Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 27 (2024), No. 2-B, pp. 625–637
DOI : 10.47974/JDMSC-1889

Hybrid bioinspired approach for secret sharing algorithm and ownership transfer optimization in cloud based models

Himanshu V. Taiwade *
Premchand B. Ambhore
Department of Computer Science and Engineering
Government College of Engineering
Amravati
Maharashtra
India

Abstract

It is widely accepted that secret sharing models like Shamir cryptosystem allows cloud designers to deploy highly secure multichannel data transfer mechanisms. But these systems are majorly static, and do not incorporate context-aware share-selection techniques. Moreover, SaaS based cloud deployments require ownership transfers for efficient real-time operations. These ownership transfer mechanisms are backed by selection encryption models assisting in permission-aware data sharing. Scholars have put forward pre-emptive and bioinspired models to accomplish these tasks, but nearly all of them are still sophisticated or demonstrate limited flexibility in real-time scenarios. The proposed structure first gathers cloud logs for various temporal requests and groups them based on IP & resource constraints with the goal of getting around these problems. The modified rules are initially tested on dummy ownership requests, and are later on real-time ownership-transfer scenarios for validation of their efficiency levels based on accuracy of misconfiguration detection, delay needed for processing the requests, consistency of blocking invalid ownership requests, and request throughput levels. Based on this evaluation, The accuracy might be increased by 3.5% using the suggested model, reducing delay by 2.9%, while having 6.4% higher consistency, and 8.3% higher throughput than existing secret sharing & ownership transfer methods under similar deployment scenarios.

Subject Classification: *68M25.*

Keywords: *Secret-sharing, Encryption, GWO, Cloud models, QoS (Quality of Service), Bioinspired models.*

* *E-mail:* himanshu.taiwade@gmail.com

1. Introduction

Cloud storage has recently emerged as a topic of intense academic interest in the field of information storage. The widespread use of software-as-a-service and cloud computing is primarily to blame for this [1, 2]. Both software as a service and cloud computing have emerged as significant trends in the information storage sector in recent years that support threshold changeable secret sharing scheme (TCSS) for encryption operations. Unlike traditional storage hardware, which consists of up of servers, network devices, storage devices, application software, public access interfaces, access networks, and client applications, cloud storage is a multi-component system. This makes the construction of users' own data centers obsolete. Users are not obliged to make expensive investments in the infrastructure's hardware and software, nor are they forced to develop redundant storage platforms for themselves [3, 4] that use Physical unclonable function with Shamir Sharing (PUFS). However, a large number of companies and individuals are reluctant to trust third-party service providers with their sensitive data due to worries over both the data's security and its usefulness. The government's surveillance is not open to public scrutiny, and there are no protections in place to secure individuals' personal information [5]. The simplest way to guarantee the confidentiality of data while it remains on a single cloud server is to encrypt it on the client before uploading it to the cloud and to decode it once it has been received. This is true in spite of the fact that the data are encrypted. However, using this technique necessitates the development and maintenance of a large number of keys, which substantially raises the bar for the required level of computational complexity [6, 7]. The cloud storage service will be completely worthless in the event that a natural disaster or any other disruption occurs, and there is a possibility that the data may not even be retrievable. One of the most significant limitations of a cloud storage system that just consists of one server is this limitation. An option that is gaining in popularity and is called as a distributed cloud may overcome the problems that were described before that are associated with cloud storage solutions that use only one server [7]. In addition, research [9, 10] conducted on distributed computing via Attribute-Based Encryption and Proxy Re-Encryption (ABE PRE) has led to the development of a wider variety of applications that may be used with distributed cloud computing. This ensures that no other method may be used to obtain the original data [11]. The growing need for more secure ways to store digital data led to the creation of this new type of cloud storage system. This requirement specifically addressed the increasing popularity of cloud

