Journal of Soft Computing Paradigm (JSCP) (2020)
Vol.02/ No. 01
Pages: 24-35
http://irojournals.com/jscp/
DOI: https://doi.org/10.36548/jscp.2020.1.003

Development of Secure Cloud Based Storage Using the Elgamal Hyper Elliptic Curve Cryptography with Fuzzy Logic Based Integer Selection

Dr. A. Pasumpon Pandian,
Professor,
Computer Science Engineering,
KGiSL Institute of Technology,
Coimbatore, India.
Email id: pasumponpandian32@gmail.com

Abstract: The technological advancements in the field of the information and communication technology led to the development of more promising cloud paradigm that allows online provision of services such as platform, software and infrastructure. The infrastructure services provided by the cloud allows the user data to be stored and accessed ubiquitously unlike the arrays that are available on the premises. However the security of the data that are being stored in the internet are still under research. This remains as major inhibitor for the adoption of cloud service in spite of its reliability, elasticity, high computational capabilities and the pay as you go possibilities. So the paper puts forth the construction of a secure storage as service in the cloud computing by utilizing the cryptography system based on Elgamal. The proposed method encrypts the data to be stored using the Elgamal that incorporates the hyper elliptic curve cryptography for twofold encryption and further utilizes the fuzzy logic to perform the integer selection that serves as the significant attribute in defining the cloud storage security. The point addition and the double based ECC is used for generating the keys for the hyper elliptic curve cryptography. The twofold security model put forth is validated using the MATLAB on the terms of efficiency observed on securing the data stored in cloud as well as the cost and the execution time endured by the proposed twofold security. The results shows that the protection offered by the twofold security is much better compared to the prevailing.

Keywords: Cloud Paradigm, Storage as Service, Security Challenges, Two Fold Security, Elgamal, HECC, Fuzzy Logic

1. Introduction

The technological growth that has caused tremendous enhancements in the way of humans and the day today activities in turn generates huge amount of information’s that hold valuable insights. For e.g. the information’s generated through the wireless sensor networks, social networks, images streamed from satellites etc., therefore it becomes necessary to store information’s such that they could be accessed ubiquitously irrespective of time and place.

This was made possible with the evolution of the cloud paradigm that rendered services on pay as go model. The infrastructure as service provided by the cloud allowed the information's to be stored, managed, and maintained remotely. The cloud also allowed its users to access the data from anywhere at any time. It utilizes the web as well as the centralized servers located remotely to back up the information's of the users. It also allows the users and the organizations adopted to it to use the applications without establishing it but accessing their own documents, this invention makes significantly more efficient processing by concentrating energy, memory, handling and velocity transfer. The three major service models defined by the "national institute standards and technology" for the cloud computing are SaaS-Software as service, PaaS- platform as service, IaaS- Infrastructure as service SaaS is closely linked to the application service provider (ASP) and the device distribution models on demand for computing. SaaS ' hosted application management model is similar to ASP, where the provider hosts the software of the customer and delivers it over the internet to licensed end-users and IaaS provides the infrastructures as service, for e.g. it provides the storage facilities, data center space along with the servers and the network components. Some of the examples are Cisco Metapod, Digital Ocean, Amazon Web services, Microsoft Azure etc. whereas the platform as service provides the complete platform that is essential in constructing an organization , so this type of services completely eludes the investments cost and the maintenance cost that is essential for the organization. The figure.1 below show the service delivered by the cloud.

