Advances In Security And Privacy Of Data In Cloud Computing: Survey And Discussions

Vijaita Kashyap, Shikha Jain

ABSTRACT: In recent years the use of cloud computing is rapidly growing day by day, as we know that the cloud computing mechanism provides the storage of large amount of data, any user can access the data from anywhere with the help of internet. Cloud computing provide to users a centralized virtual environment and infrastructure without using the cost for physical or active infrastructure in a multiple way. Cloud provides the access of large multimedia data such as the video, audio, image and text etc. In this paper, we have presents the comparative performance analysis for the key generation, encryption time and decryption time for the encryption and decryption standard techniques.

KEYWORDS: Cloud computing, Key, encryption, Decryption.

INTRODUCTION

In today's world the internet is very popular among the not only urban area but also in rural area, Internet totally change the human life, by which a person can perform a various task without going anywhere like banking, marketing, railway reservation, education etc., internet will generate huge amount of data and all the generated data stored in a special space known as cloud computing. As we know that the cloud computing will provide the facility to user to access the data from anywhere and elsewhere, to protect and secure to stored data in a cloud is very challenging task now a days because the attacker may be insider or may be outsider. Cloud computing is a set of information technology services such as the software, hardware, infrastructure, computer network, number of resources and storage of data. Cloud computing services are deployed by the three different models such as the platform as a service (PaaS), software as a service (SaaS) and infrastructure as a service (IaaS), the all mentioned services are used by the authenticate user only in the cloud computing. There are number of key features in the case of cloud computing such as the connectivity of the internet, always is a self service means a user can access always on demand way, location independent resources and transparent cloud usage. The cloud service provider will maintain the automated load balancing, resource allocation and use computing resource tools. Cloud computing provides the on demand services for the stored data and other resources, so security is a very challenging and vital task in cloud computing, there are some techniques to protect the data, authenticate the authorize user, blocked and identified the attacker etc. some encryption and decryption algorithm also used to protect the data from the sender end and also with the receiver end, encryption and decryption techniques are based on the key concepts such as the symmetric key concepts and asymmetric key concepts, key pair (public and private key) etc.

- *Vijaita Kashyap Chitkara University Institute of Engineering and Technology, Chitkara University, Punjab, India. vijaita.kashyap@chitkara.edu.in.*
- *SHIKHA JAIN, Assistant Professor, ABES Engineering College, Ghaziabad, Uttar Pradesh, India. shikha.jain@abes.ac.in*

Here the key size is a represented with a bit size. Some different techniques to the detection and prevention of network attack form the attacker or intruder is the integration of the some integrated cryptographic techniques in to a control the cloud computing system. The cryptographic based approach is a very promising technology that will be able to protect t information from the third parties such as the unauthenticated or illegitimate users. The objective of the present study is to develop a secure and safe framework for the encrypted and decrypted control system in a cloud computing, here we provides the literature review for the some previous techniques based on their key size, their encrypted and decrypted techniques, key may be symmetric or asymmetric key combination etc.

RELATED WORK

Data storage is very challenging task in the present scenario as everyone is using internet and generating the huge amount of data, but clouds computing is solve the issue of storage space, so we stored all the internet data on cloud computing in minimum cost and resource with using some security constraint, here we discuss the some literature work already done by the researchers. Attar N, Shahin M et al. [1], in this paper author present the novel security mechanism for the cloud computing stored data before storage, by using key management techniques with encryption and decryption concepts. Their proposed scheme also considered for the reducing the cost of cloud computing and enhance the security model for the stored data, they compare the various key management scheme with 128 bit, 192 bit and 256 bit with different techniques. Nidhi Shah et al. [2] In this paper author presented the survey for the cloud computing techniques and their resources, they discussed the various issues such as the cloud storage, cloud security, data accuracy and consistency of stored data with using shamir's key management techniques and enable data sharing and efficient transmission of data for the users. As we know that the key generation and management is a vital part in the cloud computing to maintain the security, George Amalarethinam et al. [3] in this paper they present the comparative analysis between the various cloud computing security techniques such as the AES, DES and Blowfish, here the major concern is the maintain security without affecting the speed. They showed their proposed algorithm Blowfish gives better solution than the previous techniques and also provide best encryption algorithm for the given data. R. Velumadhava Rao et al. [4] In this paper author proposed the hierarchical group key management techniques for a cloud environment, they proposed the cryptographic key combination for the securing of data based on key distribution server, the all key is generated by the group member secret

values and decrypt with also group member secret value as decided by the key distribution server. Antonio Celesti et al. [5] In this paper author present the gap issues as discussed by the cloud security alliance and following its guidelines, here author discussed the cloud to edge computing to meet the data confidentiality, data integrity, non-repudiation in cloud computing. The proposed approach shows the developed security extensions better compare with previous techniques performance. Yongkai Fan et la. [6] In this article author discussed the privacy preservation de-duplication scheme for the cloud computing environments. Here they proposed the trusted execution environment based on the secure de-duplication scheme, with using secure key management which improves the security enables and ability to resist with plain text attack and cipher text attack in cloud computing.

