Webology, Volume 18, Number 1, 2021
ISSN: 1735-188X
DOI: 10.29121/WEB/V18I1/45

A Cryptographic Approach for Cloud Based Healthcare Applications

Dr. M. Anand Kumar[1] Dr. Kamelsh Chandra Purohit[2] and Mr. Anuj Singh[3] , Sonali Gupta[4]

[1]Professor, Department of Computer Applications, Graphic Era Deemed To Be University, Dehradun, India
[2]Associate Professor, Department of Computer Science, Graphic Era Deemed To Be University, Dehradun, India
[3]Assistant Professor, Department of Computer Science and Engineering, Graphic Era Deemed To Be University, Dehradun, India
[4]Assistant Professor, Department of Computer Science and Engineering, Graphic Era Hill University, Dehradun, India

ABSTRACT

The rapid development in communication technologies paved the way of new integrated health care systems. Such development s provides more flexibility to health care services by providing a platform to share health care data between different health care stake holders. The patient's record consists of a different type of information such as patient information, medical histories, immunization studies, laboratory reports and other sensitive information. The ability to freely share group data among participants in cloud computing increases the effectiveness of work in collaborative settings and offers a wide range of possible uses. Cloud computing is one of those digital technologies used in health care applications for storage and transmitting of medical data between various medical expects. Even though, the cloud based application provides better solution for the health care application but arises several challenges respect to security, confidentiality and privacy of medical information. This paper proposed a cryptographic approach to provide the security for the secure exchange of sensitive information in cloud environments. The experimental result shows that the proposed model is suitable for the majority of applications with little overhead in terms of efficiency.

Keywords: Access control, Cloud computing, Decryption, Encryption, Medical applications, security and Privacy.

INTRODUCTION

Cloud computing has emerged from the concept of distributed software architecture. It plays a vital role in e-health care systems. It provides efficient services for both medical professionals and patients in storage, processing and renewing health related information with good productivity and quality [1]. It provides the easiest way to access the patient information from several locations where the information is distributed among different services. In the past few decades, cloud based

Webology, Volume 18, Number 1, 2021
ISSN: 1735-188X
DOI: 10.29121/WEB/V18I1/45

computing and storage has increased acceptance [2]. These technologies are transforming each and every activity and also increases the efficiency of application that make use of cloud computing. Currently, most of the corporates store all their business data in cloud servers owing to the limited storage capacity and need for easy access. This is one of the smart alternatives for businesses and administrations to evade the expense of establishing and preserving storage devices that are stored locally. [3].

Although the cloud based server offers consumers and enterprises, an accessible and practical storage solution, it also poses security risks. For instance, malevolent users and cloud providers both have the potential to attack a cloud environment. In these situations, it's crucial to guarantee the safety of the cloud-stored data [4]. A key agreement procedure can be used in cloud computing to promote secure and effective data sharing by generating a shared conference key for numerous participants to assure the security of their subsequent interactions.

