

Introduction to CryptoCloud in Cloud Computing

Er. Sharanjit Singh, Er. Rasneet Kaur Chauhan
Department of CSE

Guru Nanak Dev University RC Gurdaspur, Punjab, INDIA

Abstract: Cloud Computing is evolving very fast. It can be considered as next generation architecture for computing. Thus cloud computing is combination of numerous computing resources that are accessible via internet. The technological advancements in performance of a processor, its virtualization, and the fast and reliable network connectivity are all positive factors for businesses and organizations for adopting the cloud computing model. This cloud computing model also makes an economic sense for a number of organizations because it allows a rapid application development and the deployment is done by utilizing tools and platforms that are already there in-place, wholly tested, and proven to be fully functional. However, the rapid growth of the cloud computing market has also raised many serious concerns regarding data security and data governance, and these are considered to be the major barriers to broader adoption of cloud computing.

Keywords: Cloud Computing; Security; Service Models; Components.

I. INTRODUCTION

Cloud Computing is the name given to the recent trend in computing service provision. This trend has seen the technological and cultural shift of computing service provision from being provided locally to being provided remotely and en masse, by third-party service providers. Cloud Computing is a used to describe both type of application and platform. As a platform it supplies, configures and reconfigures servers and resources. The servers can be virtual machines or physical machines. On the other side, it describes applications that could be extended to be accessible through internet and thus for this purpose, powerful servers and data centers are used to host the web services and web applications. From time to time, great innovations are done without any wholly new discoveries and technological breakthroughs. Electric vehicles are a nothing but a combination of existing auto body frames with electric motor technologies. The Internet is also networked computer devices with the resources on a global scale. Thus, it is about how the existing and mature technologies and new knowledge is mixed this is how advanced, valuable and innovative products and services are introduces into our life. In the same way, cloud computing is also nothing but a new model of information delivery that utilizes both existing technologies and resources available. Cloud Computing has thus became one of the most discussed and talked about technologies in the recent times and has thus got a lot of attention from organizations, media as well as analysts because of a large number of opportunities it is offering to all. Many companies have invested in Cloud Computing by building their own public clouds, such as Google, Amazon and Microsoft. These companies often release new features and various updates of their services. For instance Amazon Web Services (AWS) released a Security2 and Economics3 center on their website so as to address and give community and academic advice regarding these issues. Thus, there are still a lot of doubts about the security for enterprises and organizations to adopt Cloud Computing. Hence, the issues of security and risks in Cloud Computing for enterprises and organizations must be researched and various solutions for those problems should be applied.

II. CRYPTOGRAPHY OVERVIEW

The major issue in adopting the cloud is its security. The data that is stored in the cloud get increasing day by day and thus we need some kind of mechanisms to make sure that the data is stored in a secured manner without any illegal unauthorized access. Security for data that is stored in the cloud is an important issue. Also providing integrity to data that is distributed over cloud has also been a challenging one. The main solution to deal with this type of difficult situation is make use of the cryptographic methods in cloud. Thus, we will describe several different cryptographic techniques that are used to protect the data that is used in the cloud and thus prevent data and information from being leaked and also to ensure that the privacy has been maintained. These cryptographic methods are used to provide the security for the Confidentiality as its main characteristics.

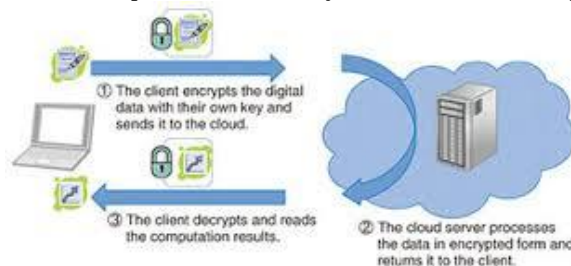


Fig. 1. Cryptography

III. CRYPTOGRAPHIC ALGORITHMS

- **Data Encryption Standard (DES)**

The Data Encryption Standard (DES) is a symmetric key block cipher. At the encryption side, DES takes a 64-bit plaintext and in return creates a 64-bit ciphertext, at the decryption side it takes the 64-bit ciphertext and in return creates a 64-bit plaintext, and the same 56 bit cipher key is used for both encryption process and decryption process. This encryption process is thus made of two permutations i.e. P-boxes, which are also called as initial and final permutation, and the sixteen Feistel rounds

