Comparison between RSA and Triple DES in Cloud Environment

Navrang Pal Kaur
Department of Computer Science
Punjabi University, Patiala
boparainova@gmail.com

***Abstract*— The goal of the paper is to discuss comparisons in RSA and Triple DES algorithms in cloud environment. There are concerned three aspects on which we will compare algorithms: (i) Avalanche Effect: - small changes in plaintext or key will change the cipher text is known as advance effect. Either change in on bit of plaintext or key will change no. bits of output value. (ii)Memory required: - Different algorithms required different memory space to perform the operation. The memory space required by any algorithm is determined on the basis of data size, no. of rounds etc. From different algorithm an algorithm is consider best which use small memory and perform best task. (iii) Simulation time: - The time required consumed by algorithm to complete the operation is known as simulation time. It depends on processor speed, algorithm complexity. Small simulation time is desirable requirement. There is considered implementation of cryptographic algorithms in cloud environment by using software libraries and simulators. Finally, there are discussed some possibilities to maximize the speed of execution of cryptographic algorithms, emphasize the importance of parallelization of algorithms.**

Index Terms — *Cloud computing, RSA, triple data encryption standard, cryptography, avalanche effect.*

*****

I. INTRODUCTION

Cloud computing delivers infrastructure, platform, and software that are made available as subscription-based services in a pay-as-you-go model to consumers. These services are referred to as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) in industries. [1]

Today communication is an important aspect in people’s life. In this situation, cryptography – a study and practice of protecting information – is often used. The goal of this paper is to discuss comparisons of RSA and Triple DES algorithms in cloud environment, emphasizing possible improvements and vulnerabilities in implementation of cryptographic algorithms, usage of cryptographic frameworks and libraries, as well as the speed of execution of implemented cryptographic algorithms.

At the beginning of the paper, there is given a brief overview of cloud computing, data security. Further in the paper, RSA and Triple DES is introduced. There is also simulation of two algorithms in cloud environment by using cloud simulator. There are software frameworks which provide cryptographic functionality are compared with each other by the speed of execution of algorithms. The goal of this comparison is to construct some guidelines which help select a feasible solution for implementing a cryptographic functionality in software. Finally, there are discussed some general possibilities of maximizing the speed of execution of cryptographic algorithms. Results concerning the speed of execution of implemented cryptographic algorithms are based on practical experiments – by the authors, there were written and utilized computer programs (in Java programming language) for measuring the time of running specific cryptographic algorithms implemented in software frameworks/libraries (Java Platform Standard Edition, Eclipse Juno). The methodology used for measuring the speed of execution of cryptographic algorithms is discussed further in this paper. [2]

Triple DES: - It was enhancement of DES. And used to remove the mid-in-the-middle attack occurred in 2-DES. In this 3 times iterations of DES encryption on each block is performed. In 3-DES the 3-times iteration is applied to increase the encryption level and average time. Common method of 3-DES is Minus Encrypt-Decrypt-Encrypt (-EDE). Each iteration of 3-DES using –EDE will encrypt a block using a 56-bit key. After encryption use a different 56-bit key to decrypt the block. On the last pass, a 56-bit key is used to encrypt the data again. This is equivalent to using a 168-bit encryption key.

RSA: - This is public key encryption algorithm developed byRon Rivest, Adi Shamir and Len Adlemen in 1977. It is most popular and a symmetric key cryptographic algorithm. It may used to provide both secrecy and digital signat ure. It uses the prime number to generate the public and private key based on mathematical fact and multipl ying large numbers together. It uses the block size data in which plaintext and cipher text are integers between 0 and n1 for some n values. Size of n is consired 1024 bits. In this two different keys are used for encryption and decryption purpose. As sender knows encryption key and receiver knows decryption key.[3]

For triple-DES, the plaintext is split into many blocks and the algorithm operates on the successive 64 bit blocks of plaintext. The key length of triple-DES is 192-bit, given a plaintext P and three encryption keys K1, K2 and K3 and is defined as follows [4]:

C = EK3 [DK2 [EK1 [P]]]

The generated plaintext does the following five functions:

a) an initial permutation (IP);
b) a complex function labeled fk, which involves both permutation and substitution operations and depends on a key input;
c) a simple permutation function that switches (SW) the two halves of the data;

d) the function fk again,

e) And finally a permutation function that is the inverse of the initial permutation (IP-1).