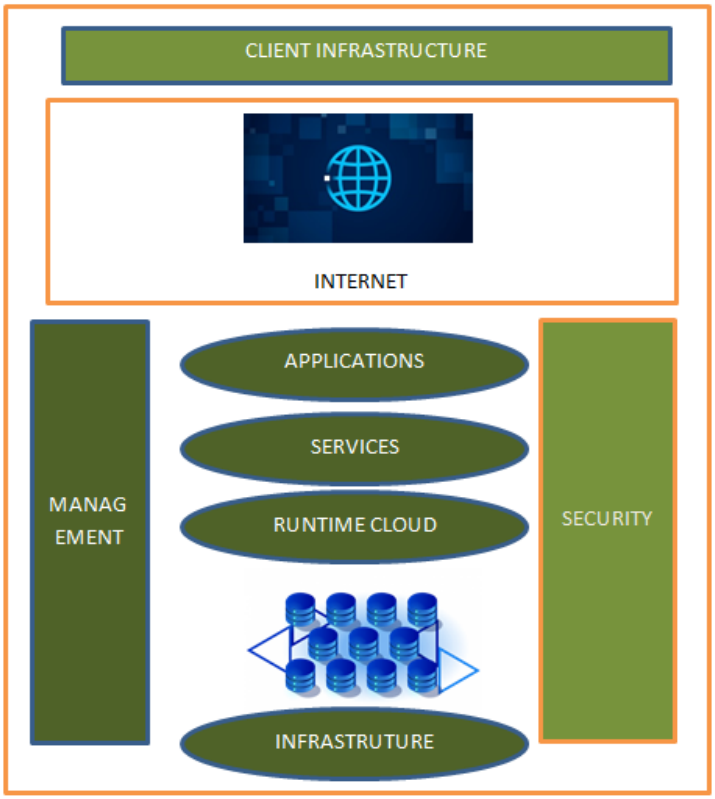

Figure 1 Cloud Computing Architecture

PaaS provides basic software applications and elective services to the client to build cloud based applications without installing any software from their side. It also provides a variety of applications and services to deploy numerous applications. SaaS allows users access software applications without installing them on their own computers [5]. Four Classifications of cloud computing can be defined based on the service models: (1) The Public cloud, where network assets are rented or allocated to public users and organization. Here service provider is responsible for allocating

Webology, Volume 18, Number 1, 2021
ISSN: 1735-188X
DOI: 10.29121/WEB/V18I1/45

resources to the users. (2) In Private clouds, the resources are allocated to only selected users or organization. Such type of services provide better security to the cloud resources when compared to other applications; (3) A community cloud, that is a type of cloud architecture, allows a group of different businesses to access platforms and services and share data. It is owned, managed, and operated by one or more community-based organizations, a third party, or a combination of them; and (4) Public and private clouds can coexist in a hybrid cloud environment. Creating a unified, automated, and the well-managed computing environment is the major goal of combining these clouds (Public and Private). [6].

Literature Review

A model that enables universal, practical, on-demand access to network utilities such as cloud-servers, computer network components, facilities, data storage and applications, that can be quickly allocated to the users with limited effort from management or service providers is known as cloud computing. It provides the flexibility for the users in accessing any type of resources over the internet without any burden from the client side. It is possible to keep private files on the cloud using Google Drive. Even before the data leaves the device, Google Drive encrypts it using the TLS (Transport Layer Security) standard. Then it is put on the drive. The data encrypted first with the use of 256-bit AES (Advanced Encryption Standard) in the client side and transmitted over the network to the destination.. The data is further secured by adding a second layer of encryption using rotating master keys to the AES encryption keys used to encrypt the data [7].

Since ancient times, safe communication has been a goal of both cryptography and encryption. Symmetric-key cryptography protects data by encrypting it using a special key that is shared by the sender and the recipient [8]. The rapid evolution of cloud computing is the outcome of technological advancement. With the use of the internet, cloud computing enables on-demand access and access from any part of the globe.

In an Amazon S3 region, Amazon S3 redundantly stores objects across numerous facilities. This redundancy aids in data repair in the event of a problem with data corruption [9]. Versioning is another technique used by Amazon S3 to maintain all of the objects that are saved in our Amazon S3 bucket. So it is possible to recover from user error and application problems with versioning [10]. Similar to Google, Amazon utilizes server-side encryption to protect data when it is at rest, or when it is kept in discs in Amazon S3 data centres. 256-bit AES is utilized to encrypt the data.

The authors of [11] discussed the cloud security challenges that have been incorporated into SLA. They discuss the complexity of SLA in their paper in order to help businesses comprehend the various security levels that are being used. The work by [12] examines a variety of fundamental concepts that can be constructed using distributed computing as well as determine practical methods to benefit from developing innovation. In their study [13], which specifically highlighted cloud computing, the authors analyzed the list of consequences associated with the cloud data storage and proposed several mechanisms to over the issues related to data privacy.