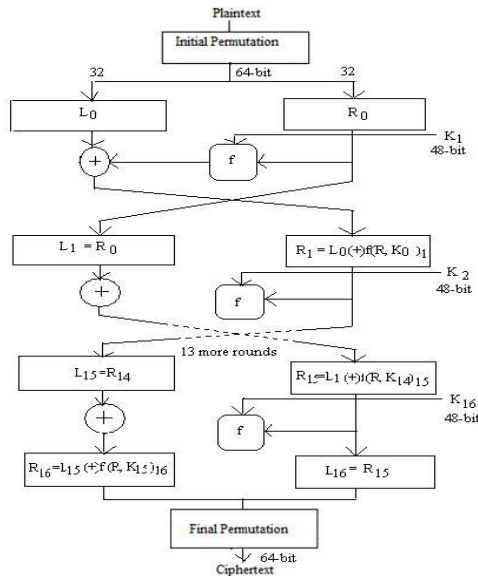


Fig. 2. Encryption with DES

- **Advanced Encryption Standard (AES)**

Advanced Encryption Standard is a symmetric key block cipher technique that was published as FIPS-197 in Federal Register in December 2001 by National Institute of Standards and Technology (NIST). This is a non-Feistel cipher. It encrypts the data with a block size of 128-bits. It makes use of 10, 12, or fourteen rounds. Hence depending on number of rounds, the key size could be 128, 192, or 256 bits as shown in figure. It operates on 4×4 column major order matrix of bytes also known as the state.

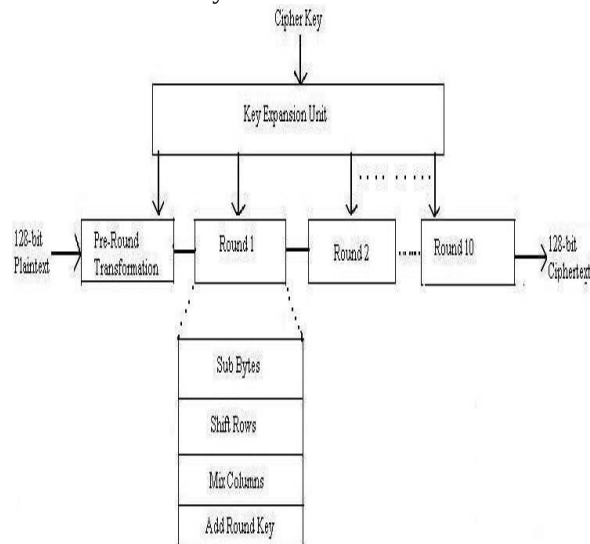


Fig. 3. Encryption with AES

- **Triple-DES**

An easy way of increasing the key size of DES is by using Triple DES so as to guard it against the attacks without designing a completely new block cipher algorithm. It is thus an enhancement version of DES. It is used to remove the man-in-the-middle attack occurred in 2-DES. In this, triple iteration of DES encryption on each and every block is done. In 3-DES the triple iteration is done to increase the encryption level and also average time. Common method of 3-DES is the Minus Encrypt-Decrypt-Encrypt (-EDE).

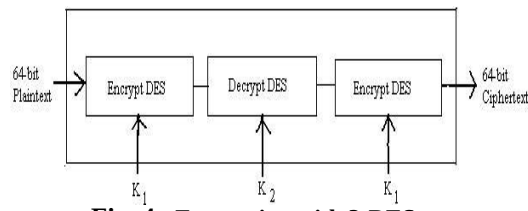


Fig. 4. Encryption with 3-DES

- **RSA**

RSA is a public key algorithm that is based on the difficulty of prime factorization. Similar to most of the public key password features, RSA password is also block encrypted, but is different from other block encryption which are used in a secret key algorithm like DES (Data Encryption Standard) in the way that the length of the plain text and a key is a variable; hence in other words, a relatively long length of the key can also be used for considering of a secure and a reliable system, and also a relatively short length of the key that is used for an efficient system.

