A Survey for Comparative Analysis of various Cryptographic Algorithms used to Secure Data on Cloud

Binita Thakkar¹,
School of Computer and Systems Sciences
Research Scholar¹,
Jaipur National University
Jaipur, Rajasthan, India.

Dr. Blessy Thankachan²
School of Computer and Systems Sciences
Associate Professor²,
Jaipur National University
Jaipur, Rajasthan, India

Abstract--Cloud computing is the recent trend for the growth in IT industry. We are able to store any amount of data on cloud today whether it is text, image, audio, and video and many more. Storing data on cloud is easy but it is very important that the data which we store on store is also secure. Many cryptographic algorithms have been implemented to maintain the privacy of data over cloud. In this paper, we will make a comparative analysis of various cryptographic algorithms used over cloud to secure data. This analysis will be made using various performance metrics.

Keywords-- Cloud computing, symmetric algorithms, asymmetric algorithms

I. INTRODUCTION

Data is a small unit of information. It is a critical aspect from which information is created. Data can be any text, image, audio or video. It is very important to manage and store this data. Today, data is mainly stored on cloud. Data on cloud can be stored in various ways. But it is more important that data stored on cloud should be secure.

NIST defined cloud computing as "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" [1]. Cloud computing has become one of the most emerging trend. This is because it provides many services to its customers and at a very low cost. The only issue with cloud computing is security of cloud. Security of data can be achieved by applying the principles of confidentiality, authentication, integrity, non-repudiation, access control and availability.

To maintain the privacy of data, principle of confidentiality is most important. Confidentiality ensures that the data is shared only by the sender and the intended recipient. This means, it is important that the sender uses some technique in which the data can be identified only by the receiver and not by any unauthorized user. The process of converting a readable message in a non-readable form is called encryption. The reverse process of converting back the non-readable message in the readable form is called decryption. Cryptography is defined as study of techniques to form a secure communication.

There are three ways of using cryptography: by converting plain text to cipher text, symmetric key algorithms and asymmetric key algorithms. Converting of plain text into cipher text can be done using substitution techniques in which a character in plain text can be replaced by any other character, number or symbol and using transposition techniques in which some permutations and combinations are used to encrypt the plain text characters.

Symmetric key algorithms are one in which same key is used for both encryption and decryption. There are many symmetric key algorithms like DES, triple DES, AES, Blowfish and IDEA. These algorithms works on different input size blocks and different input size keys. Asymmetric key algorithms use two keys, one for encryption and another different key for decryption. Various asymmetric algorithms like RSA and Diffie-Hellman are used.

II. LITERATURE REVIEW

P. Mell and T. Grance [1], defined cloud computing as a model of providing access to shared resources. They defined five characteristics of cloud as on-demand self-service, broad access network, resource pooling, rapid elasticity and measured service. They identified that a cloud model is based upon the three service models as Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and infrastructure-as-a-Service (IaaS). They also proposed that cloud basically works on any of the four deployment models-private cloud, public cloud, hybrid cloud or community cloud.

L. Alhenaki et al. [2] made a study on security in cloud computing. The study identified various security issues on cloud related to applications, data storage, management of client, operating systems used. The study also identified threats and attacks on cloud related to data loss, data breach, insider and API's. Solutions and countermeasures for the attacks were analyzed.

D. Dhaivat et al. [3] discussed various issues and threats on cloud based upon deployment model and service models. The authors identified issues like multi-tenancy risk, data and encryption, data leak risks, identity and access

management's risks over public cloud, private cloud and hybrid cloud. Risks related to data security, network security, data integrity, data place, data outflow were identified in IaaS, SaaS and PaaS service models.

S. Chaudhary et al. [4] made a comparative study of cryptographic algorithms like DES, 3DES, AES, RSA, DH and hybrid techniques like dual RSA, AES-RSA, RSA-AES-DS on the basis of efficiency. The study concluded that efficiency of symmetric algorithms are more than asymmetric algorithms and efficiency of hybrid techniques is average but is more secure.

S. Sharma et al. [5] proposed a hybrid algorithm takes input data file, splits it into three equal parts, encrypts each part with AES, RC4 and DES algorithms, merges the encrypted parts and then uploads the file to cloud. Comparative analysis of AES and hybrid algorithm was done on the basis of various file sizes, encryption time and decryption time. The study concluded that hybrid algorithm has better execution time and results compared to AES.

K. Sajay et al. [6] proposed a new hybrid algorithm using Homomorphic and Blowfish algorithms. In this, the input text is first encrypted using homomorphic algorithm. The output obtained is then encrypted using Blowfish algorithm. The output obtained is the final resulted cipher text. The study concludes that the new proposed algorithm is better than traditional algorithms.