PROPOSED METHOD

In this section we present the proposed method with compare the other techniques and solve the issue in security for the stored and when extract the data. As we know that the cloud computing provide the data storage in an efficient way, therefore the need of security for the stored database is play a vital role in cloud computing environment. To implement the security constraints we used the key management techniques such as the symmetric an asymmetric keys including public and private key pair. The efficient way of distribution and access of the cloud data is maintain by the key distribution centre and the authenticity of users is also verify and validated by the same. The number of encryption and decryption algorithms is presents such as the advanced encryption standard, and data encryption standards, RSA algorithm, Elliptic curve cryptography algorithm etc. The key distribution centre share the key among two different parties and both parties access the data with the help of these keys combination. Public key cryptographic algorithm generally provide the one way functionality and ease to attack, while the public and private key concept is tow way functionality and less chance of attack than public key cryptographic algorithm. The below figure shows our proposed methodology block diagram to implement the security while accessing the data form cloud computing.

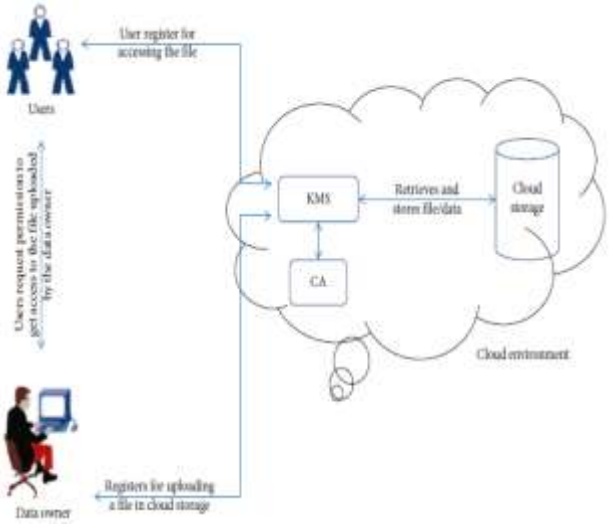

Fig 1: *Proposed method block diagram.*

In the above diagram we used total five components for implementation of the security constraints in cloud computing, these components are data users, data owner, cloud storage, key management system and certificate authority. Initially data owner upload the file on cloud computing and have full control on the uploaded file with unique id for each file, then user is the person who wants to access this file along with their security credentials and authorization access, then the key management system perform very interesting role with cryptography techniques and having the encryption and decryption, maintain data origin authenticity, maintain data integrity etc. the certificate authority is approve the authentication of keys and finally the last components cloud storage simply used to store the files and response when the authenticate user want to access the file.

EXPERIMENT RESULT

In this section we discuss about the experimental result study for the various cryptography techniques as mentioned in the literature survey section. As we know that the stored data is on cloud is available from everywhere with the help of internet connection therefore access time and security for the cloud data is very challenging task for the researchers in current scenario. Time is generally total time of generation of keys, distribution of keys, encryption time for the algorithm and decryption time for the algorithm, finally we can say that the each factor is having important role to affect the overall time. The below figure shows the comparative simulated experimental study for the number of techniques in the security and time constraints.

Table 1. *Time taken for the generation of keys.*

Key Size	Method	Time Taken
48 bits	Previous	500
	RSA	480
64 bits	Previous	980
	RSA	950
128 bits	Previous	1350
	RSA	1310
256 bits	Previous	1700
	RSA	1665
512 bits	Previous	2280
	RSA	2245

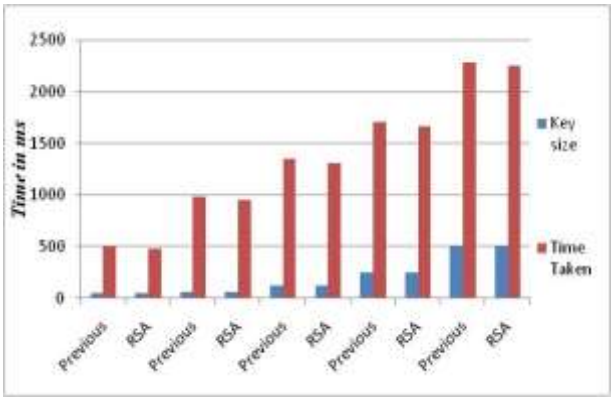

Fig 2: *The above figure presents the comparative solutions for the previous and RSA method with using different number of key size.*

Table 2. *Time taken during the encryption process .*

Key Size	Method	Time Taken
48 bits	Previous	70
	RSA	90
64 bits	Previous	140
	RSA	150
128 bits	Previous	210
	RSA	225
256 bits	Previous	300
	RSA	310
512 bits	Previous	420
	RSA	440

