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 12, Issue 1, January 2023

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| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 1, January 2023 ||

| DOI:10.15680/IJIRSET.2023.1201044 |

Encryption of Data within Networked Resources: A Study of DNA Based Mechanisms

Vanishka Mohan Dubey, Subhash Chander Dubey

M.Tech Student, Department of Electronics and Communication Engineering, Govt. College of Engineering and Technology, Jammu (J&K), India

Professor, Department of Electronics and Communication Engineering, Govt. College of Engineering and Technology, Jammu (J&K), India

ABSTRACT: The technology is enhancing and so does the threats associated with the signal transmission. Cloud plays a critical role in the data storage and transmission within different user groups. Cloud provides resources at cheap and best prices that is a primary reason for the popularity of the cloud. The issue however arises when multiple users interact with cloud having varying intensions. To this end, this paper discusses the security mechanisms that can be used to enhance cloud trust. Each strategy has some merits along with demerits. This paper discusses the merits and shortcoming of security mechanisms within cloud. DNA encryption that is based on complex DNA structure of humans discovered to be most effective in tackling security threats within cloud computing. This paper also discussed the future enhancements that can be made for handling the security threats within cloud. The metrics that can be enhanced with the security procedures includes execution time, throughput and key size.

KEYWORDS: Cloud, security, DNA, throughput, key size

I. INTRODUCTION

Cloud provides the resources to the users on pay per use basis that is a primary reason for the success of the cloud model. As number of users associated with cloud increases, so does the threats associated with it. The cloud based model is a subscription based service providers. The cloud model includes platform, infrastructure, and information related services. The malicious users however can cause problems with the cloud storage and other services. Due to the competitive environment, each cloud service provider wishes to provide best and quality services to the users. In case, trust of the users is not maintained, user or customer retention will be an issue. To this end, cloud service provider uses security mechanisms. The security mechanisms could be many. Some of the security mechanisms includes RSA, DES, DNA and many more. RSA is one of the most used mechanism to provide security within cloud but there exists an issue that key is shared within the sender and receiver. This will cause issue of data theft. Thus, some modification to the existing RSA based mechanism is required. Data encryption standard is another security mechanism that is used within the cloud. However this security mechanism has become obsolete due to the problem with the key size. DNA encryption is one of the most commonly used mechanism that can be used to enhance the security of the cloud. The DNA based encryption is dependent upon the human DNA which is quite complex. Thus, cracking security of the DNA encryption is difficult. Within this research, DNA encryption is explored and future perspective is suggested.

This is paper presents the discussion about the cloud security mechanisms and is organized as under.

- Section 1 provides the generation discussion of the security and its requirements within cloud.
- Section 2 highlight the work that is being done within cloud to ensure security.
- Section 3 presents the problems discovered from the literature in terms of research gap.
- Section 4 gives the proposed methodology that can be used to enhance security
- Section 5 concludes the research.

II. LITRATURE REVIEW

The critical evaluation of the existing literature is presented to extract best possible technique from the available resources.

| |e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.118| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 1, January 2023 ||

| DOI:10.15680/IJIRSET.2023.1201044 |

(Sohal and Sharma 2018)discussed the DNA encryption mechanism. The DNA encryption takes the input as file or media files. The received data is encrypted and stored. The encryption is based on human DNA which is complex and hence not easily decodable. The formed key is complex and hence high security is achieved with this encryption.

(Kudtarkar et al. 2015) proposed security mechanism for the data storage. The security mechanism is provided at Cloud service provider end. The customer however required to pay for the service. RSA encryption is used in this case for security.

(Akhil et al. 2018) proposed advanced encryption standard for the cloud storage. 64 bit key is used for the encryption. The execution speed associated with the encryption is low but security is not complex. The data theft can be an issue as obsolete encryption mechanism was used in this case.

(Chase et al. 2019) proposed a cyber security mechanism for enhancing security of cloud. The cloud security is given utmost importance in this case. The security mechanism that is used is based on RSA encryption. Key size is small and encryption is not strong. This type of encryption can lead to the loss of data and theft as well.

(Shaukat and Hassan 2017) Proposed encryption mechanism that is handled at service provider end. The service level agreement is done between the cloud service provider and clients. The service provider charge for the service they provide. Overall, this mechanism is expensive. Furthermore, execution speed depends upon the length of the file to be uploaded within the cloud.

(Deshmukh 2018)proposed multiway encryption strategy. The extreme level security is provided using DNA encryption in this case. The issue with this approach is collision. Multiple data files can generate same key specifying location of data. Same key means same location and hence existing data will be lost in case new data generate same key for storage.

(Esposito et al. 2018)proposed bock chain-based mechanism in which each block is encrypted with separate key. The security is enhanced in this case however overall cost of encryption is enhanced in this case. The key size is substantial and difficult to decode.

(Jana et al. 2018)proposed memory replication based mechanism for enhancing the security of cloud. This mechanism copy the critical data and stores them at different locations. Encryption is provided at all the locations of data. In case one block is corrupted, then to check, other block is compared against the attacked block. This mechanism however is complex and time consuming.

