CGC International Journal of Contemporary Technology and Research
ISSN: 2582-0486 (online) Vol.-5, Issue-1; DOI: 10.46860/cgcijctr.2022.12.31.331

Securing Cloud using Biometric Cryptographic Techniques

Anuj Kumar Gupta
Chandigarh Group of Colleges
Email id: anuj.coecse@cgc.edu.in

Abstract*: *One of the best on-demand network access services to a significant shared pool of computer resources in the modern world is cloud computing. Many well-known economic advantages of cloud computing exist. Without having to own the underlying hardware, cloud computing enables users to take advantage of the combined benefits of three computing models for storage (Infrastructure as a Service), operating system (Platform as a Service), and software (Software as a Service) at their own premises. In spite of these financial advantages, public clouds are still not widely used, particularly by businesses. In terms of virtualized, geographically dispersed data centers, private clouds are now used by the majority of large enterprises, but they rarely serve as the primary source of resources. The main cause of this is the security risks associated with the current cloud infrastructures, which include server setup errors, software defects, power outages, hardware failures, malware, and insider threats. The goal of the research is to compare several biometric cryptography approaches for cloud security based on a variety of different criteria.

***Index Terms* – Cloud Computing, Cloud Security, Authentication, Biometrics, Cryptography.**

I. INTRODUCTION

The research area of cloud computing is relatively young. The use of cloud computing has increased at a rapid pace in past decade. NIST [1] defines cloud computing as "a model for enabling 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". Because users frequently save sensitive information with cloud storage providers, who may not always be totally trusted, ensuring cloud computing security is important in this setting.

Cloud computing offers its customers capabilities like inexpensive storage, simple data accessibility, flexibility (anytime, anywhere, with any resource), and mobility (on the go), which increases their advantages. It attains a large number of consumers which require either infrastructure (servers, storage space, bandwidth etc. Infrastructure as a Service) or Operating System (Platform as a Service) or some licensed application software (Software as a Service). Clouds may be broadly classified in following three categories as shown in table 1 below:

a) Public
b) Private
c) Hybrid

1.1 Cloud Computing Components

Three delivery models, four deployment models, and five characteristics make up the cloud computing model [1]. Location-independent resource pooling, on-demand self-service, quick flexibility, wide network access, and measured services are the five main features of cloud computing [6]. However, security concerns related to confidentiality and integrity puts hindrances in path of users to go for cloud computing. Authentication is a key component of an advanced computing architecture since it serves as the main security component. Identity theft is thus one of the main problems with cloud computing [2].

TABLE 1: TYPES OF CLOUDS WITH DESCRIPTION

Type of Cloud	Description
Public Cloud	The user cannot see the computing infrastructure since it is located on another party's property. Additionally, the user has no control over the infrastructure for shared computing.
Private Cloud	The computing infrastructure is exclusive to the specific company and is not shared. Private clouds cost more money and offer greater security.
Hybrid Cloud	Hybrid clouds combine both public and private clouds, giving them their own benefits.

In the past, private information kept on personal computers was secured physically and verified physically in addition to utilizing usernames and passwords. However, since the information is stored on a third party's server where physical protection is not possible in today's world of cloud computing, usernames and passwords could potentially be compromised or forgotten. Public clouds, where services are offered in a virtual environment using pooled physical resources and are available over a public network like the Internet, are the most well-known form of cloud computing

to many users. Although the cloud may be adaptable and economical, security remains the biggest hurdle to overcome due to a lack of data protections and compliance regulations; as a result, security is the cloud's greatest barrier.

There are no possible instances where data can be allowed to leak to the unauthorized parties and the purpose can only be fulfilled by deploying an effective and efficient authentication mechanism that can ensure the security of data stored over cloud by the user.

Once an authentication module is created, user can be ensured about the safety of the important data. The main security issues with cloud are:

1. ***Privacy and Confidentiality*** - Data that has been outsourced to the cloud must provide users with some confidence that unauthorised users cannot access it at any cost. The user of the cloud should have enough faith in the security of the data being stored there. This can only be ensured by strict security regulations at the cloud service provider level.
2. ***Security and Data Integrity*** - A few approaches for encryption and decryption can be used to provide data security. In addition to ensuring data security, cloud service providers should put in place mechanisms to check the accuracy of the data stored in the cloud..

1.2 Parameters affecting cloud security

There are several security issues with cloud computing because it incorporates so many different technologies, including networks, databases, operating systems, virtualization, resource scheduling, transaction management, load balancing, concurrency control, and memory management [8]. Many of these systems' and technologies' security issues are also present in cloud computing. For instance, the network that connects a cloud's systems must be secure. For instance, when mapping virtual machines to real machines, it must be done safely. Data security includes both encrypting data and making sure that the proper guidelines are followed for data exchange. The algorithms used to allocate resources and manage memory must be secure. Finally, malware detection in clouds may be possible via data mining approaches.