Recently, the authors [14] developed an identity based encryption with the concept of revocable storage scheme and extended the concept of encryption scheme to allow key updation and cipher-

Webology, Volume 18, Number 1, 2021
ISSN: 1735-188X
DOI: 10.29121/WEB/V18I1/45

text update functions. They also demonstrated that the RS-IBE scheme does not adhere to the RS-correctness IBE's property. They also suggested a method to change the current RS-IBE arrangement. The study [15] addressed the growing implementation of cloud based applications in the health care sectors as well as several security concerns. Data theft assaults are among the most serious security lapses involving cloud-based healthcare data, for example. The authors' main concern is deploying a fog computing facility to secure sensitive healthcare records in the cloud. Participants can generate session keys and communicate securely using a tri-party one-round mutual authentication approach based on substitution and permutation cryptography.

Proposed work

Initially, this research used three types of trusted cryptographic procedures, including Elgamal, Blowfish and MD5 Hash function to build the security design. The plain-content P_t is first encrypted using Blowfish before being scrambled. Elgamal encryption is also used to encode the key_k that is used for encryption. The output content C_t and the output key C_k will then be delivered to the destination. While waiting, the plain-content message process will be calculated using MD5. At that point, Elgamal encryption will be used to encrypt the messaging process. C_m will now be sent to goal together with C_t and C_k. The key is first decoded using Elgamal decoding at the collector end. Next, the Cipher-content is decoded using the newly acquired key. While waiting, the message process is calculated using SHA.

Then the beneficiary side's verification process is compared with the hash value that is received from the source address. This proposed model mainly concerned with sensitive medical records that uses both symmetric and asymmetric cryptography to provide all aspects of security features. The aforementioned model revealed that, in order to provide the highest level of security, the algorithm's block and key sizes needed to be sufficiently large. It was discovered that the encryption time needed to be cut in order to achieve greater performance, which is another component of performance. The analysis led to the formulation of the suggested architecture as

- Blowfish and IDEA are replaced with a 512-bit block cypher.
- A time-saving algorithm for the encryption procedure.
- Real-time application-supporting algorithms, such as those for speech data.

The SF Block cypher is a 512-bit block cypher. Based on the Substitution Permutation Network design principle, this block cypher was implemented. (SP Network). The cipher-text block is built from an unit of plain text, the key, and numerous alternate rounds. The proposed model uses 512 bits as the block size for encryption algorithm. With the key size is 512 bits. The paper [16] contains the algorithm's implementation. The functioning of the architecture is depicted in the following figure.

Webology, Volume 18, Number 1, 2021
ISSN: 1735-188X
DOI: 10.29121/WEB/V18I1/45

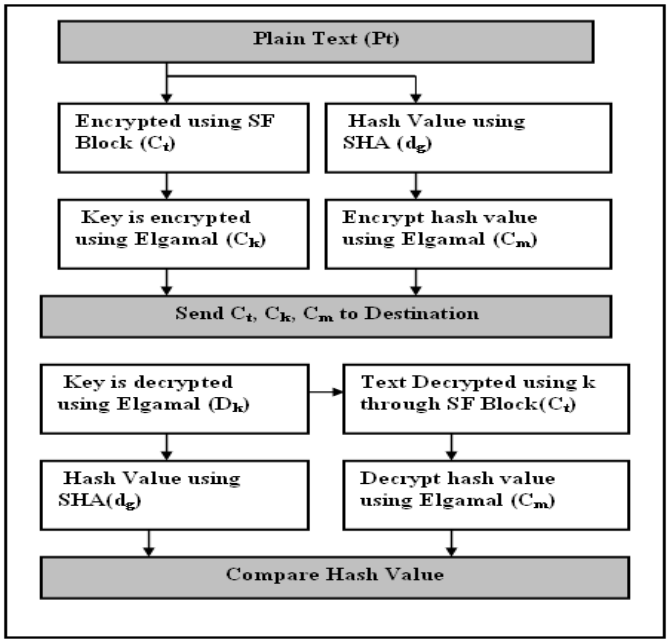

Figure 2 Proposed Security Architecture

Finally, three algorithms—the 512-bit SF Block cypher, the Elgamal algorithm, and the SHA-2 hash function—were used to build the design. The investigation demonstrates that the suggested model was more performing and more secure than the old model when compared to other current methods. The functioning of the architecture is depicted in the following figure.