(Meng et al. 2018)proposed tree based mechanism for providing security within cloud. In this approach, file is not stored at single location rather it is stored at multiple locations for enhancing security. The key size is a biggest advantage in this case.

(Singh et al. 2015) proposed elliptical encryption based mechanism in this case. The encryption strategy is 128 bits and provide random key for encrypting the file.

(Awad et al. 2018) proposed a chaos encryption mechanism for security in cloud. The encryption at each block is randomized. This means, encryption key is changed with each block for making the complex encryption strategy.

Table 1: Comparative analysis of different security Schemes

Reference	Technique used	Advantage	Disadvantage
(Kudtarkar et al. 2015)	Multiple cloud storage with encryption	Enhanced the encryption mechanism with complex key size	The implementation of this mechanism is difficult
(Akhil et al. 2018)	AES based cloud security	The decryption leads to same data without compression	Collision could be an issue in case same key is generated for different blocks

| |e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.118| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 1, January 2023 ||

| DOI:10.15680/IJIRSET.2023.1201044 |

(Chase et al. 2019)	Cyber insurance provisioning and security	Multiple copies of data is maintained for reliability	Accuracy of data can be an issue
(Shaukat and Hassan 2017)	Encryption strategy	The availability of data is enhanced using this mechanism	Collision problem exists
(Deshmukh 2018)	Three level protection technique	Data security and privacy is provided with the help of this mechanism	Cloud storage is extensively used and hence cost is enhanced
(Esposito et al. 2018)	Block chain based access control	The secure cloud storage is provided	Collision of data can be an issue in this case.
(Jana et al. 2018)	Memory replication mechanism	Sensitive information is encrypted and hence data loss is not an issue	Extra space is consumed and hence cost is high.
(Meng et al. 2018)	Hierarchal framework	Clustering mechanism is used to analyses the data quickly	Cost in terms of space is required
(Singh et al. 2015)	Elliptic Curve Digital Signature Algorithm (ECDSA)	Fast encryption mechanism along with decoding is achieved with this approach	Collision problem exists
(Awad et al. 2018)	chaos based encryption strategy	The privacy and confidentiality is achieved with this approach	Back up services are not provided with this approach.

Resource sharing is achieved with the cloud based services. Malicious users can access the shared resources and cause critical issues related to data theft. To this end, data security based mechanisms as discussed in this literature can be used. The DNA encryption can be used to provide security of critical information and restore the reliability of cloud.

III. RESEARCH GAP

DNA encryption ensures that complex encryption can be provided for enhanced security within cloud. The encryption associated with DNA is complex. The biggest issue that is discovered includes collision. This type of issue arises as the same data can lead to same type of key. The key in this case specifies the location where data is going to be stored. The stored data will be erased in case other data location is similar to the new data. This issue can eb resolved only if multiple DNA patterns are supported by the new encryption mechanism.

The parametric comparison table for essential and absent features in existing work along with future enhancement is given in table 2.

| |e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.118| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 1, January 2023 ||

| DOI:10.15680/IJIRSET.2023.1201044 |

Table 2: Parametric comparison with essential and absent features

FEATURE	QUANTITY AND DESCRIPTION	PROBLEM
Steps	• Loading files and data • Performing encryption • Downloading • Decryption	Specifies the phases that are going to be performed for data transmission
Performing security	DNA based encryption with random key support	Division method of encryption is used within DNA
Size of the key	64 to 128 bits	Size of the key will decide the complexity of the approach
Time	Amount of time it takes to executes algorithm	The contents that already exists will not be uploaded and hence time consumption reduces.
Future Work	The complex file encoding may be an issue and must be resolved	----

IV. METHODOLOGY OF PROPOSED WORK

The methodology of the work is divided into multiple steps and is given in figure 1. The overall phases associated with the proposed approach are elaborated in this section.

Phase 1: Loading files
First of all, file is required to be selected. This file will be selected from the client end. The client will transmit the file towards the service provider. The client can transmit the files only if cloud service provider and clients have service level agreement.

Phase 2: Performing encryption
The hash chain mechanism is applied with the division method for encryption. The overall mechanism includes the data selection and applying division operator for generating a key. The key is checked for redundancy. The redundancy can be an issue and may cause data loss. So, this problem must be rectified to use this approach.

Phase 3: Downloading
After the encryption is performed, data can be downloaded at the client end. It is important to note that data is encrypted at the service provider end. The downloaded file is not in customer understandable format. It must be decrypted for understanding by the client.

