IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 11, Issue 10, October 2022

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.118

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 10, October 2022||

| DOI:10.15680/IJIRSET.2022.1110079|

Comparison of Encryption Standards for Enhanced Security within Cloud

Er. Rishabh Sharma*, Dr. Simmi Dutta , Er. Neeraj Dubey

P.G. Student, Department of Computer Engineering, Govt. College of Engg. & Technology, Jammu, India*

Head of Department, Department of Computer Engineering, Govt. College of Engg. & Technology, Jammu, India

Assistant Professor, Department of Computer Engineering, Govt. College of Engg. & Technology, Jammu, India

ABSTRACT: Online security is critical for every field due to enhanced participation of users in online activities. Research has been done and protocols have been devised to tackle the issue of security within online as well as offline applications. One of the most commonly used security standards which is obsolete right now is RSA. As attackers become more advanced, we need enhanced security standards for tackling the issue of attacks. This paper provides the work done to achieve security within cloud. The security standards described in this section include RSA, AES and block chaining based approach. The results attained from these approaches are described in terms of reliability. Block chaining based approach accommodating RSA appears to be the best with highest reliability rate.

KEYWORDS: Cloud, RSA, AES, Block chaining

I. INTRODUCTION

Cloud provides resources to the user on pay per use basis. The cloud popularity is growing day by day due to least cost and high availability of resources [1]. Cloud provides resources to the customers on demand basis and using layered model approach. The structure of the layered model is given within figure 1.

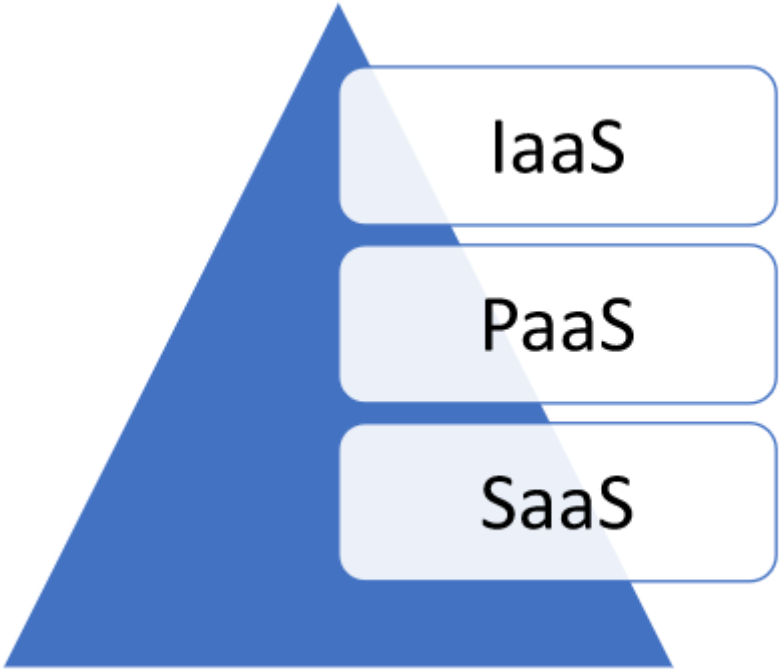

Figure 1: Cloud service model

The layered approach with IaaS indicates infrastructure as a service [2]. Attack at this layer is difficult as cloud attacks are generally oriented towards software and hardware is rarely affected by software attacks [3]. Platform as a service

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 10, October 2022||

| DOI:10.15680/IJIRSET.2022.1110079|

provides system softwares to the client. The PaaS can be attacked by the attacker. The Software as a service is another layered model that can be attacked and must be secured.

Some users of the cloud may be genuine but some of the users may be malicious and attacks will always be conducted by the malicious users [4]. To this end security procedures come into play. RSA was first in the list used to provide security by encrypting the data being transmitted over the network. The key length was appropriate for the cloud since space is saved but security through this system is limited [5]. To overcome the issue data encryption standards were employed within cloud to secure VMs. The symmetric key encryption however is not suitable for cloud as more space is consumed and hence extra cost for securing the VMs will be encountered. The advanced encryption standard is modification of existing DES approach that can be used as a alternative to existing AES approach. The issue however with block chaining remains in this approach.