1.3 Security Issues faced by Cloud computing

Whenever a discussion about cloud takes place, there is always much to do regarding its security. There may be chances that users sensitive data stored on cloud may be lost or hacked. A rogue user may also be able to access the cloud by pretending to be another user, infecting the entire cloud. This has an impact on numerous customers who share the compromised cloud. These are Data issues, Privacy issues, Infected applications and last but not the least Security issues.

Clients always keep their significantly valuable data on clouds that require authentication at the login interface of the cloud which can be done more reliably using physiological and behavioural biometric traits of a human being like fingerprints, face, iris, gait, ear, palm-prints, signature etc. instead of using passwords and PINs. Advancing one step further towards having secure clouds, [4], [6], [13], [14], [21] have used these biometric traits to crate biometric cryptographic keys to provide encryption based security in a cloud computing environment. DES, Blowfish, Triple-DES, DSA, RSA and SHA-1 are the algorithms that can be employed for deployment.

1.4 Data Security Techniques

A. SYMMETRIC TECHNIQUES

DES

Data Encryption Standard is what it stands for. For each 64-bit block of data, a 56-bit key is applied. It was the initial encryption standard that NIST had authorised [1]. Despite being created with "strong" encryption, this method takes 16 rounds of controls and can operate in a variety of modes. To provide data protection with integrity, we combined the DES algorithm with a destruction-editing technique [17]. Every round in a transaction utilises a unique 48-bit round key that is generated using DES algorithms from the constant cypher key. A formerly transcendent symmetric-key technique for the encryption of electronic data is the Data Encryption Standard (DES). It has a significant impact on the development of modern cryptographic systems. The block cypher known as DES transforms a set length string of plaintext bits into a second sequence of cipher-text bits with the same length through a jumble of operations. For the most part, the block size is 64 bits due to DES. DES also uses a key to modify the modification, thus only those who are aware of the precise key used to encrypt may execute a decryption. DES has currently been superseded with the Advanced Encryption Standard because it has been found to be insecure for a number of applications (AES) [18].

BLOWFISH

The encryption algorithm is symmetric. It has a 64-bit block cypher created by Bruce Schneider that is much quicker than DES on a Power PC-class computer and was improved for 32-bit mainframes with large data storage. The range of key lengths is 32 to 448 bits. There are 16 rounds in all. Blowfish was created as a readily accessible replacement for DES or IDEA, which are used in a lot of production. [18].

3DES

The development of the Data Encryption Standard (DES) cypher approaches is detailed in Triple DES (3DES),

also known as the Triple Data Encryption Algorithm (TDEA or Triple DEA). TDES operates with a 64-bit block size and employs 48 processing rounds, similar to DES. To increase the amount of encryption and security, 3DES produces three iterations [18]. Utilizing DES 56 bit keys, it creates three encryption and decryption permissions for the block.

B. ASSYMETRIC TECHNIQUES

RSA

The RSA algorithm, created in 1977 by Ronald Rivest, Adi Shamir, and Leonard Adleman, employs the characteristics of generative homomorphism encryption. The RSA key size is 1024 bits. The maintenance of encryption and digital signatures is made possible by the usage of RSA, which is frequently employed in public key approaches. The reason why huge administration suppliers like Google mail, Yahoo mail, and many more are implementing this method to deliver security to their clients is because RSA offers the best security strategy by encrypting the sensitive data [19].

DSA

It provides a specific method to safeguard data on cloud computing through the presentation of independent research of security methods. Digital signature capabilities are provided via the DSA (Digital Signature Algorithm) technology, which is used to authenticate messages [11]. Digital signatures are governed by the Federal Data Processing Standard, or DSA. The NIST first introduced DSA. It is used to find unapproved changes to data that has been transmitted from the source to the receiver.

Diffie-Hellman Key exchange

Only the secret-key exchange protocol is introduced by Diffie-Hellman. The discrete logarithm problem is used, although not for digital signatures or authentication, nor are public key exchange protocols involved. Actually, the secret key was set by the sender and the recipient [12]. Elliptic curve cryptography is used for data encryption while the Diffie Hellman Key Exchange method links organisations to ensure data secrecy.

The rest of the paper is organized as follows. Related Work is given in section II. Comparative analysis of security techniques is presented in section III. Section IV presents concluding remarks.

its own. Once again encrypted by the server's private key, the decrypted template is then saved in the database alongside the username for later use. After the initial registration, the identical concept is applied in phase 2 upon login.