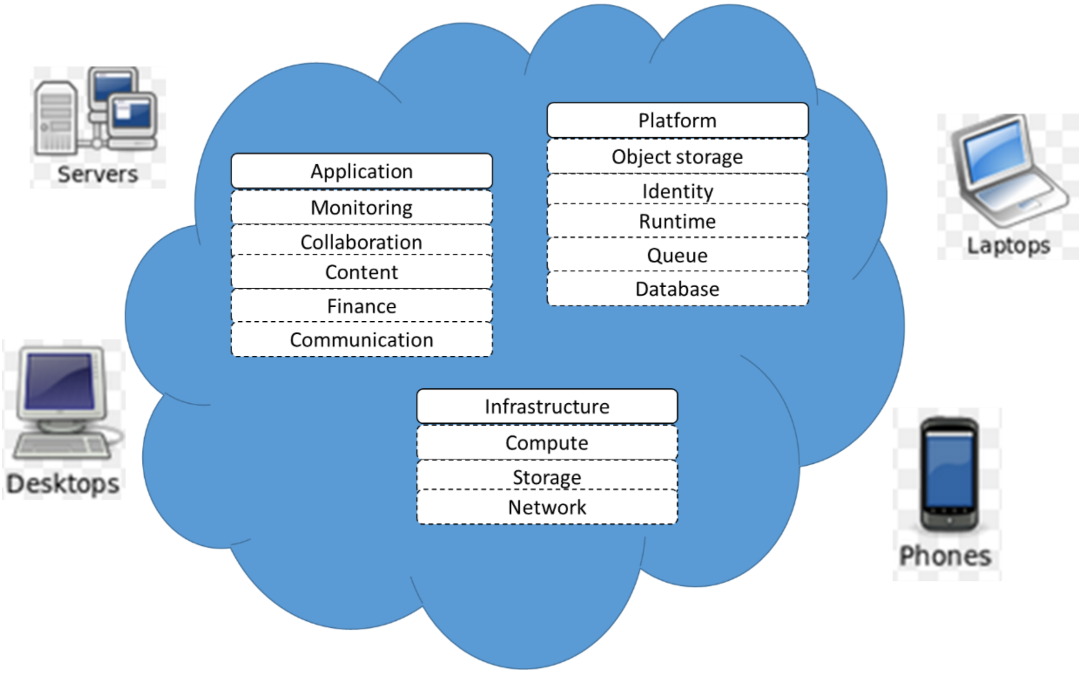


Figure.1 Cloud Services

Though the cloud provides a cost effective and the convenient service, the security provisions of the cloud storage as service are still questionable and under research, they storage provided by the cloud are liable of being attacked by the common attackers or hackers as it has the personal information's of many organizations and individuals. So securing the information becomes essential, on the cloud storage, though different traditional methods and methods such as identity based cryptography, chaos based cryptography model, and DNA based cryptography are followed currently, the paper tries to develop a more secure cloud storage utilizing the two fold cryptography devised incorporating the Elgamal and the Hyper Elliptic curve cryptography. This is procedure to formulate a cryptography based on two fold is piled with the related works in the section 2, the proposed work in section 3, the performance analysis in section 4 and the Conclusion in section 5 followed by the references.

2. Related works

Jabernet al [1] elaborates the use of securing the data in the cloud databases using the cryptography, Li, et al [2] address the security issues in the cloud computing utilizing the cryptography that is accomplished based on identity. Mugunthan et al [3] shows the effective cryptographic methods utilization in the localization of the data observed using the wireless sensor networks that re engaged in the internet of things Rahmani et al [4] proposes an encryption as service to secure the data stored in the cloud.

Bhalaji, et al [5] puts forth the "Efficient and Secure Data Utilization in Mobile Edge Computing by Data Replication. The author Tobin et al [6] in his paper proposes an "Chaos-based cryptography for cloud computing." Suma, V et al [7] proposes the block chain in securing and maintaining the privacy of the information's stored in the cloud. Belej et al [8] proposes the "The cryptography of elliptical curves application for formation of the electronic digital signature." The figure.2 below shows the single encryption followed in the current systems