computing. A secret trading strategy based on multidimensional space point properties and the Lagrange interpolation approach was discovered in 1979 [12, 13]. This method was developed by two distinct individuals. The participants all have access to the same secret material, but only those with at least k other participants will be able to decipher it. Unlike the traditional method of encrypting data, secret sharing does not require encryption keys; however, the drawbacks of this approach include multiple times the original data's storage overhead, more complex coding and decoding, and a substantial amount of random data generation. The standard encryption technique requires encryption keys in order to guarantee data security. Consequently, its exclusive use during that period was to serve as a medium for the long-distance storage of comparatively modest quantities of data, including encryption keys [14]. The notions of secret sharing and erasure coding have emerged as a result of this problem in networked storage. It is now generally acknowledged as a basic cryptographic technique and is a component of many secure protocols, such as secure multiparty computing and threshold cryptography. Finally, Shamir's technique was refined to MDS (Maximum Distance Separable) array codes [10], [15], when he created a stunning and successful perfect threshold method [15] by polynomial interpolations. [10] gives an explanation. The fact that n minus k equals a number of constants describes this code. Therefore, the lowest bound of the information theory is equal to 1/n, the number of data required to reconstruct an erased column. This is information theory's lowest bound (n minus k). Following the previous part is one in which a hybrid bioinspired model is suggested with the intention of improving the performance of secret sharing in cyber physical cloud installations that are based on ownership transfer scenarios. In the third and last section of this paper, the model was validated by comparing its performance to that of other models that had been implemented in situations that were equivalent to those that were being investigated. In conclusion, this paper provides several deployment-specific observations concerning the proposed model along with proposals for additional enhancements for facilitating real-time use cases.

2. Architecture of the suggested hybrid Bioinspired Model for optimizing Secret sharing attainment of Ownership-transfer-based cyber physical Cloud deployments

As per the review of exiting security models, it can be observed that these models are majorly static, and do not incorporate context-aware share-selection techniques. Researchers have proposed pre-emptive and

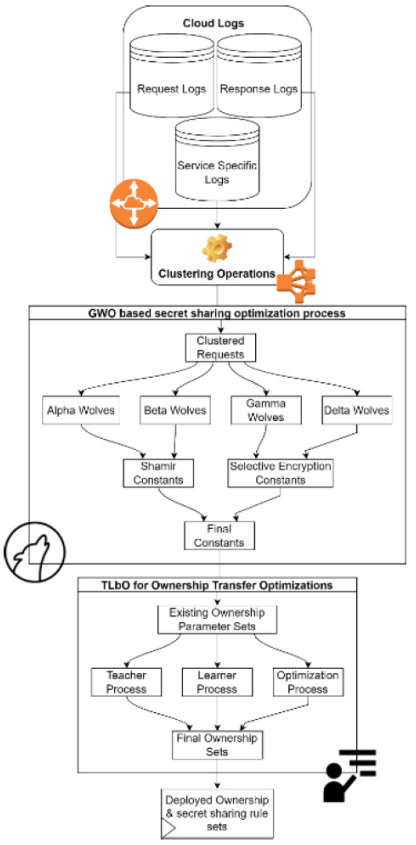

Figure 1

Design of the proposed secret sharing & selective encryption model with ownership transfer optimizations

bioinspired models for carrying out these tasks, however, these frameworks are either highly sophisticated or exhibit little flexibility in real-time scenarios. This section addresses the development of a hybrid bioinspired model for enhancing ownership-transfer-based cyber-physical cloud installations' secret sharing performance in an attempt to get past these issues.

The suggested model's flow is shown in Figure 1, wherein it is obvious that the model first collects cloud logs for different temporal demands and classifies them according to IP and resource limitations. These logs help

distinguish requests with low computing needs from ones with high computational needs. The model trains a Grey Wolf Optimizer (GWO) to select secret sharing parameters based on this separation, that assists in improving QoS (Quality of Service) levels while maintaining high security levels. The secret sharing configuration parameters identified by GWO are used to train a Teaching-Learning based Optimizer (TLbO), which assists in reconfiguration of ownership transfer rules. The modified rules are initially tested on dummy ownership requests, and are later applied to real-time ownership-transfer scenarios for validation of their efficiency levels.

To perform these tasks, the model extracts following cloud log entities,

- IP addresses of requesting entities
- Resources requested by these entities
- Response time for each resource access
- Status of response (Valid or Invalid)

Based on these metrics, a k Means based clustering process is deployed, which assists in separation of these requests into low & high computational requirement requests. These computational requirements (CRs) are estimated for all 'Valid' requests via equation 1,

$$CR_{IP} = \sum_{i=1}^{N_{req}} \frac{RT_i}{Max(RT)} * \frac{S_i}{Max(S)} * \frac{NR_i}{Max(NR)} \quad \ldots(1)$$

