: $C = M^E \bmod (n)$

Similarly Plain text is calculated by formula: $P = M^D \bmod (n)$, where n is product of prime numbers.

Later it was found that there can be weak keys too in RSA so a new concept of digital signature was introduced along with RSA algorithm.

II. LITERATURE SURVEY

.

In [1], both symmetric and asymmetric algorithms are analysed at different attributes like key length, block size, number of rounds, power consumption, avalanche effect, processing time and resource consumption. Here analysis is done based on parameters like encryption time, decryption time, and memory consumption and avalanche effect.

In [2], a concept of multi-cloud is discussed which is also called as inter clouds (cloud of clouds) in order to enable storage of data on multiple clouds so as to enhance security. So here data encoding technique ensures encryption of client's data and then splitting ensures the data is split into three different cloud servers. In this paper author described the proposed multi-cloud architecture along with the description of different algorithms in cloud.

Cloud Computing, its benefits, and challenges along with data storage and data security issues are discussed in [3]. Types of existing algorithms for security are also being discussed and comparative analysis of these algorithms is done in [3].

In [4], there is a talk about cloud computing's security concerns and challenges prevailing in cloud computing. Problem formulation is done according to different security concerns, kept in mind.

In Paper [5] security issues are being categorised for cloud computing, mainly focussed on SPI model (SaaS, PaaS, IaaS), in order to identify the most important threats to cloud computing. Along with this, vulnerabilities are also been discussed which allows an attack to be successful, and later the relationship between these threats and vulnerabilities are described in the paper.

[6] Discusses the effectiveness of each algorithm and later comparison table is being formulated after analysing each algorithm based on different factors.

In [7] there is a detailed description of different algorithms and their working mechanism, later they were analysed on different parameters so as to find a suitable algorithm to be used in cloud computing

III. SURVEY

Several studies have been done on different cryptographic algorithms. Several papers have been published studying the comparison of different algorithms based on several factors in order to find a suitable one.

AUTHOR	TYPE	TITLE	OBJECTIVE
Pradeep Semwal and MK Sharma (2017)	Thesis	"Comparative study of different cryptographic algorithms for data security in cloud computing"	Performance of cryptographic algorithms is analysed based on different factors.
Karan Kundar, Theres Bemila, Lokesh Jain, Nayan Makasare, Shashikant Sharma (2016)	Thesis	"Comparative study of various security algorithms applicable n-Multi-Cloud Environment"	Concept of Multi-Cloud is discussed to ensure data security, along with analysis of different algorithms used in cloud.
Supriya Kinger; Randeep Kaur (2014)	Thesis	"Analysis of Security algorithms in cloud computing"	Cloud benefits along with challenges related to cloud are being discussed and later analysis of algorithms is done.
Anshu Parashar; Rachna Arora (2013)	Thesis	"Secure-User data in cloud computing using encryption algorithm"	Security concerns and challenges have been discussed related to cloud computing and problem is formulated based on these concerns
David G Rosado; Keiko Hashizume; Eduardo B Fernandez; Eduardo Fernandez-Medina (2013)	Thesis	"An analysis of security issues for cloud computing"	Security issues are being categorised for cloud computing, and relation between vulnerabilities and threats is discussed.
Abhishek Sachdeva; Dr. Prerna Mahajan (2013)	Thesis	"A study of Encryption algorithms AES, DES, and RSA for security"	Discusses the effectiveness of each algorithm and later comparison table is being formulated after analysing each algorithm based on different factors.

Supriya; Gurpeet Singh (2013)	Thesis	"A study of Encryption Algorithms for information Security"	There is a detailed description of different algorithms and their working mechanism, later they were analysed on different parameters so as to find a suitable algorithm to be used in cloud computing.

IV. CONCLUSION

We studied basic concepts of Cloud Computing, its benefits, challenges, along with the security concerns attached to it. We studied the types of cryptographic algorithms, that is Asymmetric and Symmetric algorithms. Different cryptographic algorithms are later analysed based on different factors in order to find out the best suitable algorithm for data security in cloud computing. Based on processing time, we studied that blowfish showed a good performance than other algorithms and based on the studies, AES was found better than DES and 3DES as it took less time in encryption and decryption. We also studied through several papers that Blowfish has a maximum avalanche effect due to the number of XOR operations involved in it. According to studies, it was found that DES has lower avalanche effect than AES. We also studied that different algorithms are vulnerable to cryptanalysis attacks, like we studied DES is vulnerable to linear and differential cryptanalysis whereas 3DES, Blowfish are vulnerable to brute force attacks. As per studies, it was found that DES is the most insecure algorithm.

Thus, Encryption and Decryption time, usage of memory and avalanche effect can be the basis of comparison of both the asymmetric and symmetric algorithms.

V. REFERENCE

[1] Pradeep Semwal; MK Sharma, "Comparative Study of Different Cryptographic Algorithms for Data Security in Cloud Computing", International-Journal on Emerging Technologies (Special Issue NCETST-2017)

[2] Theres Bemila; Karan Kundar; Lokesh Jain; Shashikant Sharma; Nayan Makasare, "Comparative study of various Security-Algorithms applicable in Multi-Cloud Environment", International-Journal of Advanced Research in Computer and Communication Engineering, Vol.5, Issue-3, 2016

[3] Supriya Kinger; Randeep Kaur "Analysis of Security Algorithms in Cloud Computing", IJAIEM, Vol. 3, Issue 3, March 2014

[4] Anshu Parashar; Rachna Arora"Secure User Data in Cloud Computing Using Encryption Algorithms", (IJERA), Volume 3 Issue 4, Jul-Aug 2013, pp.1922-1926

[5] David G Rosado; Keiko Hashizume; Eduardo B Fernandez; Eduardo Fernandez-Medina "An Analysis of Security Issues for Cloud Computing", Journal of Internet Services and Applications, 2013

[6] Abhishek Sachdeva; Dr. Prerna Mahajan "A Study of Encryption Algorithms AES, DES and RSA for Security", Global Journal of Computer Science and Technology Network, Web and Security, Volume 13, Issue 15, Year 2013

[7] Supriya; Gurpeet Singh "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security", International Journal for Computer Applications (0975-8887), Volume 67-No.19, April 2013