II. ANALYSIS OF SECURITY APPROACHES

This section presents the study of existing approaches with results.

A. AES

The advanced encryption standard is most commonly used within cloud as it is much more secured as compared to existing data encryption standard and triple DES [6]. The key characteristics of this encryption standard is given as under

- It is a block cipher.
- The size of the key can vary from 128 to 256.
- Encryption of blocks can be 128 bits each.

AES performs the operation on bytes rather than on individual bits. This is an advantage if cloud-based system is not used but disadvantage if cloud-based system is used since extra cost will be encountered. Encryption will take place in rounds [7]. In case key size is of 128 bits then 10 rounds will be required for encryption. In case key size is of 192 bits then 12 rounds required for encryption and in case 256-bit key size is used then 14 rounds of encryption will be required.

Encryption process uses substitution, shift row operation and mix column operation [8]. The decryption process is the reverse of encryption process. This encryption standard is built into the CPU's for increasing execution speed of the processor [9]. The suitability of this approach is however in question for multiple blocks.

Key size(bits)	Data Block size	Reliability
128	1024	0.4
128	2048	0.6
128	4096	0.7
256	1024	0.5
256	2048	0.7
256	4096	0.7

The obtained results in terms of reliability with different key length in the range of 0 to 1 is given as Table 1.

Table1: Reliability results in terms of key and block size

The trend of reliability indicates that it is directly proportional to block size. This means bigger block size result in more reliability [10].