Where, RT, S & NR represents response time, size of request, and number of resources needed to process these requests, when each IP is sending N_{req} individual requests. kMeans groups all "Valid" IP requests by picking random starting centroids based on these CR values. Due to the random nature of the selection procedure, the results of this clustering method vary from run to run and iteration to iteration. These clusters assist in identification of Shamir's secret sharing constants. These constants include, number of shares (n), and number of recovery shares (k), which must be decided for individual clusters to provide contextual security under real-time use cases. An optimizer based on GWO is utilised to complete this operation, and it operates in the manner described below,

- Setup of the GW Optimizer is done by initializing the following constants,
  - o Total iterations that will be used to reconfigure Wolves (N_i)

- Total Wolves that will be reconfigured during these iterations (N_w)
- Individual Wolf learning rates (L_w)

- For individual clusters, estimate N_w Wolf configurations via the following process,
  - Estimate values for n & k via equations 2 & 3 as follows,

$$k = STOCH(L_{w_i} * \underline{CR_{IP}}, \underline{CR_{IP}}) \quad \ldots(2)$$

$$n = STOCH(k, \underline{CR_{IP}}) \quad \ldots(3)$$

Where, *STOCH* is a Markovian process used to generate stochastic number sets, and $\underline{CR_{IP}}$ represents the average computational requirements for individual clusters.

  - As per these values of k, n apply Shamir Encryption for $n + k$ dummy requests via equation 4,

$$S(x) = \sum_{i=1}^{n} \left[s(x_i) \prod_{j=1, j \neq i}^{n} \frac{x - x_j}{(x_i - x_j)} \right] \bmod p \quad \ldots(4)$$

Where, x & p are the input data and a prime number which is larger than both n & k value sets.

  - These data samples are decrypted as per equation 5,

$$s(x) = (M + s_1 * x + s_2 * x^2 + \ldots + s_{n-1} * x^{k-1}) \bmod p \quad \ldots(5)$$

Where, $s_1, s_2, \ldots s_{n-1}$ are stochastic numbers between 1 and $p-1$

  - Based on these processes, estimate Wolf fitness via equation 6,

$$f_w = \sum_{i=1}^{n} \frac{d_i}{Max(d)} * \frac{1}{n * len(S_i)} \quad \ldots(6)$$

Where, d represents the delay needed to perform encryption & decryption operations.

  - Generate such Wolf configurations for individual clusters.

- Once all Wolves are generated, then estimate Wolf fitness threshold via equation 7,

$$f_{th} = \sum_{i=1}^{N_w} f_{w_i} * \frac{L_{r_i}}{N_w} \quad \ldots(7)$$

- Using this threshold level, modify Wolf status as follows,
  - o Change Wolf to 'Alpha', if $f < \frac{f_{th}}{2}$
  - o Otherwise, Change Wolf to 'Beta', if $f < f_{th}$, and modify its learning rate as per equation 8,

$$L_w(New) = L_w(Old) + \frac{L_w(Old) - \underline{L_w(Alpha)}}{\underline{L_w(Alpha)}} \quad \ldots(8)$$

Where, $\underline{L_w(Alpha)}$ is the average learning rate of all 'Alpha' Wolves

  - o Otherwise, Change Wolf to 'Gamma', if $f > L_w * f_{th}$, and modify its learning rate as per equation 9,

$$L_w(New) = L_w(Old) + \frac{L_w(Old) - \underline{L_w(Beta)}}{\underline{L_w(Beta)}} \quad \ldots(9)$$

Where, $\underline{L_w(Beta)}$ is the average learning rate of all 'Beta' Wolves

  - o Else, change Wolf to 'Delta' and modify its learning rate as per equation 10,

$$L_w(New) = L_w(Old) + \frac{L_w(Old) - \underline{L_w(Gamma)}}{\underline{L_w(Gamma)}} \quad \ldots(10)$$

Where, $\underline{L_w(Gamma)}$ is the average learning rate of all 'Gamma' Wolves

  - o Repeat this process for all iterations.

Following the completion of all iterations, choose Wolf with the lowest fitness and utilise its (k,n) values to encrypt the data using the Shamir secret sharing procedure.