Performance Metrics

Several experimental strategies are employed, including various encryption encoding methods, various data packet sizes,0 various data kinds, and various key sizes. Base64 encoding and hexadecimal encoding are two examples of the types of encoding that are employed. The used packet sizes range from 0.5 MB to 20 MB. For each chosen method, several forms of data, such as text, documents, and photos, are utilised. To track the effectiveness of the chosen algorithms, specifically power consumption, several key sizes are used. Equation contains the formula to compute the typical encryption time (1).

$$\text{Avg Time} = \frac{1}{Nb}\sum_{i=1}^{Nb}\frac{Mi}{Ti}(Kb/S \qquad (1)$$

The throughput of an encryption technique is determined using encryption time. It displays the encryption's speed. Equation is used to determine the encryption scheme's throughput.

$$Throughput = \frac{Tp}{Et}$$

(2)

Several methods exist for measuring the energy required for encryption and decryption. The first approach to measuring energy usage is to make the assumption that normal operations use an average amount of energy and then assess how much more energy encryption techniques utilize. This approach merely keeps track of the fraction of the energy that can be calculated using the

Webology, Volume 18, Number 1, 2021
ISSN: 1735-188X
DOI: 10.29121/WEB/V18I1/45

following equations. For one run, the battery life is utilized in proportion terms.

$$OneRun = \frac{Change\_in\_Batterylife}{No\_of\_Runs} \quad (3)$$

Average battery Consumed per iteration

$$\sum_{1}^{N} \frac{Battery\_consumed/Iteration}{No\_of\_Runs} \quad (4)$$

By calculating the number of CPU cycles utilized in computations linked to cryptographic procedures [16], the second technique of security primitives can also be quantified. Equation 5, which is illustrated below, was used to calculate the energy cost of encryption.

$$B\_cost\_Encryption(am\ pere-cycle) = \tau * I \quad (5)$$

B_cost denotes cost of the encryption

$$Total\_Energy\_Cost = \frac{B\_cost\_encryption}{F(Cycles/Sec)} \quad (6)$$

$$Energy\_cost = Total\_Energy\_cost * V \quad (7)$$

Therefore, algorithm energy usage to complete its task (encryption or decryption) is given by

$$Energy = Volt * I * N * \tau \quad (8)$$

N: denotes No of Clock Cycles
Volt: denotes the supply voltage of the system

On order to evaluate the algorithm's security issues, frequency distribution analysis and autocorrelation analysis were also carried out. The test for auto-correlation [17] mostly evaluates an auto-correlation line.

$$C(\tau) = \frac{1}{p}\sum_{n=1}^{p} a_n a_{n+\tau} \quad (9)$$

In this case, may be thought of as a phase shift in the sequence an. The similarity between the sequence and its phase shift is measured by the coefficient C (an). When an is random, C(an) is quite tiny for the majority of other values of, and this is usually maximum when a = 0. The suggested system's security strength is assessed using the autocorrelation analysis, which provides the data's randomness following each round of encryption.

Performance Evaluation

Two widely used symmetric encryption algorithms, Blowfish and AES, were employed to evaluate the performance of the proposed approach [18]. For the chosen cryptographic methods, the performance of encryption schemes was measured using a variety of performance criteria, including energy consumption, changing data kinds including text, documents, and images, key size and the data size. With the work, the replication system has already been tested [19]. To ensure that the

Webology, Volume 18, Number 1, 2021
ISSN: 1735-188X
DOI: 10.29121/WEB/V18I1/45

results are reliable and valid for comparing the various methods with the suggested approach, the experiments are run multiple times.

A) Encryption Process

The calculation of the encryption times for the algorithms such as Blowfish, AES and the proposed scheme of SF Block cipher was done. It is the total amount of time needed to transmit encrypted content from plain-text. The throughput of the scrambled calculation is then determined using the computed encryption time. For the test, various files with size of the file ranging from 35 Kb to 9000 Kb were employed. It provides the encryption rate. The following table presents the encryption time for different file size. The figure shows the variation between different algorithms.