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 10, October 2022||

| DOI:10.15680/IJIRSET.2022.1110079|

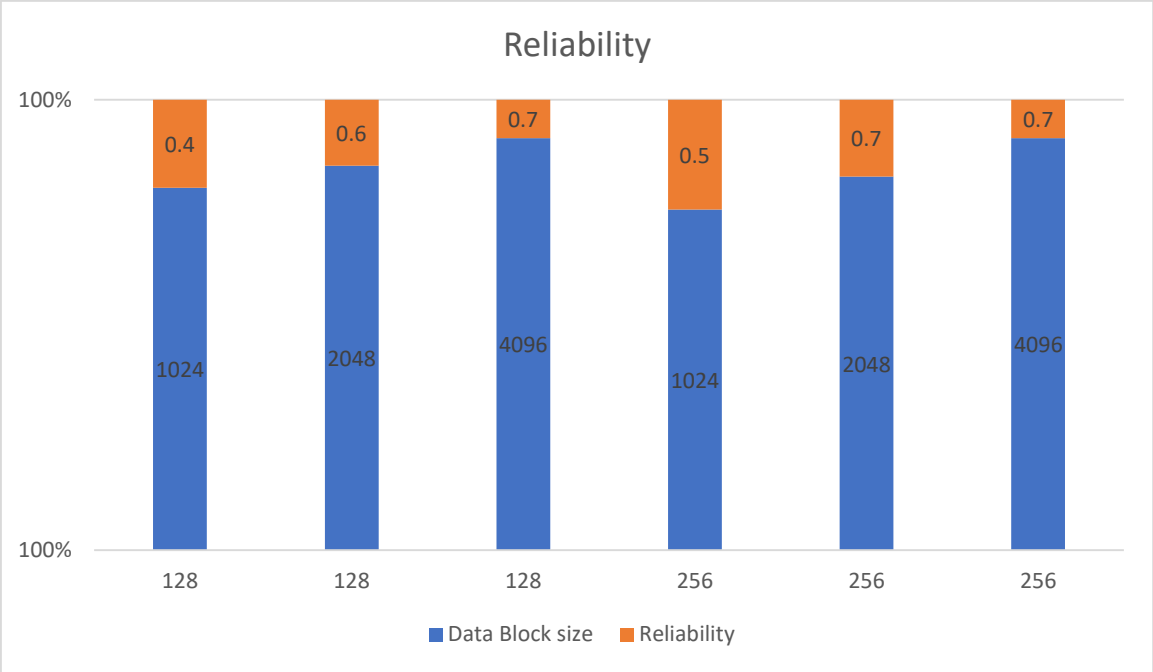

Figure 2: Reliability corresponding to block size and key size

B. RSA

This approach is also simple and used earlier but now it is obsolete [11]. The demonstration of RSA on cloud however can be useful [12]. The primary reason for the same is random key formation. The key size will be of 256 bits. This encryption can be applied on every block within the cloud corresponding to same user to generate key size in collaboration of bytes [13]. This means formed key can be of larger size as compared to advanced encryption standard. The result in terms of reliability is given in table 2

Key size(bits)	Data Block size	Reliability
128	1024	0.2
128	2048	0.3
128	4096	0.3
256	1024	0.4
256	2048	0.5
256	4096	0.6

Table 2: Reliability corresponding to RSA

Although RSA shows least performance as compared to AES [14]. The result shows increased reliability with the block size.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 10, October 2022||

| DOI:10.15680/IJIRSET.2022.1110079|

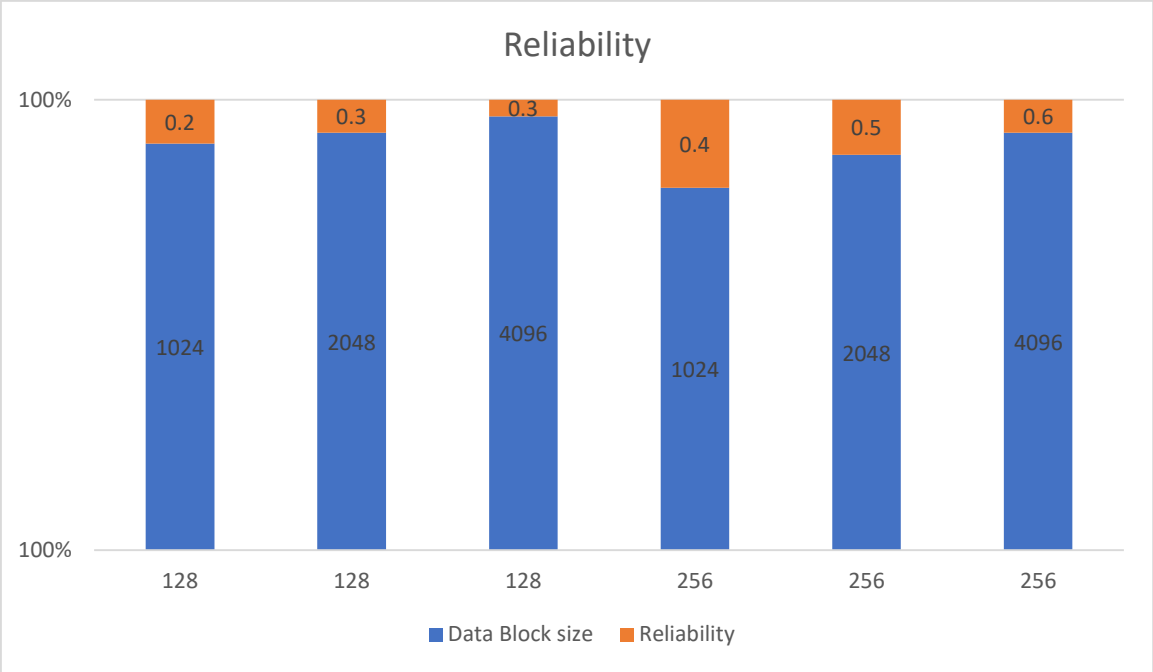

Figure 3: Reliability for RSA with block size.

C. BLOCK CHAINING

This is modern day security model that is commonly employed within the financial institutions for extra security [15]. Each user will be assigned blocks within the cloud space [16]. The security within the blocks will be achieved by applying encryption standards on blocks [17]. The encryption standards with AES and RSA is given in Table 3.