K. Patel [7] made a comparative analysis of AES, DES and Blowfish algorithms on 10 small files and large file respectively based on execution time and memory usage. The study concludes that DES is better in terms of execution time, Blowfish is better in terms of memory usage; DES is good for small data files. All algorithms performance is equal on large data files.

N. Advani et al. [8] made a comparative analysis of DES, 3DES, AES, Blowfish, RSA, RC2, RC4, RC6, A5/1, A5/2, Twofish, Threefish, ECC, DH algorithms. The study concluded that AES is good symmetric algorithm, RSA is good asymmetric algorithm, Blowfish and RC variations are more vulnerable, Twofish and Threefish less secured compared to AES.

A. Yusufzai et al. [9] made a study of various security issues and challenges and RSA, DES and AES algorithms based on block size, key length, speed and key used. The study concluded that AES takes less execution time, DES takes less time for encryption, and RSA uses large memory size and longest time for encryption.

A. R. Wani et al. [10] made a comparative analysis of AES, DES, Blowfish, 3DES, RC4, IDEA, TEA algorithms on 10 different file sizes on the basis of encryption time, decryption time, memory usage, security and performance. The study concluded that encryption time for RC4 is minimum and that for 3DES is maximum, decryption time for RC4 and AES is minimum and 3DES is maximum and

memory usage of IDEA and TEA is less and RC4 is more. AES is best in terms of security, performance and memory usage.

N. Anwar et al. [11] the authors made a study of various cryptographic algorithms like AES, Blowfish, DES, 3DES, RSA, DSA, ECC based on performance metrics such as key size, block size, number of rounds, efficiency, vulnerability and applications of algorithms. The study concluded that symmetric algorithms were suitable for image processing, wireless and e-commerce applications whereas asymmetric algorithms were suitable for internet banking, web and mobile applications.

M. A. Al-Shabi [12] made a comparative analysis of DES, 3DES, AES, Blowfish, RSA, Diffie-Hellman (D-H) and ECC algorithms based on various metrics like battery consumption, time consumption, block size, number of rounds and attacks on algorithms. The study concludes that AES algorithm is better in time consumption and D-H is superior to RSA.

R. Kumar et al. [13] made a study on various algorithms used for securing data on cloud like DES, Blowfish, AES, 3DES, RSA, D-H and stated its advantages and disadvantages. The authors concluded that AES uses least time for execution whereas RSA utilizes more memory as well as encryption time. The least encryption time was consumed by DES and least memory utilization was by Blowfish.

Enas Elgeldawi et al. [14] made a survey on comparative analysis of symmetric cryptographic algorithms based on various metric like structure of algorithm, encryption and decryption time, throughput and memory utilization. The analysis showed that AES was more secure and Blowfish was faster.

N. Wahid et al. [15] made a Comparison of DES, AES, 3DES, RSA, Blowfish Cryptographic Algorithms based on various metrics. The result analysis showed that Blowfish has the fastest Encryption and Decryption time, high entropy and it requires less memory usage. Avalanche effect and number of bits required for encoding was high in AES. RSA was slow and required more memory for execution.

S.Rajeswari et al. [16] made a survey on various cryptographic algorithms DES, Blowfish, RC2,3,5,6, 3DES, AES, RSA, DSA, D-H, El-Gamal. The study stated that Blowfish has better throughput and power consumption and AES could be broke by brute force attack. So to adhere maximum security, use of better algorithm was required.

T. Mohanaprakash et al. [17] made a study for securing cloud data using RSA, AES, DES, Blowfish, Homomorphic and IDEA encryption algorithms and made a comparative analysis of the algorithms based on

scalability, security, data encryption capacity, authentication type, memory usage and execution time.

P. Semwal and M. K. Sharma [18] made a comparative analysis of DES, 3DES, AES, Blowfish and RSA cryptographic algorithms based on encryption time, decryption time and memory usage. The study concluded that Blowfish is best in memory requirement, good for small applications and requires less execution time. RSA requires large memory and more execution time. AES has high avalanche effect and is good for privacy and security.

R. G. Saranya and A. Kousalya [19] made a comparative analysis on study of cryptographic algorithms DES, Blowfish, RC2, RC5, RC6, 3DES, AES, RSA, DSA, Twofish, IDEA, El-Gamal, D-H, Homomorphic. The study stated that single algorithm cannot be trusted and security could be increased by applying multilevel algorithms.

T. Ramaporkalai [20], author studied various security algorithms in cloud computing like DES, AES, 3DES, Blowfish, IDEA, Homomorphic, RSA and D-H and concluded that a more efficient algorithm was required to enhance the security of data.

O. K. J. Mohammad et al. [21], made a study of cryptographic algorithms based on key size, performance and output size. The study concluded that symmetric algorithms are faster and efficient and AES is most efficient algorithm followed by DES, 3DES, RC4 and Blowfish.