While for RSA algorithm, the processed plaintext is also encrypted in blocks. The binary value of each block should be less than some number n. That is, the block size must be less than or equal to log2 (n); let the block size is 2k bits, where $2k < n \leqq 2k + 1$, here n=12 byte. Encryption and decryption are of the following form, M= plaintext block and C= cipher text block:

$C = M^e \bmod n.$

$M = C^d \bmod n = (M^e)^d \bmod n = M^{ed} \bmod n.$

II. RELATED WORK

Eman M.Mohamed et al. [5] proposed that Amazon EC2 provider must use AES to ensure the most security in user data. They gave three advices to the Amazon EC2 cloud user, the first when you are not interested in higher security of the data and are interested about the performance of the algorithm then blowfish, DES or AES are used. The second advice is that when you are interested in higher security of the data then AES is used which is the highest security algorithm. Finally the third advice, AES is suitable to Amazon EC2 which it is the most secured and also takes less time to encrypt.

ENISA [6] investigated the different security risks related to adopting cloud computing along with the affected assets, the risks likelihood, impacts, and vulnerabilities in cloud computing that may lead to such risks.

Balachandra et al [7] discussed the security SLA’s specifications and objectives related to data locations, segregation and data recovery.

Kresimir et al (2010) [8] discussed high level security cloud computing model such as data integrity, payment, and privacy of sensitive information. Kresimir discussed different security management standards such as ITIL, ISO/IEC 27001 and Open Virtualization Format (OVF).

Mladen A. Vouk [9] in their paper discusses the concept of cloud computing, the issues it tries to address, related research topics, and a “cloud” implementation based on VCL technology. The experience with VCL technology is excellent and the work on additional functionalities and features that will make it even more suitable is carried out for cloud framework construction.

Mehmet Kuzu et al. (2012) [10] proposed an efficient similarity searchable symmetric encryption scheme. For this, they utilized locality sensitive hashing which is widely used for fast similarity search in high dimensional spaces for plain data. They proposed LSH based secure index and a search scheme to enable fast similarity search in the context of encrypted data.

Ooi Beng Chin (2009) [11] suggested that Cloud Computing is changing a large part of the IT industry. Cloud Computing is turning into reality a dream that has long been cherished by the IT industry by delivering to users "infinite" computing resources in a pay-as- you-go manner. Building a scalable data management system on existing commercial Cloud platforms, such as Amazon EC2, poses a grand challenge.

RAN Shuanglin (2012) [12] suggested that the contents of data security are more extensive in the cloud. This security policy designed the data in the cloud computing just to solve the client's own data security protection. Once the data is stored into the public cloud, the protection of its data security will be more complex both from a technical and management. It is believed that the proposed "technology + management" Safety management philosophy which will be an important direction to address the cloud computing security issues in the future.

Uma Somani et al. (2010) [13], in their paper, had tried to assess Cloud Storage Methodology and Data Security in cloud by the implementation of digital signature with RSA algorithm. The proposed algorithm for implementing Digital Signature with RSA Algorithm is carried out using the following steps: a. Key Generation Algorithm b. Digital signing, c. Encryption, d. Decryption, and e. Signature verification

Zhang Xin (2012) [14] talked about data safety model in cloud computing. Firstly, it summarizes the cloud computing data application mode and gives data application system model in cloud computing system. Secondly, it evaluates the basic safety of cloud computing data platform. At last it gives cloud computing data application system model.

According to The Economist Ludwig Siegele in a 2008 article [15], it will have huge impacts on the information technology industry, and also profoundly change the way people use computers.

III. COMPARISON RESULTS

Comparison of secret key and public key based 3-DES and RSA algorithms is done. RSA solves the trouble of the key agreement and key exchange problem generated in secret key cryptography .But it does not solve the entire security infrastructure. So 3-DES is used. RSA and 3-DES differ from each other in certain features. In decryption 3-DES is better than all other algorithms in throughput and power consumption.