Approach	Key size(bits)	Data Block size	Reliability
AES	128	1024	0.6
RSA	128	2048	0.5
AES	256	1024	0.5
RSA	256	2048	0.7

Table 3: Block chaining with encryption standards

The block security increases when block size is increased. Initially the security with AES is better but as the block size is increased security of RSA with block chaining is increased [18].

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 10, October 2022||

| DOI:10.15680/IJIRSET.2022.1110079|

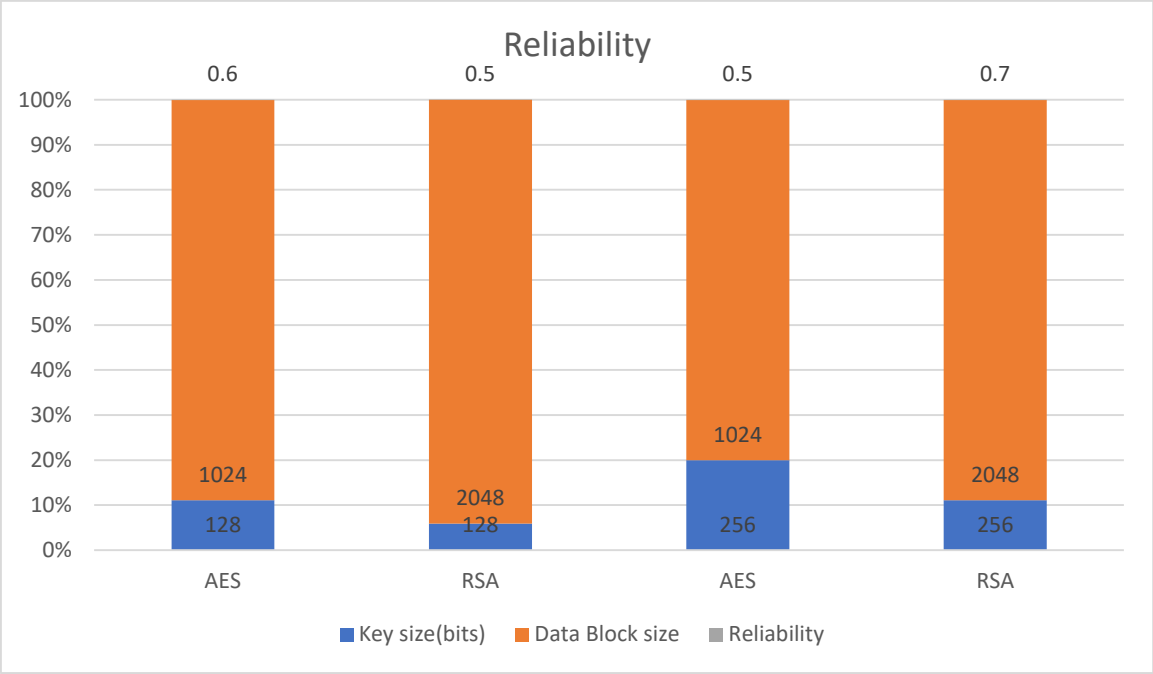

Figure 4: Reliability of block chaining with RSA and AES

III. COMPARTIVE ANALYSIS

The comparative analysis is done to extract best possible result in terms of security of block within cloud. The comparative analysis is given in table 4

Algorithm	Key size(bits)	Data Block size	Reliability
RSA	128	1024	0.2
RSA	128	2048	0.3
RSA	128	4096	0.3
RSA	256	1024	0.4
RSA	256	2048	0.5
RSA	256	4096	0.6
AES	128	1024	0.4
AES	128	2048	0.6
AES	128	4096	0.7
AES	256	1024	0.5
AES	256	2048	0.7
AES	256	4096	0.7
Block Chaining with AES	128	1024	0.6
Block Chaining with RSA	128	2048	0.5
Block Chaining with AES	256	1024	0.5
Block Chaining with RSA	256	2048	0.7

Table 4: Comparative analysis

From the comparative analysis for the large block size RSA algorithm can be useful

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 10, October 2022||

| DOI:10.15680/IJIRSET.2022.1110079|

IV. CONCLUSION

The cloud security is critical and must be provided using encryption standards. The RSA encryption may be obsolete but can be useful within the block chaining. The AES encryption can be useful but the key size is large and complex. When cloud is used the cost will be encountered depending upon the key size. As the key size can be large hence extra cost will be encountered while storing the key. The key size however will allow the highest form of security and reliability. As clear from the comparative analysis, block chaining security can be further improved by the use of RSA approach with different encryption for each block corresponding to each user.

