International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Improved Biometric Authentication Using Blockchain Based Biometric Authentication Model

[1]M. S. Kavitha, [2]Annapantula Sudhakar, [3]KNH Srinivas, [4]Paritala Jhansi Rani, [5]Harsha B. K., [6]Sk. Riyaz Hussain

Submitted: 01/10/2023 **Revised**: 21/11/2023 **Accepted**: 02/12/2023

Abstract: In recent decades, Biometric Blockchain Authentication Models are becoming an optimal model on convenience and safety.With user enrolment on the system based on biometric details, the information is management by the administration model as a template and using this the authentication is conducted via an authentication module.Biometric is one of the safest waysover different applications that secures the data in the form of passwords. However, it suffers mostly from the attacks due to leakage of biometric information that prunes the access of intruders. In this paper, we develop a blockchain based security model for the Biometric Blockchain Authentication Model to secure the data and avoids data leakage. The model is designed in such a way that it verifies and secures the entire data in block ledgers. The experimental validation is conducted to test the efficacy of authentication. The results of simulation show that the proposed authentication model achieves higher degree of security than other methods.

Keywords: *Biometric Authentication, Blockchain, Authentication System, intruders*

1. Introduction

It is secure and convenient to employ biometric blockchain authentication models. Enrolling biometric information is handled by an administrative module that stores and manages templates of information; an authentication module compares the newly entered information to those templates. In comparison to traditional techniques like passwords, biometric information is unique and protected for each individual, making it more secure than passwords [1]. However, because biometric information is immutable, a leak of biometric information might lead to subsequent security issues [2]. Furthermore, biometric information is maintained by a central module in general, which reduces the safety and dependability of authentication systems [3].

Biometric template security has been the primary focus of previous research [4,5] to reduce the risk. Templates are created by extracting predefined features from biometric data, combining them with hash values, and then storing the result. Although the template avoids direct leakage of the original information, once the template is exposed, the original information can be estimated by reverse engineering [6,7].

An entirely new Biometric Blockchain Authentication Model (BBAM) has been developed to address the limitations and shortcomings of the current techniques. As an emerging technology, blockchain enables application systems to create resilient security mechanisms without the need for a centralised authority [8-10].

For two reasons, BBAM incorporates blockchain technology: a distributed, decentralised mechanism for an auditable mechanism and processing biometric authentication for handling biometric data. BBAM makes it possible to securely handle biometric information by dividing each template into fragments and storing them on the blockchain for multiple clients. BBAM uses a blockchain-based authentication system that allows every client on the blockchain to complete transactions without the need for a central authority. In BBAM, every transaction is confirmed and documented with a timestamp, therefore all authentication activity is recorded and can be traced back to a specific transaction in the blockchain.

Due to its blockchain-based distributed management, blockchain-based decentralised authentication, and blockchain-based audit mechanism (BBAM), it is distinct from prior works in that it enhances the security of biometric information through distributed

[1]*Associate Professor, Department of Electronics and Communication Engineering, R. M.K. Engineering College, Gummidipoondi, Kavaraipettai, Tamilnadu, India.* ***msk.eee@rmkec.ac.in***
[2]*Associate Professor, Department of ECE, GMR Institute of Technology, Rajam, Andhra Pradesh, India.* ***sudhakar.a@gmrit.edu.in***
[3]*Associate Professor, ECE Department, Sri Vasavi Engineering College, Tadepalligudem, Andhra Pradesh, India.* ***knh.tridents@gmail.com***
[4]*Deputy Manager, HCL Technologies, Hyderabad, Telangana, India.* ***Jhansi.infoarea@gmail.com***
[5]*Department of ECE, CMR Institute of Technology, Bengaluru, Karnataka, India.* ***harsha405@gmail.com***
[6]*Department of Electronics and Communication Engineering, Rajiv Gandhi University of Knowledge Technologies – Nuzvid, Andhra Pradesh, India.* ***riyazhussain786@gmail.com***

management, it increases the reliability of authentication operations, and it guarantees the transparency of biometric information flow. We compared BBAM's authentication time to that of the current system and found it to be faster, which led us to conclude that it was reliable. When it comes to real-world settings, BBAM delivers reliable authentication while introducing only a minor performance hit.