Table 1 Encryption Time

S.No	Packet Size (KB)	Time Consumption(Encryption)		
		Blowfish	AES	SF Block Cipher
1	49.00	59.0	36.0	56.0
2	59.10	39.0	36.0	38.0
3	100.09	94.0	61.0	90.0
4	247.12	121.0	90.0	112.0
5	321.24	167.0	134.0	164.0
6	694.45	234.0	256.0	210.0
7	899.12	254.0	256.0	258.0
8	963.09	213.0	187.0	208.0
9	5345.15	1324.0	1376.0	1237.0
10	7310.39	1432.0	1543.0	1366.0

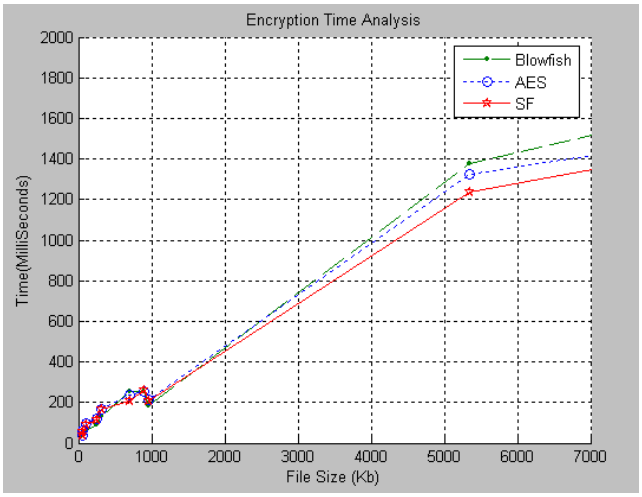

Figure 3 Encryption Analysis

Webology, Volume 18, Number 1, 2021
ISSN: 1735-188X
DOI: 10.29121/WEB/V18I1/45

B) Decryption Process

The time for the decryption procedure with the various file sizes was calculated in a manner similar to that of encryption. The following figure shows how long the decryption process takes for different input size. The figure shows the variation between different algorithms.

Table 2 Decryption Time

S.No	Packet Size (KB)	Time Consumption(Decryption)		
		Blowfish	AES	SF Block Cipher
1	49.00	65.00	38.00	61.00
2	59.10	45.00	39.00	43.00
3	100.09	89.00	71.00	79.00
4	247.12	120.00	145.00	112.00
5	321.24	167.00	234.00	168.00
6	694.45	243.00	256.00	212.00
7	899.12	223.00	252.00	259.00
8	963.09	243.00	342.00	206.00
9	5345.15	1224.00	1371.00	1216.00
10	7310.39	1435.00	1443.00	1363.00

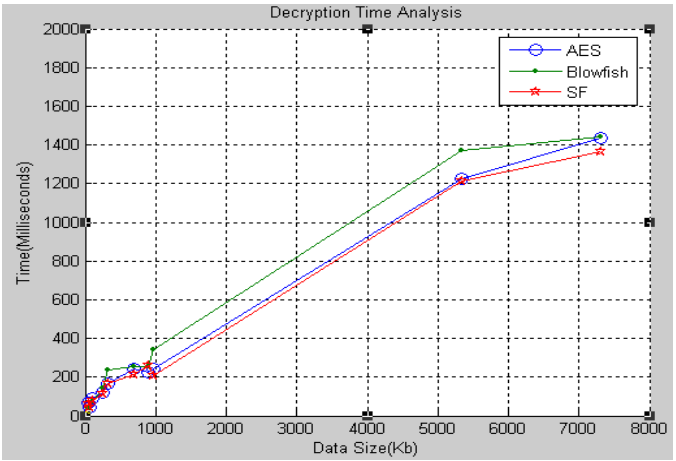

Figure 4 Decryption Analysis

C. Throughput (Encryption and Decryption)

The speed of encryption is defined by the encryption plot's throughput. There is a reduction in the power utilization calculation at the point where the throughput of the encryption calculation expands. Figures 5 and 6 shows the throughput of encryption and unscrambling, respectively. According to the analysis, the proposed scheme has the better throughput when compared to that of the existing models.