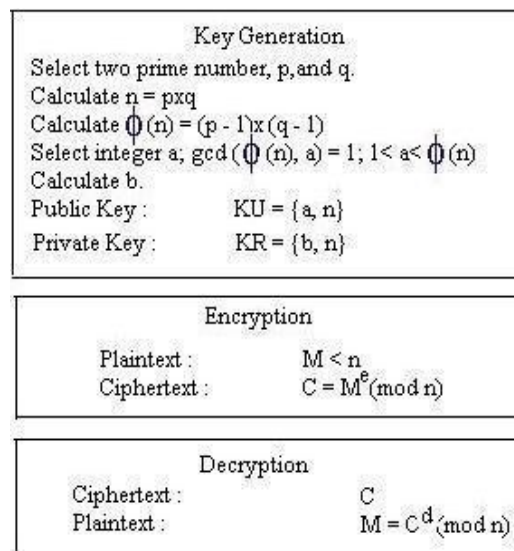


Fig. 5. Encryption with RSA

- **Blowfish**

It makes use of a block cipher of 64-bit block. It uses a key of variable length which ranges from 32 bits to 448 bits. It is one of the public domain encryption algorithms. Blowfish algorithm was designed by Bruce Schneider in 1993 as a fast alternative to the existing encryption algorithms. Blowfish has around 16 rounds or less. Blowfish is a highly secure cipher and uses encryption that is free of patents and copyrights. No attack is yet successful against Blowfish, though it suffers from the weak keys problem.

It has a 16-round Feistel cipher and makes use of a large key-dependent S-boxes. Its structure resembles the CAST-128, which makes use of fixed S-boxes. Each line thus represents 32 bits. The algorithm thus keeps two sub key arrays i.e. a 18-entry P-array and four 256-entry S-boxes. The S-boxes thus accepts 8-bit input and hence produce 32-bit output. One entry of a P-array uses every round, and then after the final round, and each half of a data block is XOR-ed with any one remaining unused P-entry.

IV. PERFORMANCE ANALYSISPARAMETERS

The data will be encrypted using the cryptographic algorithms such as, AES, DES, RSA, Blowfish and 3-DES. By using these algorithms, the speed-up ratio and the mean processing time for different inputs is calculated.

- **Files of different Data types**

In this it is checked if the encryption has any dependency on the type of data. Different data type files like image, textual, audio and video of nearly 50MB in size are chosen and the encryption time of different cipher algorithms is thus calculated for these data types. The key size of AES, DES, 3-DES, RSA, Blowfish are kept at minimum values as 128, 56, 112, 1024, 32 bits respectively. Block cipher mode used is ECB. Figure shows the execution time of the algorithms for different data type files.

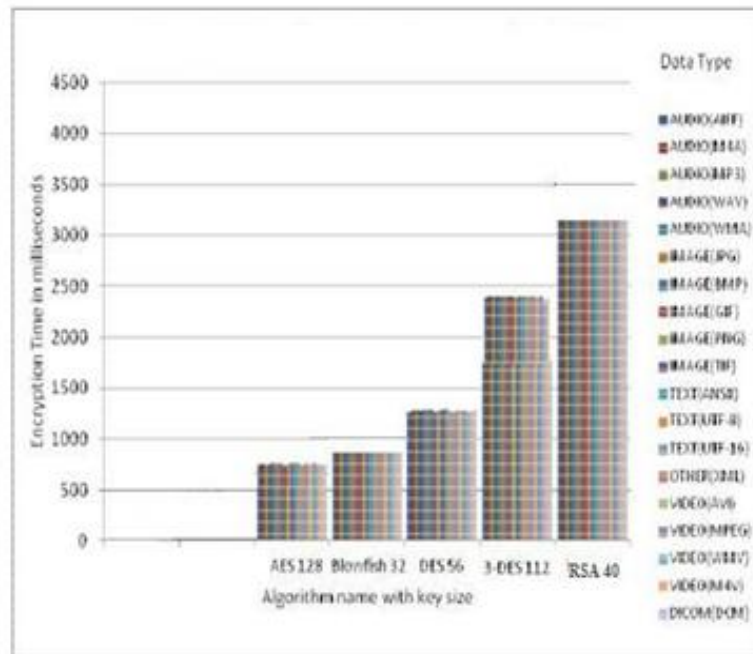


Fig. 6. Encryption time Vs Cipher Algorithm for files of different data type

It is clear that encryption time for all the data type is almost same. It shows that the encryption time does not change according to the type of the data. Encryption only depends on the number of bytes in the file and hence not on the type of file.

- **File of different data densities**

Here it is checked if encryption depends on the data density or not. Encryption rate is hence evaluated for two different data density file i.e. a sparse file and a dense file. For a cipher algorithm, key size and block mode are kept at bare minimal parameters. The results of execution are shown below:

Algorithm Name	Dense (62398454 Bytes)		Sparse (7308128 Bytes)	
	Encrypt Time(ms)	Encryption Rate(MB/s)	Encrypt Time(ms)	Encryption Rate(MB/s)
AES 128	534	105.62	634	107.64
DES 56	1530	39.84	1803	37.64
3-DES 112	4368	16.52	5078	16.53
RSA 1024	5289	7.69	7511	6.73
Blowfish 128	721	82.79	853	82.69

Table 1. Execution rate for sparse and dense data file

It shows that the encryption time is not affected by the data density in a file. The variation in time with respect to these different algorithms thus follows the same pattern for both dense and sparse files. Hence the encryption rate for particular cipher algorithm remains the same, though the file is dense or sparse. It depends only on the number of bytes present in the file.