III. COMPARATIVE ANALYSIS OF SECURITY ALGORITHMS

The Table 01 shows the comparison of various cryptographic algorithms for securing data over cloud based on various parameters made in the survey. The parameters considered are key size, block size, number of rounds, execution time, key used and memory usage. The advantages and disadvantages are also stated.

TABLE I. COMPARISON OF CRYPTOGRAPHIC ALGORITHMS IN CLOUD

Algorithms/ Parameters	AES	RSA	Blowfish	IDEA	DES
Key size	128, 192 or 256 bits	>than 1024 bits	32-448 bits	128 bits	56 bits out of 64 bits
Block size	128, 192 or 256 bits	Variant	64 bits	64 bits	64 bits
Rounds	10, 12 or 14 depending on key size	1	16	8.5	16
Encryption Type	Symmetric	Asymmetric	Symmetric	Symmetric	Symmetric
Key used	Same key for encryption and	One key for encryption and	Same key for encryption and	Same key for encryption and	Same key for encryption and

	decryption	another key for decryption	decryption	decryption	decryption
Execution Time	Very fast	Slowest	Fast	Slow	Same as AES
Data encryption Capacity	Huge amount of data	Small data	Less than AES	Small data	Less than AES
Security	High	Considered secure	Considered secure	Inadequate	Inadequate
Memory usage	Low RAM	Highest memory usage	Less than 5 kb	Highest memory usage	More than AES
Scalability	Yes	No	Yes	No	Yes
Advantages	Most efficient, Less memory, Strong key size, Good speed, time	Easy to share public key	Less memory, Good speed, No attack yet	Rounds complex, large key size	Least encryption time, good power consumption and throughput
Disadvantages/limitations	Brute force attack, software implementation is complicated	Slow, more CPU time and battery power, data compromised by man-in-the-middle	Throughput, key management	Too many operations involved	Key small, initial and final permutation not clear

AES algorithm is important for electronic sensitive data, cyber security and government computer security. AES has been created for and implemented by U.S government to protect sensitive information [22]. Blowfish algorithm has been implemented on various formats of files like image, audio, video, text, document and portable document format [23]. The result has proved to be stable.

IV. CONCLUSION

Cloud computing is important and effective service to provide various resources to the customers especially for storing data. Sensitive data are prone to be more vulnerable. It is important that sensitive data should be stored confidentially. So, security of data is the most essential and crucial aspect. The security can be achieved by applying cryptographic algorithms. The most important aspect of algorithm depends upon input block size and input key size used. Comparative analysis using different parameters of various cryptographic algorithms used to secure data over cloud was made to identify the pros and cons. The survey concludes that symmetric algorithms are more effective and efficient. AES and Blowfish algorithms requires less encryption time. Blowfish algorithm is best in terms of memory utilization.

REFERENCES

- [1] P. Mell and T. Grance, "The NIST Definition of Cloud Computing (draft)," *NIST Spec. 800.145*, p. 7, 2011.
- [2] L. Alhenaki, A. Alwatban, B. Alamri, and N. Alarifi, "A Survey on the Security of Cloud Computing," in *2nd International*