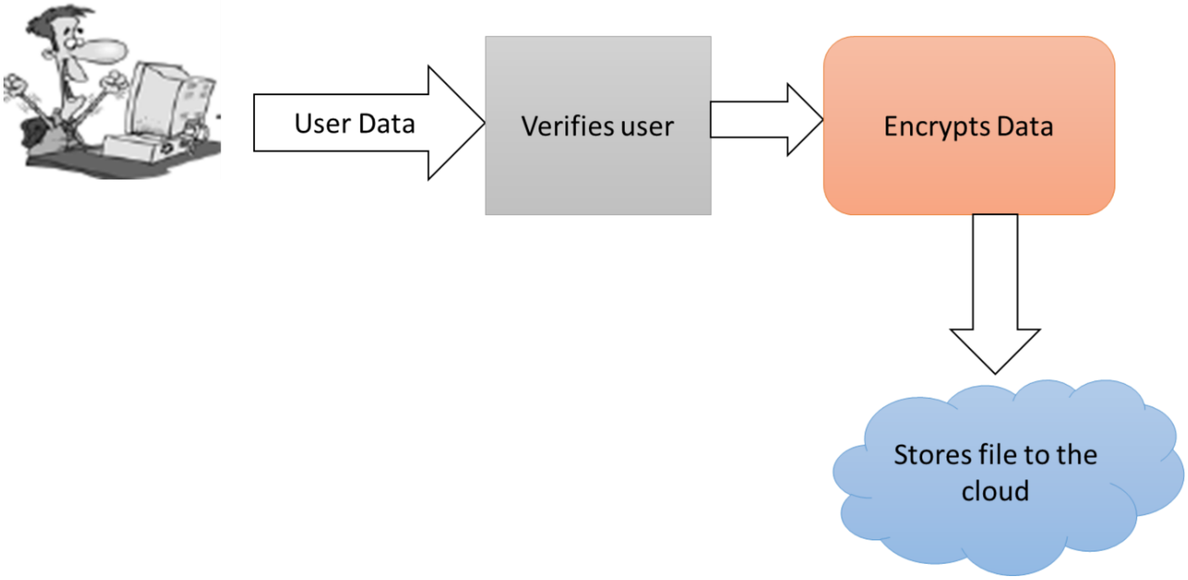


Figure.2 Encryption in cloud

Smys, S. et al [9] presents the "DDOS Attack Detection in Telecommunication Network Using Machine Learning." R. Shanmugalakshmi et al [10] provides the "Fault Analysis Attacks and Its Countermeasure using Elliptic Curve Cryptography." Haoxiang et al [11] proposes the "Trust Management of Communication Architectures of Internet of Things." Barkha et al [12] puts forward the "Implementation of DNA cryptography in cloud computing and using socket programming."

Shakya et al [13] proposes the. "An Efficient Security Framework For Data Migration In A Cloud Computing Environment." Shahzadi, etal [14] proposes the Security of Cloud Computing Using Adaptive Neural Fuzzy Inference System." And Mugunthan, S. R et al [15] puts forth the "Soft Computing Based Autonomous Low Rate DDOS Attack Detection and Security for Cloud Computing."

R. Kavitha et al [16] proposes the "Medical big data analysis: preserving security and privacy with hybrid cloud technology." Ramakrishnan, S et al [17] proposes the. “Cryptographic and Information Security Approaches,” Mosola et al [18] proposes the "Client-side encryption and key management: enforcing data confidentiality in the cloud."

The paper puts forth the construction of a secure storage as service in the cloud computing by utilizing the cryptography system based on Elgamal. The proposed method encrypts the data to be stored using the

Elgamal that incorporates the hyper elliptic curve cryptography for twofold encryption and further utilizes the fuzzy logic to perform the integer selection that serves as the significant attribute in defining the cloud storage security. The point addition and the double based ECC is used for generating the keys for the hyper elliptic curve cryptography.

3. Proposed work

The virtualization of the resources in the cloud computing has made it more cost efficient and prominent area of research. Recently the business, the organizations and many institutions depends on the cloud service for, software, platform and infrastructure to elude the investment and maintenance cost. However it is open to common attacks and hacks as the services are rendered over internet, this paves way for constructing a security frame work for the cloud paradigm. Using the proposed frame work the user initially encrypts his data and with the proper integer selection that is out forth by the fuzzy rule system that is operates based on the Mamdani's method, and once again encrypts the data employing the hyper elliptic cryptography where the point addition and the double based ECC is used for generating the key

The flow diagram below provides the stage of the proposed process to secure the data stored in the cloud.