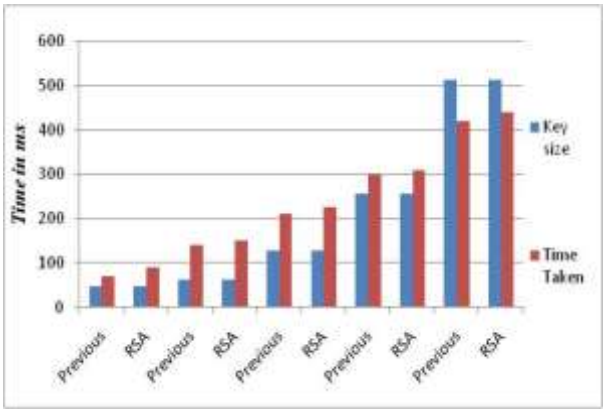

Fig 3: *The above figure presents the comparative solutions for the previous and RSA method with encryption time taken.*

Table 3. *Time taken during the decryption process .*

Key Size	Method	Time Taken
48 bits	Previous	60
	RSA	50
64 bits	Previous	110
	RSA	100
128 bits	Previous	180
	RSA	160
256 bits	Previous	280
	RSA	265
512 bits	Previous	375
	RSA	350

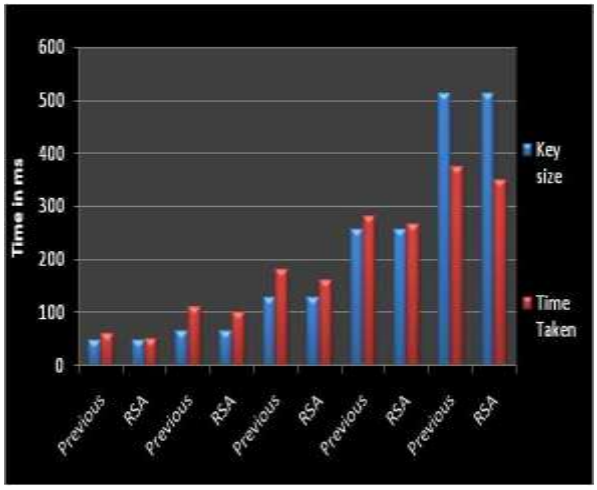

Fig 3: *The above figure presents the comparative solutions for the previous and RSA method with decryption time taken.*

CONCLUSION

In this paper, we have presents the comparative performance analysis for the key generation, encryption time and decryption time for the encryption and decryption standard techniques. In the proposed architecture key management systems perform a very vital role and protect the file and data which is shared among the number of users and protect them against the insider or outsider attacker. In future we also used some advanced algorithm which is similar or strong than the RSA algorithm but consume less power and less storage capacity for the same number of key generation, and also focus with some access control of data such as revocation mechanism of data and user access control.

REFERENCES

[1]. Attar N, Shahin M, “A Proposed Architecture for Data Security in Cloud Storage Space”, Journal of Biostatistics and Biometric Applications, Vol-3, 2018, pp 1-7.

[2]. Nidhi Shah, Digvijay Mahida, “Data Security in Cloud Computing : A Comprehensive Survey”, International Conference on Current Research Trends in Engineering and Technology, 2018, pp 434-438.

[3]. D.I. George Amalarethinam, H.M. Leena, “A Comparative Study on various Symmetric Key Algorithms for enhancing Data Security in Cloud Environment”, International Journal of Pure and Applied Mathematics, 2018, pp 85-94.

[4]. R. Velumadhava Rao, K. Selvamani, S. Kanimozhi, A. Kannan, “Hierarchical group keymanagement for secure data sharing in a cloud-based environment”, John Wiley & Sons, Ltd., 2018, pp 1-16.

[5]. Antonio Celesti, Maria Fazio, Antonino Galletta, Lorenzo Carnevale, Jiafu Wanb, Massimo Villari, “An approach for the secure management of hybrid cloud–edge Environments”, Future Generation Computer Systems, Elsevier ltd. 2019, pp 1–19.

[6]. Yongkai Fan, Xiaodong Lin, Wei Liang, Gang Tan, Priyadarsi Nanda, “A secure privacy preserving deduplication scheme for cloud computing”, Elsevier ltd. 2019, pp 127-135.

[7]. Y. Kiran Kumar, R. Mahammad Shafi, “Model-Driven Platform for Service Security and Framework for Data Security and Privacy Using Key Management in Cloud Computing”, International Research Journal of Engineering and Technology, Vol-6, 2019, pp 1464-1470.

[8]. Shahin Fatima, Shish Ahmad, “Secure and Effective Key Management Using Secret Sharing Schemes in Cloud Computing”, International Journal of e-Collaboration, Vol-16, 2020, pp 1-15.