Once the data communication is initialized, then Ownership Transfer requests can arrive from different IP addresses. These requests are processed via a Teacher-Learner based Optimization (TLbO) Model, which works as per the following process,

- Initiate the learning process by setting up the following constants,
  - o Total Particles used for processing ownership requests (N_p)
  - o Total iterations for which these particles will be analyzed (N_i)
  - o Individual learning rate for these particles (L_r)

- For every ownership request, estimate the following parameter sets,
  - o Cluster number of the IP
  - o Packet size of the requests (PS)
  - o Previous request status (R_{stats})
- Estimate the fitness of this request via equation 11,

$$f = CR_{IP} * \frac{PS}{Max(PS)} * \underline{R_{stats}} \quad \ldots(11)$$

- Now, generate N_p particles as per the following process,
  - o Stochastically select N node IPs from the network, and segregate them into $\frac{N}{2}$ invalid request IPs, and $\frac{N}{2}$ valid request IPs
  - o From each of these IPs, send ownership requests for the same resource, and estimate their average fitness levels via equation 12,

$$f(New) = \frac{2}{N}\sum_{i=1}^{\frac{N}{2}} CR_{IP_i} * \frac{PS_i}{Max(PS)} * \underline{R_{stats_i}} \quad \ldots(12)$$

    This value is estimated for both 'Valid' and 'Invalid' IP addresses.
  - o Find fitness of this particle via equation 13,

$$f_p = \frac{f}{f(New)_{valid}} + \frac{f(New)_{invalid}}{f} \quad \ldots(13)$$

  - o After doing this for each particle, use equation 14 to find the fitness threshold,

$$f_{th} = \sum_{i=1}^{N_p} f_{p_i} * \frac{L_{r_i}}{N_p} \quad \ldots(14)$$

  - o As per this threshold level, mark particle as 'Teacher' when $f < f_{th}$, else mark it as 'Student'
- After each iteration, modify learning rate of each 'Student' particle as per equation 15,

$$L_r(New) = L_r(Old) + \frac{L_r(STOCH(Teacher))}{Max(L_r(Teacher))} \quad \ldots(15)$$

Where, $L_r(Teacher)$ represents learning rate for 'Teacher' particles.

To create new "Teacher" and "Learner" combinations, this process is repeated for every iteration while particles are updated continually.

After the iterations are over, the 'Teacher' particle with least fitness is picked and verified for approval of ownership transfer status. This is done with the help of equation 16,

$$f(Teacher) < 1 \quad \ldots(16)$$

If this condition is true, then the current ownership request closely matches 'Valid' requests, and thus can be passed to the cloud for further processing operations. Otherwise, this request is blocked, and next request is evaluated via the TLbO process.

3. Result evaluation and comparative analysis

The presented secret sharing & ownership transfer optimization model uses a combination of clustering, GWO and TLbO for processing data and control requests. All data requests are initially processed via the GWO Model, which assists in selection of secret sharing keys for the Shamir cryptosystems. These keys are selected based on low delay and high security operations, which assists in improving speed, while ensuring higher safety against data-level attacks. The model is further optimized for all control (ownership transfer) requests, with the help of TLbO based optimizations. The suggested framework could improve QoS performance while maintaining information & control-level security for real-time requests because of these optimisations. The model's performance was confirmed against three distinct attack types: Man-in-the-Middle (MITM), Distributed Denial of Service (DDoS), and Worm Hole (WH). This performance was evaluated on the Network Simulator (NS2.34), under the following network conditions,

As per these network configurations, the values for end-to-end delay (D), packet delivery ratio (PDR), throughput (T), and energy (E) needed for communications. These parameters were evaluated under 5000 different Number of Communication Sequences (NCS), with 3% WH, 3% DDoS, and 4% MITM communication requests. Due to which during every set of evaluation, 10% of all requests were attacks. Under these attacks, QoS levels were estimated and compared with TCSS [2], PUFS [3], and ABE PRE [9] which were referred under similar scenarios. Based on this strategy, the communication delay can be observed as in the Figure 2.