Features	**3-DES**	**RSA**
Key used for encryption and decryption	Same keys are used	Different keys are used
Scalability	Scalable (due to varying key size and block size)	No scalability
Avalanche effect	Not effected	Effected
Power consumption	Low	High
Throughput	High	Low
Confidentiality	High	Low

Table 3: Comparison between 3-DES and RSA algorithms.

IV. CONCLUSIONS

The selected algorithms 3-DES and RSA are discussed in cloud environment. As 3-DES is secret key based algorithm suffers from key distribution and key agreement problems .But RSA consumes huge quantity of time to achieve encryption and decryption process. Comparison result showed that 3-DES has better performance than RSA. From the Comparison results, I evaluated that throughput of 3-DES algorithm is much better than the throughput of RSA algorithm.

V. REFERENCES

[1] Armbrust M, Fox A, Griffith R, Joseph A, Katz R, Konwinski A, Lee G, Patterson D, Rabkin A, Stoica I, Zaharia M. “A view of cloud computing”, Communications of the ACM 2010.

[2] Vladislav Nazaruk, Pavel Rusakov,” Implementation of Cryptographic Algorithms in Software: An Analysis of the Effectiveness” Scientific Journal of Riga Technical University Computer Science. Applied Computer Systems, 2010, Volume 43.

[3] Atul Kahte”Cryptography and Network Security, 2nd Ed”.

[4] Yan Wang, Ming Hu , ” Timing evaluation of the known cryptographic algorithms”, College of Computer Science Wuhan University of Science and Engineering, 2009 International Conference on Computational Intelligence and Security

[5] Eman M.Mohamed, Hatem S. Abdelkader , Sherif EI-Etriby “Enhanced Data Security Model for Cloud Computing”, The 8th International Conference on Informatics and Systems (INFOS2012) - 14-16 May Cloud and Mobile Computing Track

[6] ENISA, "Cloud computing: benefits, risks and recommendations for information security," 2009,http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment, Accessed On July 2010.

[7] Balachandra Reddy Kandukuri, Ramakrishna Paturi and Atanu Rakshit, "Cloud Security Issues," in Proceedings of the 2009 IEEE International Conference on Services Computing, 2009.

[8] Kresimir Popovic , Zeljko Hocenski, "Cloud computing security issues and challenges," in The Third International Conference on Advances in Human-oriented and Personalized Mechanisms, Technologies, and Services, 2010.

[9] Mladen A. Vouk “Cloud Computing – Issues Research and Implementations”, Journal of Computing and Information Technology - CIT 16, 2008.

[10] Mehmet Kuzu, Mohammad Saiful Islam, Murat Kantarcioglu, “Efficient Similarity Search over Encrypted Data”, Department of Computer Science, The University of Texas at Dallas Richardson, TX 75080, USA, 2012 IEEE 28th International Conference on Data Engineering.

[11] Ooi Beng Chin, “Cloud Data Management Systems: Opportunities and Challenges”, 2009 Fifth International Conference on Semantics, Knowledge and Grid @2009 IEEE

[12] RAN Shuanglin, “Data Security Policy In The Cloud Computing”, Digital Media Department of Communication School, Guizhou University for Nationalities, Guiyang, China, The 7th International Conference on Computer Science & Education (ICCSE 2012) July 14-17, 2012. Melbourne, Australia, @ 2012 IEEE

[13] Uma Somani, Kanika Lakhani, Manish Mundra, “Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing”, 2010 1st International Conference on Parallel, Distributed and Grid Computing (PDGC - 2010), @2010 IEEE

[14] Zhang Xin, Lai Song-qing, Liu Nai-wen , “Research on Cloud Computing Data Security Model Based on Multi-dimension” , International Symposium On Information Technology In Medicine And Education, @2012 IEEE

[15] L. SIEGELE, Let it rise: A survey of corporate IT.The Economist, (Oct., 2008).