The three most popular symmetric key cryptography algorithms—DES, AES, and Blowfish—were fairly compared by Thakur et al. in their discussion in [15].

II. RELATED WORK

Sugumaran et al [10] discussion of data protection strategies and their suggested architecture for cloud-based data security. Their design was created to store data in the cloud securely utilising symmetric key block cypher technology, which provides access to data more quickly.

In order to safeguard the data from unauthorised access, Monikandan et al. [11] have presented an encryption technique to solve the security and privacy concerns in cloud storage. Two methods can be used to assault data. An administrator having access to user data constitutes an insider attack. Third parties can access user data when there is an outside attack. To prevent unwanted access to the data saved in cloud storage, the Author presented a symmetric encryption method merging substitution cypher and transposition cypher. Their suggested method involves transforming plain text into the associated ASCII text for each alphabet, with keys ranging in size from 1 to 256. Large amounts of data can be encrypted in cloud storage with symmetric encryption because of its speed and computational efficiency.

A "Three-way system" that simultaneously assures data security, authentication, and verification has been proposed by Prashant et al. (12). To ensure the privacy of the data kept in the cloud, they used digital signatures and Diffie Hellman key exchange along with the AES algorithm.

Sanjukta Pal et al. [13] have discussed cryptography combined with the fingerprint biometrics. They have generated the encryption key using fingerprints and deduced the information from the key using fingerprint matching algorithm. To implement the above concept, sender’s recent fingerprints have been used to construct the key. For decryption, the sender’s Database fingerprint images, which are already kept by receiver at receiver’s end, have been used.

S. Kavin Hari Hara Sudhan et al. [14] have discussed AES and RSA data security algorithms for cloud security. They have utilised two separate algorithms: RSA is used for symmetric key encryption and decryption, while AES is used for asymmetric key encryption. In Phase 1 of their two-phase technique, users must sign up on the cloud. When registering, the consumer provides a biometric sample that will be encrypted with a public key obtained from the authentication server and decoded with a private key of

The key issue was how the algorithms performed in various conditions. The comparisons that are shown take into account how the algorithms behave and perform under various data loads. These factors—speed, block size, and key size—were used to compare the systems. Java programming was used to construct the simulation programme. It was determined that blowfish outperforms other widely used encryption techniques.

Three encryption algorithms—DES, 3DES, and AES—have been compared by Alanazi et al.[16] in terms of nine parameters, including key length, cypher type, block size, security, potential keys, potential ASCII printable character keys, time needed to check all potential keys at 50 billion keys per second, among others. This investigation comes to the conclusion that AES outperforms DES and 3DES in terms of performance.

III COMPARATIVE ANALYSIS

The paper discussed various techniques that can be used for data security; all these techniques have their own pros and cons. We have implemented on MATLAB & compared these techniques based on some well-established parameters, which will help us to understand the capability of different security methods available to authenticate data access. Also this will help is in studying their effect on cloud's performance. Following are some of the parameters we have taken to compare the above mentioned techniques shown in table 2 below:

TABLE 2: COMPARATIVE ANALYSIS

Algorithms→ Parameters↓	DES	3DES	AES	Blowfish	RSA
Key Size	56	112,58	128, 182, 256	32-448	1024 to 4096
Number of Rounds	16	48	10(128), 12(192), 14(256)	16	1
Cipher Type	SBC	SBC	SBC	SBC	
Key Type	Private key	Private key	Private key	Private key	Public Key
Speed	Slow	Very Slow	Very Fast	Fast	Slow
Block Size	64	64	128, 182, 256	64	Variant

Key Length: Key length is the size (bits) of the key used in a cryptographic algorithm. The larger the key size, higher the security, but may decrease encryption/decryption speed.

Block Size: Greater security is accompanied by slower encryption and decryption speeds for larger block sizes for a given method.

Possible No. of Keys: This depends upon key size. These are actually the possible permutations of a key. **Speed**: Speed of any cryptography algorithm is always a major concern and depends upon the key size, block size and number of rounds.

Key Type: key type may be private key or public key depending upon the type of cryptography i.e. symmetric or asymmetric cryptography.

Cipher Type: Cipher type may vary among block cipher, substitution cipher, transposition cipher etc.

IV.CONCLUSION

A comparative analysis is given based on already established parameters, helping us to understand the capability of different security methods for cloud security. As per the results computed, AES is the best method for securing cloud infrastructure. We have taken some parameters but there can be few more to be considered in future which may be power consumption, throughput, memory usage, flexibility and type of cloud. Also, MD5 and SHA-1 can be taken into consideration for implementing cloud security.