A blockchain-based security model was developed for the Biometric Blockchain Authentication Model in this study to protect the data and prevent leakage. As a result, the model verifies and secures all of the data included in block ledgers.

In this paper, we develop a blockchain based security model for the Biometric Blockchain Authentication Model to secure the data and avoids data leakage. The model is designed in such a way that it verifies and secures the entire data in block ledgers.

2. Related Works

Multiple fields such as cryptography, image processing, and computer networks all rely on the Multimodal Biometric Blockchain Authentication Model. It is possible to create a multimodal biometric authentication system by merging fingerprints and palm prints. The pixel intensity is normalised by the process of histogram equivalence. PCA is used to extract features, while Gabor wavelet fusion is used to combine them. The purpose of this model is to increase the security of the user authentication procedure [11]-[13]. Multimodal biometric traits are used with a hash key cryptographic technique to improve cloud security. Modalities such as iris and facial scanning are also part of this system capabilities. Various image processing algorithms are used to extract features from separate modalities. Swarm intelligence techniques such as Artificial Fish Swarm are utilised to improve the retrieved features. Encryption is performed using the AES technique and the hash key is produced [14].

Three biometric modalities are fused to create a multimodal cloud security enhancement approach. Binarization of the fused vectors is performed, and XOR is applied to the altered feature vectors. When storing data in the cloud, AES is used to encrypt the data before it is sent to the cloud. In order to verify the identity of a person, the face and iris modalities are used for authentication. To extract the image's feature vectors, computer vision algorithms use machine learning techniques. Self-Organized Maps and Multilayer Perceptron are used in this approach [16,17].

A multimodal biometric multifactor authentication system is implemented in a cloud environment [18]. It is not enough to rely on password-based user verification to ensure cloud data security. A password and a variety of biometric data are only two of the ways this system protects its user information. In a similar vein, a two-step verification mechanism for cloud security on mobile communication is offered. User identities are verified by iris and fingerprint scans [20, 21].

It is shown that a biometric cloud authentication system is used to manage access and ensure data security utilising multiple approaches for various cloud architectures [22]. Protecting against hill-climbing attacks, a multimodal biometric system has been implemented in the cloud to guarantee anonymity. This work employs two-way encryption. As an initial step in the authentication process, multimodal biometric encryption is employed. The next level of the process is to use Euclidean distance metric to calculate the overlapping information on the data [23].

It is proposed to use a multi-biometric cryptosystem decision level fusion approach for safe cloud file upload. For the safe handling of data, this system authentication and integrity controls provide high levels of security [24]. To secure cloud-enabled systems, multimodal biometric approaches employ context-aware models. For the MFA-MB class association rule to be implemented, a three-stage approach must be used. An improved authentication method for cloud-based PaaS and SaaS is then created using a new metric to assess the overall user experience [25].

A new technique for extracting the features from multimodal qualities is presented here that uses an entropy-based Local Binary Pattern. Users with low FAR and high FRR can be verified using the derived features because they are quite robust. [26] This is a security technique that is built into the cloud model. Key generation through various methods is examined in this study. As a consequence of testing the model with several modalities, the results were fairly accurate. In order to create a key with 256 bits of length, a transparent key generation technique is used.

3. Proposed Method

The Biometric Blockchain Authentication Model (BBAM) is introduced in this section. Thanks to the inclusion of blockchain technology in BBAM, biometric authentication may now be decentralised and disseminated without the use of a centralised authentication module. It is possible to manage template fragments and authentication operations separately in BBAM with no central authority.

This decentralised mechanism eliminates the possibility of a single point of failure, allowing for more reliable authentication. Each template is further divided into fragments, each of which is under the control of a

distinct client. Biometric data can be safely managed by segmenting it, which reduces the likelihood of the entire template being leaked.