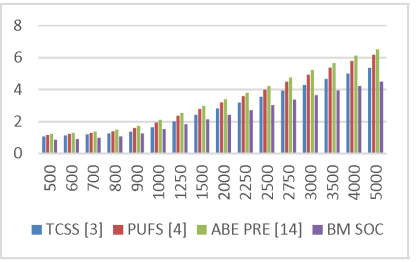

Figure 2

Communication delay under 10% attack nodes for different models

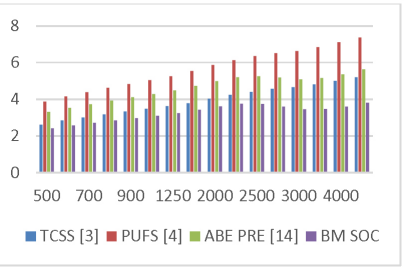

Figure 3

Communication energy needed under 10% attack nodes for different models

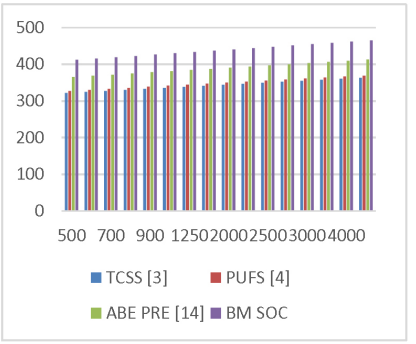

Figure 4

Communication throughput under 10% attack nodes for different models

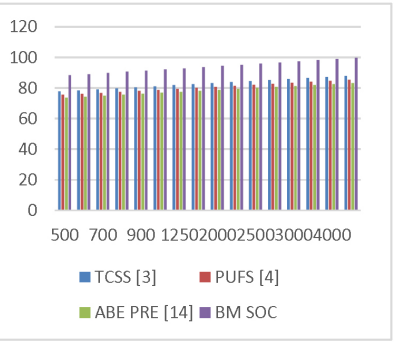

Figure 5

Communication PDR under 10% attack nodes for different models

According to this assessment and Figure 2, the proposed dual bioinspired model can be useful for high-speed deployments because it may reduce communication delay levels by 19.5% when compared with TCSS [2], 26.4% if compared with PUFS [3], and 29.8% when compared with ABE PRE [9]. This delay is reduced due to use of a high-efficiency Shamir cryptosystem with delay-aware key values, which assists in improving its QoS performance even under attacks. In the same way, Figure 3 shows the energy levels.

According to this examination and Figure 3, the proposed dual bioinspired model may reduce energy consumption levels by 8.5% in contrast with TCSS [2], 16.4% in contrast to PUFS [3], and 13.2% in contrast to ABE PRE [9], rendering it a useful instrument for high lifetime

deployments. Through the application of the TLbO approach, enabling it to reduce dependence on supervised learning procedures and provide quicker and more efficient ownership decisions, this energy consumption is minimised. Similar to this, Figure 4 shows the throughput.

The implementation of the GWO & TLbO method, allowing the model to optimize ownership transfer and secret sharing performance in real-time scenarios, is what is responsible for this throughput improvement. Similar to this, Figure 5 shows the PDR.

Figure 5 and this evaluation indicate that the suggested dual bioinspired model may enhance communication PDR by 10.3%, 14.5%, and 16.4% with regard to PUFS [3], ABE PRE [9], and TCSS [2]. This indicates that the model is useful for high-consistency deployments.

4. Conclusion and future scope

The proposed secret sharing and ownership transfer optimization model processes data and control requests using a combination of clustering, GWO, and TLbO. All data requests are initially processed through the GWO Model, which facilitates the selection of secret sharing keys for Shamir cryptosystems. These keys are chosen based on their low delay and high security operations, which contributes to a boost in both speed and protection against data-level attacks. With TLbO-based optimizations, the model is further optimized for all control (ownership transfer) requests. The proposed model is capable of enhancing QoS performance while maintaining data and control-level security for real-time requests as a result of these optimizations. This model's performance has been validated against Worm Hole (WH), Distributed Denial of Service (DDoS), and Man-in-the-Middle (MITM) attacks. It was further noted that above proposed model improvises levels of communication throughput by more than 10.4 % as compared to TCSS [2], up to 10.2% in comparison with PUFS [3], and in contrast to ABE PRE [9] it was as high as 8.3% hence shaping it to be tailor-made in case of high data rate deployments. This is largely achieved due to the process inspired by GWO & TLbO making the framework to optimize performance in case of secret sharing as-well-as for ownership transfer mechanism at the time of real-time scenarios.

Talking about large-scale networks, the model must be validated in the near future especially against large-scale networks as well as other types of attacks. Possible enhancement in terms of performance can be incepted with the help of bioinspired optimization techniques and the proper usage of deep learning-based transformer models which can lead

towards the prevention of attacks. Further Q-Learning and Auto Encoders can also be used for incrementally improving the data sharing performance in case of real-time scenarios.

References

[1] K. Yu et al., "A Blockchain-Based Shamir's Threshold Cryptography Scheme for Data Protection in Industrial Internet of Things Settings," in *IEEE Internet of Things Journal,* vol. 9, no. 11, pp. 8154-8167, 1 June 1 (2022), doi: 10.1109/JIOT.2021.3125190.