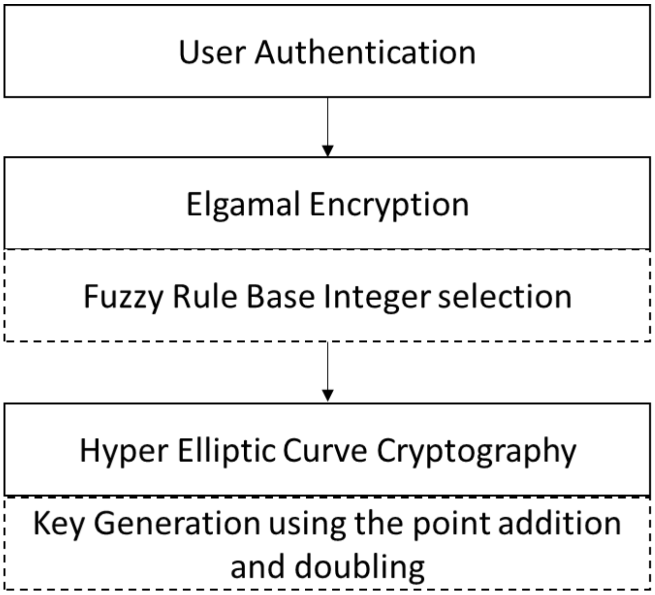
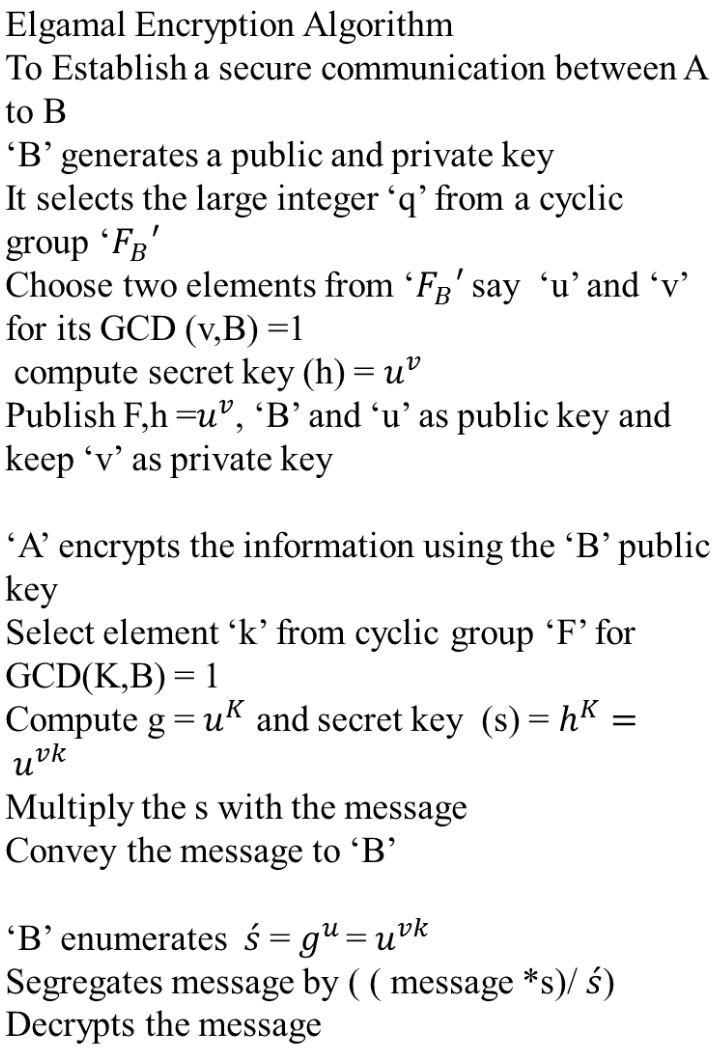

User Authentication
Elgamal Encryption
Fuzzy Rule Base Integer selection
Hyper Elliptic Curve Cryptography
Key Generation using the point addition and doubling

Figure.3 Proposed Flow

To start with the proposed model of two fold cryptography the algorithm that describes the Elgamal procedure with the two fuzzy based integer selection is discussed. The Elgamal is a cryptosystem that follows the public key cryptography, and utilizes the asymmetric key encryption for extending communication across the two members. The cryptosystem relies on the complexity of identifying discrete logarithm in a cyclic. Such even on knowing the two keys the computing the secret key is difficult in case of the Elgamal encryption, it is usually very advantageous when encrypting a larger size messages. The figure .4 below provides the Elgamal encryption algorithm, when sharing an information to the other device.