Webology, Volume 18, Number 1, 2021
ISSN: 1735-188X
DOI: 10.29121/WEB/V18I1/45

Table 3 Throughput (Encryption)

S.No	Packet Size (KB)	Time Consumption(Encryption)		
		Blowfish	IDEA	SF Block Cipher
1	49	59	78	56
2	59	39	46	38
3	100	94	104	90
4	247	121	134	112
5	321	167	198	164
6	694	234	267	210
7	899	254	342	258
8	963	213	456	208
9	5345	1324	1521	1237
10	7310	1432	1743	1366
Average		**393**	**488.9**	**374**
Throughput		**4.06**	**3.26**	**4.27**

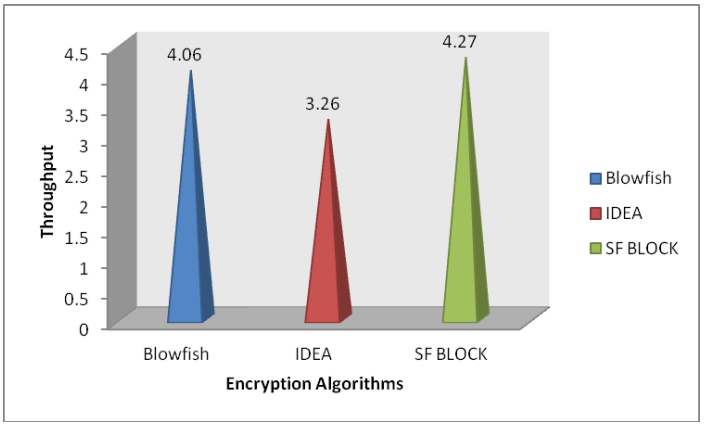

Figure 5 Throughputs (Encryption)

Table 4 Throughput (Decryption)

S.No	Packet Size (KB)	Time Consumption(Decryption)		
		Blowfish	IDEA	SF Block Cipher
1	49	65	78	61
2	59	45	56	43
3	100	89	97	79
4	247	120	131	112
5	321	167	198	168
6	694	243	301	212
7	899	223	378	259
8	963	334	423	309
9	5345	1224	1676	1216
10	7310	1435	1943	1363
Average		**394**	**528**	**382**
Throughput		**4.05**	**3.02**	**4.18**

Webology, Volume 18, Number 1, 2021
ISSN: 1735-188X
DOI: 10.29121/WEB/V18I1/45

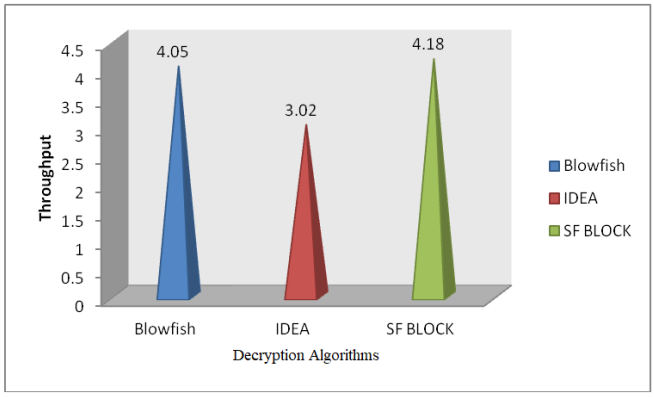

Figure 6 Throughput (Decryption)

Conclusion

Cloud computing has emerged from the concept of distributed software architecture. It plays a vital role in e-health care systems. It provides efficient services for both medical professionals and patients in storage, processing and renewing health related information with good productivity and quality. Even though, the cloud based application provides better solution for health care application but arises several challenges respect to security, confidentiality and privacy of medical information. This paper proposed a cryptographic approach to provide the security for the secure exchange of sensitive information in cloud environments. This research work presented a cryptographic approach for cloud based healthcare applications. The experimental results also show that the proposed model performs well with little overhead in terms of efficiency.