REFERENCES

[1]. NIST, http://www.nist.gov/itl/cloud/
[2]. Ari Juels, Alina Oprea, "New Approaches to Security and Availability for Cloud Data", white paper.
[3]. Ali A. Yassin, Hai Jin, Ayad Ibrahim, Weizhong Qiang and Deqing Zou, "Efficient Password based Two Factors Authentication in Cloud Computing", International Journal of Security and Its Applications Vol. 6, No. 2, April, 2012.
[4]. Renu S, Hasna Parveen O H, "Biometric Based Approach for Data Sharing in Public Cloud", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 4, Issue 2 February 2015.
[5]. H. Takabi, J.B.D. Joshi and G.-J. Ahn, Security and Privacy Challenges in Cloud Computing Environments, IEEE Security & Privacy, 8(6), 2010, pp. 24-31.
[6]. Mohammed A. AlZain, Eric Pardede, Ben Soh, James A. Thom, "Cloud Computing Security: From Single to Multi-Clouds", 45th Hawaii International Conference on System Sciences, DOI 10.1109/HICSS.2012.153.
[7]. Sanjoli Singla, Jasmeet Singh, "Survey on Enhancing Cloud Data Security using EAP with Rijndael Encryption Algorithm", Global Journal of Computer Science and Technology, Vol. 13, No. 5, 2013.

[8]. Maninder Singh and Sarbjeet Singh,, "Design and Implementation of Multi-tier Authentication Scheme in cloud", International Journal of Computer Science Issues, Vol. 9, Issue 5, No 2, September 2012.

[9]. Tamilarasi Rajamani, Prabu Sevugan, Swarnalatha Purushotham, "An investigation on the techniques used for encryption and authentication for data security in cloud computing", IIOABJ, Vol. 7, No. 5, pp 126-138.

[10]. Zarnab Khalid, Muhammad Rizwan, Aysha Shabbir, Maryam Shabbir, Fahad Ahmad and Jaweria Manzoor, "Cloud Server Security using Bio-Cryptography" International Journal of Advanced Computer Science and Applications(IJACSA), 10(3), 2019.

[11]. L. Arockiam, S. Monikandan," Data Security and Privacy in Cloud Storage using Hybrid Symmetric Encryption Algorithm", International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, No. 8, 2013.

[12]. Sharma, et al, Proposed Upbeat Digital Forensic Method for Cloud Computing Impression, CGC International Journal of Contemporary Technology and Research Vol.-2, Issue-2, 2020.

[13]. M, V. K., Venkatachalam, K., P, P., Almutairi, A., & Abouhawwash, M. (2021). Secure biometric authentication with de-duplication on distributed cloud storage. PeerJ Computer Science, 7. 2021.

[14]. S. Kavin Hari Hara Sudhan, S. Saravana Kumar "An Innovative Proposal for Secure Cloud Authentication using Encrypted Biometric Authentication Scheme" Indian journal of science and technology Vol 8, No. 35, December 2015.

[15]. Thakur J. and Kumar N.: "DES, AES and Blowfish Symmetric Key Cryptography algorithm Simulation Based Performance Analysis", IJETAE, vol. 1, No. 2, pp. 6-12, 2011.

[16]. Alanazi H., Zaidan B., Shabbir M. and Al-Nabhani Y, "New Comparative Study Between DES, 3DES and AES within Nine Factors", Journal of Computing, vol. 2(3), pp. 152-157, 2010.

[17]. Aman Kumar, Sudesh Jakhar, Sunil Makkar "Comparison Analysis between RSA and DES algorithms", International Journal of Advanced Research in Computer Science and software Engineering Vol 2, No. 7, 2012.

[18]. Srinivas B. L., Anish Shanbhag, Austin Solomon D'Souza "A Comparative Performance Analysis of DES and BLOWFISH Symmetric Algorithm", International Journal of innovative research in computer and communication and Engineering, Vol. 2, No. 5, 2014.

[19]. Talwar, J., Gurm, R., Gupta, A., "Evaluate the Performance of Load Balancing Algorithms in Cloud Computing", International Journal of Innovations in Engineering and Technology, ISSN: 2319–1058, 6(4): 154-160, April 2016.

[20]. Shipra Shand, Rahul. (2022) A Comprehensive Study on the Role of Machine Learning in Hybrid Biometric Recognition. 2022 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS), pages 85-90.

[21]. Ching-Nung yang, "Protecting data privacy and security for cloud computing based on secret sharing", International symposium on biometrics & security technologies 7:259–266, 2013.