Elgamal Encryption Algorithm
To Establish a secure communication between A to B
‘B’ generates a public and private key
It selects the large integer ‘q’ from a cyclic group ‘F_B'
Choose two elements from ‘F_B' say ‘u’ and ‘v’ for its GCD (v,B) =1
compute secret key (h) = u^v
Publish F,h =u^v, ‘B’ and ‘u’ as public key and keep ‘v’ as private key

‘A’ encrypts the information using the ‘B’ public key
Select element ‘k’ from cyclic group ‘F’ for GCD(K,B) = 1
Compute g = u^K and secret key (s) = $h^K = u^{vk}$
Multiply the s with the message
Convey the message to ‘B’

‘B’ enumerates $ś = g^u = u^{vk}$
Segregates message by ((message *s)/ $ś$)
Decrypts the message

Figure.4 Elgamal Algorithm

The integer selection from the cyclic group is done using the Mamdani fuzzy rule system that relies on the simple structures of the Min-Max operations, it evaluates the optimal value applying the triangular and the trapezoidal function and estimates the optimal value as integer to enhance the security in the cloud storage. Using the Elgamal the equations 1 and 2 shows the triangular and the trapezoidal functions respectively.

$$\mu_A(x) = \begin{cases} 0 & x \leq a \\ \frac{x-a}{m-a} & a \leq x \leq m \\ \frac{b-x}{b-m} & m < x < b \\ 0 & x \geq b \end{cases} \tag{1}$$

$$\mu_A(x) = \begin{cases} 0 & x < a \; or \; x > d \\ \frac{x-a}{b-a} & a \leq x \leq b \\ \frac{d-x}{d-c} & c \leq x \leq d \\ 1 & b \leq x \leq c \end{cases} \tag{2}$$

The optimal value with the highest ranking in the cyclic group is selected applying the fuzzy rules. This enhances the security of the information that is stored in the cloud, the second level of security is provided by encrypting the information further using the hyper elliptic curve cryptography. The hyper-ECC uses the point addition and the doubling method for generation of the key.

The hyper-ECC further encrypts the data selecting a random number ‘h’ from the set of ‘N’ numbers, where co-ordinate ‘c’, where ‘c’ is the product of the random prime number and the HECC divisor ‘D’, now a supplementary key is added, in order to encrypt the information’s, the co-ordinate is represented as the product of the supplementary key and the ‘hD’ the supplementary key is determined using the point addition and the doubling. The point addition and the doubling achieved as shown in the equation 3 and 4below

$$P_A = \frac{y2-y1}{x2-x1} |p| if \; X \neq Y \tag{3}$$

Where the ‘x’ and ‘y’ are co-ordinates on the curves, ‘X’ = {x1, y1) and Y = {x2, y2}, ‘p’ random number

$$P_D = \frac{3x1^2+a1}{2y1}|p|\ if\ X = Y \qquad (4)$$

Where ‘a ‘is a random number, based on the equations 3and 4 the key is estimated and the message is encrypted. The message by double encryption remains secured in the cloud storage. The equation 5 is framed in this regard, the equation 5 shows the message encrypted (E_M) through the HECC

$$E_M = \text{Message + supplementary key (hD)} \qquad (5)$$

And the message is decrypted (D_M) is obtained by subtracting the ‘supplementary key (hD)’ form the E_M as shown in equation 6

$$D_M = E_M - \text{Supplementary key (hD)} \qquad (6)$$

4. Performance Analysis

The proposed method with the two fold encryption is implemented with the python and evaluated using the MATLAB for the varying number of users who prefer the cloud storage. The results were analyzed in the terms of level of security provided by the proposed method, the cost of the computation and storage and the execution time. The results obtained were compared with the existing security provisions that relied on the identity based cryptography [2] and the chaos based cryptography [6] to prove the competence of the two fold security that was used in the securing the information’s.