- Conference on Computer Applications and Information Security, ICCAIS 2019*, 2019, pp. 1–7, doi: 10.1109/CAIS.2019.8769497.
- [3] D. Dhaivat, M. Nayana, T. Gajjar, G. Ghoda, D. Parekh, and R. Sridaran, "Cloud security issues and challenges," *Cyber Secur. Threat. Concepts, Methodol. Tools, Appl.*, pp. 77–92, 2018, doi: 10.4018/978-1-5225-5634-3.ch005.
- [4] S. Chaudhary, F. Suthar, and N. K. Joshi, "Comparative Study Between Cryptographic and Hybrid Techniques for Implementation of Security in Cloud Computing," pp. 127–135, 2020, doi: 10.1007/978-981-13-8253-6_12.
- [5] S. Sharma, K. Singla, G. Rathee, and H. Saini, "A hybrid cryptographic technique for file storage mechanism over cloud," *First Int. Conf. Sustain. Technol. Comput. Intell.*, vol. 1045, pp. 241–256, 2020, doi: 10.1007/978-981-15-0029-9_19.
- [6] R. Sajay, K. S. S. Babu, and Y. Vijayalakshmi, "Enhancing the security of cloud data using hybrid encryption algorithm," *J. Ambient Intell. Humaniz. Comput.*, no. 2018, 2019, doi: 10.1007/s12652-019-01403-1.
- [7] K. Patel, "Performance analysis of AES, DES and Blowfish cryptographic algorithms on small and large data files," *Int. J. Inf. Technol.*, vol. 11, no. 4, pp. 813–819, 2019, doi: 10.1007/s41870-018-0271-4.
- [8] N. Advani, C. Rathod, and A. M. Gonsai, "Comparative Study of Various Cryptographic Algorithms Used for Text, Image, and Video," *Emerg. Trends Expert Appl. Secur.*, vol. 841, pp. 393–399, 2019.
- [9] A. Yusufzai, R. Ranpara, M. Vora, and C. K. Kumbharana, *A Comparative Study of Cryptographic Algorithms for Cloud Security*, vol. 841. Springer Singapore, 2019.
- [10] A. R. Wani, Q. P. Rana, and N. Pandey, "Performance Evaluation and Analysis of Advanced Symmetric Key Cryptographic Algorithms for Cloud Computing Security," *Soft Comput. Theor. Appl.*, pp. 261–271, 2019, doi: 10.1007/978-981-13-0589-4.
- [11] M. Navid Bin Anwar, M. Hasan, M. Hasan, J. Z. Loren, and S. M. Tanjim Hossain, "Comparative Study of Cryptography Algorithms and Its' Applications," *Int. J. Comput. Networks Commun. Secur.*, vol. 7, no. 5, pp. 96–103, 2019, [Online]. Available: www.ijcnscs.org.
- [12] M. A. Al-Shabi, "A Survey on Symmetric and Asymmetric Cryptography Algorithms in information Security," *Int. J. Sci. Res. Publ.*, vol. 9, no. 3, pp. 576–589, 2019, doi: 10.29322/IJSRP.X.X.2018.pXXXX.
- [13] R. Kumar, S. Kaur, S. Sejwal, P. Narwal, and P. Jain, "Cloud Computing Data Security using Encryption Algorithms," *IIOAB J.*, vol. 10, no. 2, pp. 75–82, 2019.
- [14] E. Elgeldawi, M. Mahrous, and A. Sayed, "A Comparative Analysis of Symmetric Algorithms in Cloud Computing: A Survey," *Int. J. Comput. Appl.*, vol. 182, no. 48, pp. 7–16, 2019, doi: 10.5120/ijca2019918726.
- [15] N. A. Wahid, A. Ali, B. Esparham, and M. Marwan, "A Comparison of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish for Guessing Attacks Prevention," *J. Comput. Sci. Appl. Inf. Technol.*, vol. 3, no. 2, pp. 1–7, 2018, doi: 10.15226/2474-9257/3/2/00132.
- [16] S. Rajeswari, R. A. Zahra, and R. Kalaiselvi, "A Survey on the Different Cryptographic Techniques used for Data Access Control in Cloud Computing," *Int. J. Curr. Eng. Sci. Res.*, vol. 5, no. 4, pp. 49–53, 2018.
- [17] T. A. Mohanaprakash, A. I. Vinod, S. Raja, A. P. Kalyan, C. B. Babu, and G. Vivek, "A Study of Securing Cloud Data Using Encryption Algorithms," *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.*, vol. 3, no. 1, pp. 730–734, 2018.
- [18] P. Semwal and M. K. Sharma, "Comparative study of different cryptographic algorithms for data security in cloud computing," *Proc. - 2017 3rd Int. Conf. Adv. Comput. Commun. Autom. (Fall), ICACCA 2017*, pp. 1–7, 2017, doi: 10.1109/ICACCAF.2017.8344738.
- [19] R. G. Saranya and A. Kousalya, "A Comparative Analysis of Security Algorithms Using Cryptographic Techniques in Cloud Computing," *Int. J. Comput. Sci. Inf. Technol.*, vol. 8, no. 2, pp. 306–310, 2017, [Online]. Available: www.ijcsit.com.
- [20] T. Ramaporkalai, "Security Algorithms in Cloud Computing," *Int. J. Comput. Sci. Trends Technol.*, vol. 5, no. 2, pp. 500–503, 2017, doi: 10.5120/ijca2017915827.
- [21] O. K. J. Mohammad, S. Abbas, E.-S. M. El-Horbaty, and A.-B. M. Salem, "A Comparative Study between Modern Encryption Algorithms based On Cloud Computing Environment," *8th Int. Conf. Internet Technol. Secur. Trans.*, pp. 531–535, 2013.
- [22] NIST, "What is AES Encryption and How Does it Work?," *Searchsecurity.techtarget.com*. <https://searchsecurity.techtarget.com/definition/Advanced-Encryption-Standard> (accessed Aug. 07, 2020).
- [23] R. Cordova, R. L. Maata, and A. Halibas, "Blowfish Algorithm Implementation on Electronic Data in a Communication Network," *2019 Int. Conf. Electr. Comput. Technol. Appl. ICECTA 2019*, pp. 6–9, 2019, doi: 10.1109/ICECTA48151.2019.8959702.
- [24] A. Kahate, *Cryptography and Network Security*, 2nd edition. Tata Mc-Graw Hill, 2008.
- [25] W. Stallings, *Cryptography and Network Security Principles and Practices*, 4th edition. Prentice Hall, 2005.