[2] C. Hsu et al., "Non-Interactive Dealer-Free Dynamic Threshold Secret Sharing Based on Standard Shamir's SS for 5G Networks," in IEEE Access, vol. 8, pp. 203965-203971 (2020), doi: 10.1109/ACCESS.2020.3035278.

[3] Y. Liu et al., "On the Security of Lattice-Based Fiat-Shamir Signatures in the Presence of Randomness Leakage," in IEEE Transactions on Information Forensics and Security, vol. 16, pp. 1868-1879 (2021), doi: 10.1109/TIFS.2020.3045904.

[4] S. Chen et al., "Novel Strong-PUF-Based Authentication Protocols Leveraging Shamir's Secret Sharing," in IEEE Internet of Things Journal, vol. 9, no. 16, pp. 14408-14425, 15 Aug. 15 (2022), doi: 10.1109/JIOT.2021.3065836.

[5] M. Shamir et al., "Charged particles energization during magnetic reconnection in the Earth's magnetosphere by double layers: an analytical approach," in Monthly Notices of the Royal Astronomical Society, vol. 509, no. 3, pp. 3703-3708, Oct. (2021), doi: 10.1093/mnras/stab3236.

[6] H. Zhang et al., "Efficient and Secure Outsourcing Scheme for RSA Decryption in Internet of Things," in IEEE Internet of Things Journal, vol. 7, no. 8, pp. 6868-6881, Aug. (2020), doi: 10.1109/JIOT.2020.2970499.

[7] W. Cheng et al., "Information Leakage in Code-Based Masking: A Systematic Evaluation by Higher-Order Attacks," in IEEE Transactions on Information Forensics and Security, vol. 17, pp. 1624-1638 (2022), doi: 10.1109/TIFS.2022.3167914.

[8] A. E. -S. Ezugwu et al., "A Comparative Performance Study of Hybrid Firefly Algorithms for Automatic Data Clustering," in IEEE Access, vol. 8, pp. 121089-121118 (2020), doi: 10.1109/ACCESS.2020.3006173.

[9] J. Gao et al., "Blockchain-Based Digital Rights Management Scheme via Multiauthority Ciphertext-Policy Attribute-Based Encryption and Proxy Re-Encryption," in *IEEE Systems Journal*, vol. 15, no. 4, pp. 5233-5244, Dec. (2021), doi: 10.1109/JSYST.2021.3064356.

[10] S. K. Sharma, A. Chaurasia, V. S. Sharma, C. L. Chowdhary and S. Basheer, "GEMM, a Genetic Engineering-Based Mutual Model for Resource Allocation of Grid Computing," in *IEEE Access*, vol. 11, pp. 128537-128548 (2023), doi: 10.1109/ACCESS.2023.3333278.

[11] W. J. Jun and T. S. Fun, "A New Image Encryption Algorithm Based on Single S-Box and Dynamic Encryption Step," in IEEE Access, vol. 9, pp. 120596-120612 (2021), doi: 10.1109/ACCESS.2021.3108789.

[12] S. Jeon et al., "Cross-Layer Encryption of CFB-AES-TURBO for Advanced Satellite Data Transmission Security," in IEEE Transactions on Aerospace and Electronic Systems, vol. 58, no. 3, pp. 2192-2205, June (2022), doi: 10.1109/TAES.2021.3134988.

[13] H. Xiong et al., "A Survey of Public-Key Encryption With Search Functionality for Cloud-Assisted IoT," in IEEE Internet of Things Journal, vol. 9, no. 1, pp. 401-418, 1 Jan. 1, (2022), doi: 10.1109/JIOT.2021.3109440.

[14] C. Equihua et al., "A low-cost and highly compact FPGA-based encryption/decryption architecture for AES algorithm," in IEEE Latin America Transactions, vol. 19, no. 9, pp. 1443-1450, Sept. (2021), doi: 10.1109/TLA.2021.9468436.

[15] Sharma, Sandeep Kumar, Kumar, Anil, Ashtagi, Rashmi & Jain, Rekha. OCA: An intelligent model for improving security breach of biometric based authentication systems, *Journal of Discrete Mathematical Sciences and Cryptography*, 26:5, 1415–1425 (2023), DOI: 10.47974/JDMSC-1765.