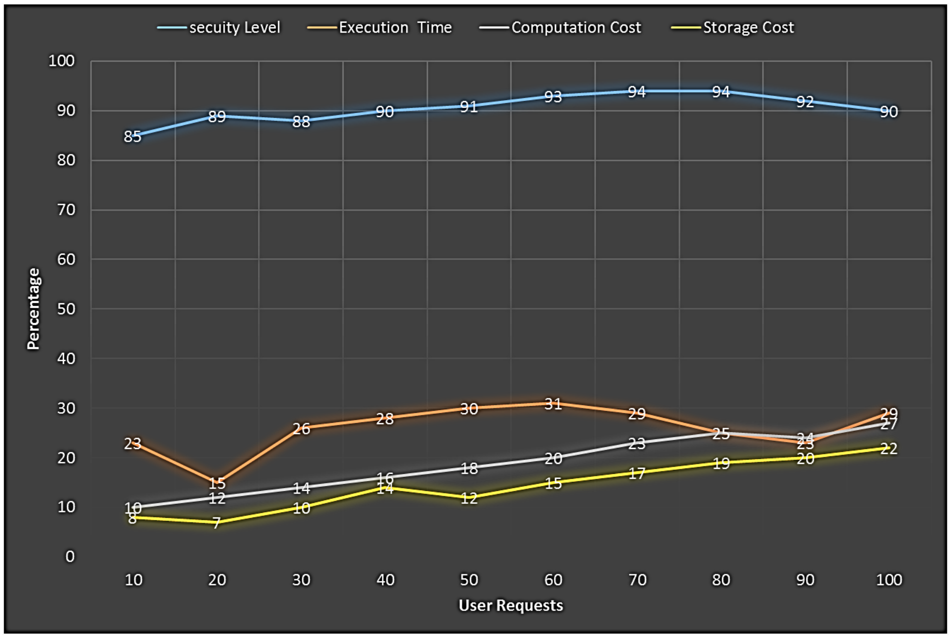


Figure.5 performance measure

The results observed on the amount of security provided over the proposed method and the cost incurred on the computation and the storage provided by the cloud and the time taken to execute the complete task shows that the two fold security with the fuzzy based integer selection is much better compared to the exiting cryptography system that identity on the identity and the chaos.

Number of user request	Two-fold cryptography			Identity Based Cryptography			Chaos based Cryptography		
	Security level in %	Cost in $	Execution time in seconds	Security level in %	Cost in $	Execution time in seconds	Security level in %	Cost in $	Execution time in seconds
10	85	18	.034	45	25	.2345	56	45	.985
20	89	20	.0567	44	30	3456	45	59	.976
30	88	23	.0799	50	35	.567	57	67	.997
40	90	25	.0987	53	40	.789	59	70	1.09
50	91	27	.1237	49	45	.856	60	73	1.2345
60	93	29	.1567	48	46	.879	63	56	1.0
70	94	30	.1678	47	47	.987	65	72	1.567
80	94	33	.1123	53	49	1.0234	50	71	1.423
90	92	32	.1724	52	54	1.567	55	70	1.895
100	90	30	.1346	51	55	1.2346	57	74	1.956

Table.1 Comparative Analysis

The table.1 above is the comparative analysis the presents the results observed for the two fold security with the fuzzy based integer selection and the Hyper-ECC that was put forth in the paper and the two existing methods of cryptosystem that relied on the identity and the chaos. The results were observed for varying number of user request that demand for a cloud storage.

5. Conclusion

To enhance the security of the data stored in the cloud the paper puts forth the twofold security that ensures the security provisioning of the cloud for the stored data by constructing a cryptosystem that relies on double encryption. The two level of security put forth utilizes the Elgamal encryption with the integer selection based on fuzzy logic and the hyper-ECC that relies on the point addition and the doubling for key generation to secure the information's in two fold. The cryptosystem was implemented in the python and evaluated using the MATLAB, the results observed shows that the two level of security put forth has a very high performance in terms of security, execution time and cost associated with the computation and storage compared to the exiting methods with the cryptography that is achieved with the identity and the chaos.