- **Encryption Algorithms having different key sizes**

It is to analyze the effect of changing the size of encryption key on encryption time. BMP file of 50MB is taken and different cipher algorithms are executed for different size. Figure shows the result of execution for key size variation.

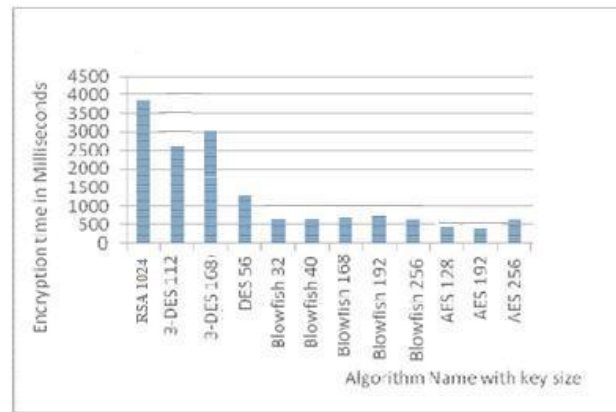


Fig. 7. Variation of key sizes for different cipher Algorithms

The execution results show that these ciphers algorithms, the encryption time changes with the change in the key size. Encryption time thus increases with the increase in the key size for block ciphers. The time variation is very small.

V. CONCLUSION

Due to the nature of the technology and architecture it is based on, cloud computing does require some preventative measures and a broader security perimeter compared to the traditional and on-premise application and data hosting. Moreover cloud computing, if properly planned and deployed, will also bring positive functional, economic, and for some organizations some additional security benefits too. The most favorable outcome is being the primary driving force due to the recent economic fallout is forcing the organizations to seek more cost effective solutions. Hence this trend of favoring cost-saving solutions is likely to continue at a rate much more consistent with the growth of cloud adoption. Different kind of cloud computing security issues are discussed here that exploit the security system. Hence, the notion of data privacy is addressed which is impossible to maintain without the security and the degree of trust afforded to a cloud service provider is being analyzed. Thus it is required for a cloud service provider to secure a data transmission at specific cloud data centers. The level of concern is likely to remain high, as the world will continue to observe some occasional cloud security incidents, and non-cloud breaches and hacker attacks. For some organizations, however, high security concerns affect the decision makers in a positive and constructive manner, rather than being a show stopper, as they would take more and more precautions and preventative measures to mitigate these risks

REFERENCES

- [1] Xing Zhou, Xiaofei Tang 2011, Research and Implementation of RSA Algorithm for Encryption and Decryption, Department of Computer Science and Technology Harbin, china.
- [2] Jansen, Wayne &Grance, Timothy. *Guidelines on Security and Privacy in Public Cloud Computing*. National Institute of Standards and Technology, 2011.
- [3] M.Shand and J.Vuillemin, "Fast Implementation of RSA Cryptography", Proc. 11th IEEE Symp. Computer Arithmetic, E.E.Swartzlander, M.J.
- [4] Liu, P. You, Y. Peng, "Security Issues and Solutions in Cloud Computing", IEEE-computer society, 2012.
- [5] R. Padhy, M. Patra and S. Satapathy, "Cloud Computing: Security Issues and Research Challenges", IJCSITS, Vol. 1, No. 2, December 2011.
- [6] M.Wallischek, B.Grobauer, E.Stöcker, "Understanding of Cloud Computing Vulnerabilities", IEEE Computer and Reliability Society, 2011.
- [7] S. Hariri, Y. Al - Nashif, "Resilient Cloud Data Storage", ACM-NSF Center for Cloud and Autonomic Computing, 2013
- [8] William Stallings, A Handbook on "Cryptography and network Security" by Pearson Education, 2009
- [9] A. Jaber, M. Fadlil, "The Use of Cryptography in Cloud environment", IEEE International Conference and Computing and Engineering, December 2013.
- [10] D.Rajesh Kumar, R. Gupta, Tanisha, "File Security in Cloud using Two-tier Encryption and Decryption", IJARCSSA, vol.3, issue 7, July 2013.