REFERENCES

[1] Thakur, K., Qiu, M., Gai, K., & Ali, M. L. (2016). An Investigation on Cyber Security Threats and Security Models. *Proceedings - 2nd IEEE International Conference on Cyber Security and Cloud Computing, CSCloud 2015 - IEEE International Symposium of Smart Cloud, IEEE SSC 2015*, 307–311. https://doi.org/10.1109/CSCLOUD.2015.71

[2] Ramaporkalai, T. (2017). Security algorithms in cloud computing. *Int J Comput Sci Trends Technol*, *5*(2), 500–502.

[3] Bhardwaj, A., Subrahmanyam, G. V. B., Avasthi, V., & Sastry, H. (2016). Security algorithms for cloud computing. *Procedia Comput Sci*, *85*, 535–542. https://doi.org/10.1016/j.procs.2016.05.215

[4] S Pallikonda, S. Y. R. (2017). Securing cloud data using encryption algorithms. *Int J Adv Res Sci Eng*, *6*(11), 1188–1193

[5] NK Khorsheed, O. K. M. R. T. H. (2015). Proposed encryption technique for cloud applications. *Int J Sci Eng Res*, *6*(9), 693–698.

[6] Tebaa, M., & Hajji, S. el. (2014). *Secure Cloud Computing through Homomorphic Encryption*. http://arxiv.org/abs/1409.0829

[7] R Kaur, S. K. (2014). Analysis of security algorithms in cloud computing. *Int J Appl Innov Eng Manag*, *3*(3), 171–176.

[8] null Tannu, null K. (2017). Enhancing data security in cloud using encryption techniques. *Indian J Comput Sci Eng*, *8*(3), 280–283.

[9] SKB Sangeetha, V. V. S. R. (2018). Enhancing cloud security through efficient fragment based encryption. *Int J Pure Appl Math*, *118*(18), 2425–2436.

[10] KV Nasarul Islam, K. M. R. (2017). Analysis of various encryption algorithms in cloud computing. *Int J Comput Sci Mob Comput*, *6*(7), 90–97.

[11] v Saranya, K. K. (2017). A modified blowfish algorithm for improving the cloud security. *Elsiyum J*, *4*(3), 1–6

[12] A Sidhu, R. M. (2014). Enhancing security in cloud computing structure by hybrid encryption. *Int J Recent Sci Res*, *5*(1), 128–132.

[13] Kartit, Z., Azougaghe, A., Idrissi, H., Marraki, M., Hedabou, M., Belkasmi, M., & Kartit, A. (2015). *Applying encryption algorithm for data security in cloud storage* (pp. 141–154). Springer.

[14] K Handa, U. S. (2015). Data security in cloud computing using encryption and steganography. *Int J Comput Sci Mob Comput*, *4*(5), 786–791

[15] MR Shinde, R. T. (2015). Encryption algorithm for data security and privacy in cloud storage. *Am J Comput Sci Eng Surv*, *3*(1), 34–39

[16] SA Abbas, M. M. (2017). Enhancing security of cloud computing by using RC6 encryption algorithm. *Int J Appl Inf Syst*, *12*(8), 27–32.

[17] Sajay, K. R., Babu, S. S., & Vijayalakshmi, Y. (2019). Enhancing the security of cloud data using hybrid encryption algorithm. *Journal of Ambient Intelligence and Humanized Computing 2019*, 1–10. https://doi.org/10.1007/S12652-019-01403-1.

[18] MZ Salem, S. S. T. E.-S. (2017). An efficient privacy preserving public auditing mechanism for secure cloud storage. *Int J Appl Eng Res*, *12*(6), 1093–1101.

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 8.118

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

Scan to save the contact details