References

[1] Jaber, Aws Naser, and Mohamad Fadli Bin Zolkipli. "Use of cryptography in cloud computing." In *2013 IEEE International conference on control system, computing and Engineering*, pp. 179-184. IEEE, 2013.

[2] Li, Hongwei, Yuanshun Dai, and Bo Yang. "Identity-Based Cryptography for Cloud Security." *IACR Cryptology ePrint Archive* 2011 (2011): 169.

[3] Mugunthan, S. R. "Security and Privacy Preserving Of Sensor Data Localization Based On Internet Of Things." *Journal of ISMAC* 1, no. 02 (2019): 81-91.

[4] Rahmani, Hossein, Elankovan Sundararajan, Zulkarnain Md Ali, and Abdullah Mohd Zin. "Encryption as a Service (EaaS) as a Solution for Cryptography in Cloud." *Procedia Technology* 11, no. 2013 (2013): 1202-1210.

[5] Bhalaji, N. "Efficient And Secure Data Utilization In Mobile Edge Computing By Data Replication." *Journal of ISMAC* 2, no. 01 (2020): 1-12.

[6] Tobin, Paul, Lee Tobin, Michael Mc Keever, and J. Blackledge. "Chaos-based cryptography for cloud computing." In *2016 27th Irish Signals and Systems Conference (ISSC)*, pp. 1-6. IEEE, 2016.

[7] Suma, V. "Security and Privacy Mechanism Using Blockchain." *Journal of Ubiquitous Computing and Communication Technologies (UCCT)* 1, no. 01 (2019): 45-54.

[8] Belej, Olexander. "The cryptography of elliptical curves application for formation of the electronic digital signature." In *International Conference on Computer Science, Engineering and Education Applications*, pp. 43-57. Springer, Cham, 2019.

[9] Smys, S. "Ddos Attack Detection In Telecommunication Network Using Machine Learning." *Journal of Ubiquitous Computing and Communication Technologies (UCCT)* 1, no. 01 (2019): 33-44.

[10] Prabu, M., and R. Shanmugalakshmi. "Fault Analysis Attacks and Its Countermeasure using Elliptic Curve Cryptography." *International Journal of Computer Science & Information Security* (2010).

[11] Haoxiang, Wang. "Trust Management Of Communication Architectures Of Internet Of Things." *Journal of trends in Computer Science and Smart technology (TCSST)* 1, no. 02 (2019): 121-130.

[12] Barkha, Prajapati. "Implementation of DNA cryptography in cloud computing and using socket programming." In *2016 International Conference on Computer Communication and Informatics (ICCCI)*, pp. 1-6. IEEE, 2016.

[13] Shakya, Subarna. "An Efficient Security Framework For Data Migration In A Cloud Computing Environment." *Journal of Artificial Intelligence* 1, no. 01 (2019): 45-53.

[14] Shahzadi, Shumaila, Bushra Khaliq, Muhammad Rizwan, and Fahad Ahmad. "Security of Cloud Computing Using Adaptive Neural Fuzzy Inference System." *Security and Communication Networks* 2020 (2020).

[15] Mugunthan, S. R. "Soft Computing Based Autonomous Low Rate DDOS Attack Detection And Security For Cloud Computing." *Journal of Soft Computing Paradigm (JSCP)* 1, no. 02 (2019): 80-90.

[16] Shanmugapriya, E., and R. Kavitha. "Medical big data analysis: preserving security and privacy with hybrid cloud technology." *Soft Computing* 23, no. 8 (2019): 2585-2596.

[17] Ramakrishnan, S. *Cryptographic and Information Security Approaches for Images and Videos*. CRC Press, 2018.

[18] Mosola, Napo Nathnael. "Client-side encryption and key management: enforcing data confidentiality in the cloud." PhD diss., 2016.