Phase 4: Decryption
The final phase is decryption. This is accomplished with the help of decryption process. The decryption process is on the basis of a key.

| |e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.118| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 1, January 2023 ||

| DOI:10.15680/IJIRSET.2023.1201044 |

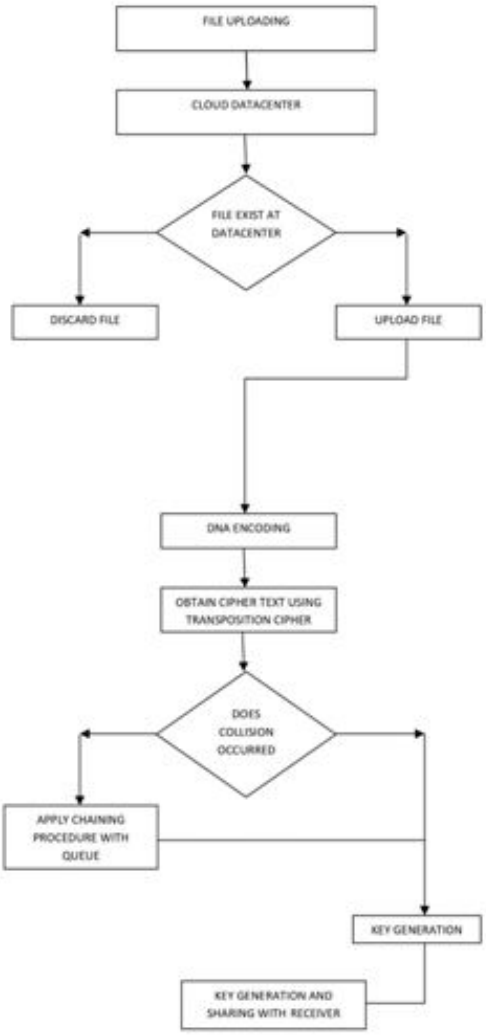

Figure 1: Flowchart for proposed system using collision handling procedure.

V. CONCLUSION

Cloud based models provide cheap and best storage and other services to the clients. The cloud service provider and client agree to the service level agreements. The security of cloud is critical for enhancing the trust of the consumer. The competition in cloud industry is also enhancing so every cloud service provider is considering trust by providing security to the client data. To this end, this research work analyzed some of the security mechanisms that can be used to enhance the customer experience. DNA encryption appears to be the best among all the security mechanism discussed. The DNA encryptions is based upon human DNA and complex key is generated that is difficult to crack. Furthermore, by incorporating collision resolution mechanism DNA encryption can be further enahcned.

REFERENCES

1. Akhil, K. M., M. Praveen Kumar, and B. R. Pushpa. "Enhanced cloud data security using AES algorithm." In 2017 International Conference on Intelligent Computing and Control (I2C2), pp. 1-5. IEEE, 2017.
2. Awad, Abir, Adrian Matthews, YuansongQiao, and Brian Lee. "Chaotic searchable encryption for mobile cloud storage." IEEE Transactions on cloud computing 6, no. 2 (2015): 440-452.
3. Chase, Jonathan, Dusit Niyato, Ping Wang, SivadonChaisiri, and Ryan KL Ko. "A scalable approach to joint cyber

| |e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.118| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 1, January 2023 ||

| DOI:10.15680/IJIRSET.2023.1201044 |

insurance and security-as-a-service provisioning in cloud computing." IEEE Transactions on Dependable and Secure Computing 16, no. 4 (2017): 565-579.

4. Deshmukh, Rachana, Rashmi Deshmukh, and Pallavi Chaudhari. "Enhanced Privacy Preservation and Data Storage Security in Public Cloud." HELIX 8, no. 5 (2018): 3726-3730.
5. Esposito, C., A. D. Santis, G. Tortora, H. Chang, and K. R. Choo. "Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy? IEEE Cloud Comput. 5 (1), 31–37 (2018)." (2018).
6. Jana, Bappaditya, Jayanta Poray, Tamoghna Mandal, and Malay Kule. "A multilevel encryption technique in cloud security." In 2017 7th International Conference on Communication Systems and Network Technologies (CSNT), pp. 220-224. IEEE, 2017.
7. Kudtarkar, Prathamesh P., Jayesh D. Pagare, Sujata R. Ahire, and Tejaswini S. Pawar. "Enhanced file security using encryption and splitting technique over multi-cloud environment." (2015).
8. Meng Y, Qin T, Liu Y, He C (2018) An Effective High Threating Alarm Mining Method for Cloud Security Management. IEEE Access 6:22634–22644 .doi: 10.1109/ACCESS.2018.2823724
9. Shaukat K, Hassan MU (2017) Internet security using encryption technique. Transylvanian Rev 25:74–82
10. Singh JP, Mamta, Kumar S (2015) Authentication and encryption in Internet. 2015 Int Conf Smart Technol ManagComputCommun Control Energy Mater ICSTM 2015 - Proc 216–219 .doi: 10.1109/ICSTM.2015.7225417
11. Sohal M, Sharma S (2018) BDNA-A DNA Inspired Symmetric Key Cryptographic Technique to Secure Internet. J King Saud Univ - Comput Inf Sci. doi: 10.1016/j.jksuci.2018.09.024

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

www.ijirset.com

Scan to save the contact details