References

1. J. Shen, T. Zhou, D. He, Y. Zhang, X. Sun and Y. Xiang, "Block Design-Based Key Agreement for Group Data Sharing in Cloud Computing," in *IEEE Transactions on Dependable and Secure Computing*, vol. 16, no. 6, pp. 996-1010
2. L. Zhou, V. Varadharajan and M. Hitchens, "Cryptographic role-based access control for secure cloud data storage systems", IEEE Trans. Inf. Forensics Secur., vol. 10, no. 11, pp. 2381-2395.
3. V. Chang and M. Ramachandran, "Towards Achieving Data Security with the Cloud Computing Adoption Framework," in *IEEE Transactions on Services Computing*, vol. 9, no. 1, pp. 138-151.
4. D. Gonzales, J. M. Kaplan, E. Saltzman, Z. Winkelman and D. Woods, "Cloud-Trust—a Security Assessment Model for Infrastructure as a Service (IaaS) Clouds," in *IEEE Transactions on Cloud Computing*, vol. 5, no. 3, pp. 523-536.
5. F. Lombardi and R. Di Pietro, "Secure virtualization for cloud computing", *J. Netw. Comput. Appl.*, vol. 34, no. 4, pp. 1113-1122, 2010.
6. S. Zawoad and R. Hasan, Cloud forensics: A meta-study of challenges approaches and open problems, Feb. 2013,
7. Darren Quick, Kim-Kwang Raymond Choo," Google Drive: Forensic analysis of data Remnants", Journal of Network and Computer Applications, Volume 40, Pages 179-193, April 2014.

Webology, Volume 18, Number 1, 2021
ISSN: 1735-188X
DOI: 10.29121/WEB/V18I1/45

8. Shakya, Subarana. "An efficient security framework for data migration in a cloud computing environment." Journal of Artificial Intelligence 1, no. 01 (2019): 45-53.
9. A. Musa and A. Mahmood, "Client-side Cryptography Based Security for Cloud Computing System," *2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS)*, 2021, pp. 594-600.
10. Gary C. Kessler, "An Overview of Cryptography (Updated Version 3 March 2016)", *Embry-Riddle Aeronautical University - Daytona Beach*, March 2016.
11. N. Sengupta and J. Holmes, "Designing of Cryptography Based Security System for Cloud Computing," *2013 International Conference on Cloud & Ubiquitous Computing & Emerging Technologies*, 2013, pp. 52-57.
12. A. Nhlabatsi *et al*., "Threat-Specific Security Risk Evaluation in the Cloud," in *IEEE Transactions on Cloud Computing*, vol. 9, no. 2, pp. 793-806.
13. A. Rao, N. Carreon, R. Lysecky and J. Rozenblit, "Probabilistic threat detection for risk management in cyber-physical medical systems", *IEEE Softw.*, vol. 35, no. 1, pp. 38-43.
14. K. Lee, "Comments on “Secure Data Sharing in Cloud Computing Using Revocable-Storage Identity-Based Encryption”," in *IEEE Transactions on Cloud Computing*, vol. 8, no. 4, pp. 1299-1300,
15. H. A. Al Hamid, S. M. M. Rahman, M. S. Hossain, A. Almogren and A. Alamri, "A Security Model for Preserving the Privacy of Medical Big Data in a Healthcare Cloud Using a Fog Computing Facility With Pairing-Based Cryptography," in *IEEE Access*, vol. 5, pp. 22313-22328, 2017.
16. M. Anand Kumar and Dr. S. Karthikeyan. 2012. A New 512 Bit Cipher - SF Block Cipher. International. Journal of Computer Network and Information Security. 4(11): 55-61.
17. M. Panda, "Performance analysis of encryption algorithms for security," *2016 International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES)*, 2016, pp. 278-284,
18. A. Banerjee and A. Kundu, "Performance Analysis of Multilingual Encryption for Enhancing Data Security using Cellular Automata based State Transition Mapping: A Linear Approach," *2020 IEEE 1st International Conference for Convergence in Engineering (ICCE)*, 2020
19. S. Vishwakarma and N. K. Gupta, "An Efficient Color Image Security Technique for IOT using Fast RSA Encryption Technique," *2021 10th IEEE International Conference on Communication Systems and Network Technologies (CSNT)*, 2021, pp. 717-722