To put it another way, a smart contract operating on the blockchain is used to implement the key functions of BBAM, such as template management and authentication recording. Because of this, at least three clients must set up BBAM, and each of these clients runs a blockchain node as part of BBAM. Only verified nodes can participate in BBAM because it is implemented as a permissioned blockchain.

Fig 1: BBAM Model

The storage and management levels of BBAM are depicted in Figure 1. Clients manage user requests in the storage layer, while blockchain nodes set up a blockchain network in the management layer. In contrast to the current server-client authentication systems, each client processes authentication and handles template fragments individually. Using a smart contract, a user can discover which other users are in charge of particular fragments. In BBAM, every authentication procedure is documented as a blockchain transaction.

Registration procedure of BBAM follows the following steps:

- *Request Enrollment*: The biometric information of a user can be captured by a sensor, and then the features can be extracted and a template can be generated.
- *Split Template*: Using a predefined segmentation function and the template generation timestamp, a single template can be divided into three distinct pieces. A template's time stamp causes it to be divided into various types of fragments.
- *Identify Nodes*: The client detects the nodes that are linked to its corresponding node.
- *Select Clients*: There are n copies of each fragment saved in the database for every client in BBAM, so the total number of clients that can be selected at random is equal to $n/3$ of the total clients.
- *Store Templates*: It is possible to save the template fragments assigned to the selected clients in the selected clients.

For BBAM, the authentication process goes like this:

- *Request Authentication*: A client gathers biometric information from a user via a sensor and then requests authentication from the server.
- *Run Contract*: For example, a user can run the LookUp smart contract to locate the necessary template fragments;
- *Return Information*: A client receives the fragment location information in the form of a URL.
- *Request Templates*: Using distinct client communications, a customer requests and receives the corresponding parts of the request template.
- *Compare Templates*: It is possible to compare the fragmented templates to the necessary information by merging them into a single template and comparing them.

4. Results and Discussions

In this section, the authentication model is implemented and validated using Ethereum blockchain using Solidity (v.0.6.0) and Geth (v.1.9.25), where the client is implemented and validated using Web3py and Python 3.8.

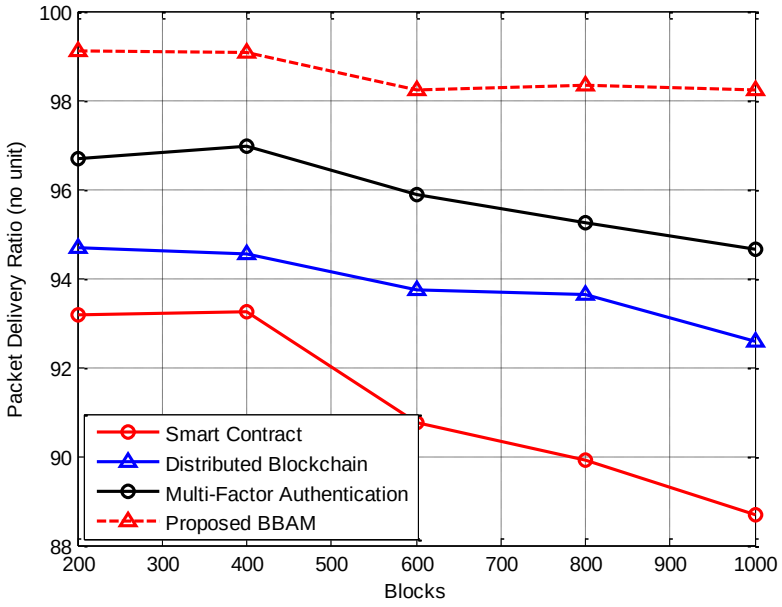

Fig 2: PDR vs. Blocks in BBAM

Figure 2 shows the results of packet delivery rate over various blocks of blockchain for optimal authentication of data in the biometric model. After the process of successful authentication, the efficacy of the system is tested in terms of packet delivery rate between the proposed and existing blockchain authentication mechanism. The results of simulation show that the proposed method achieves higher rate of successful delivery of packets.

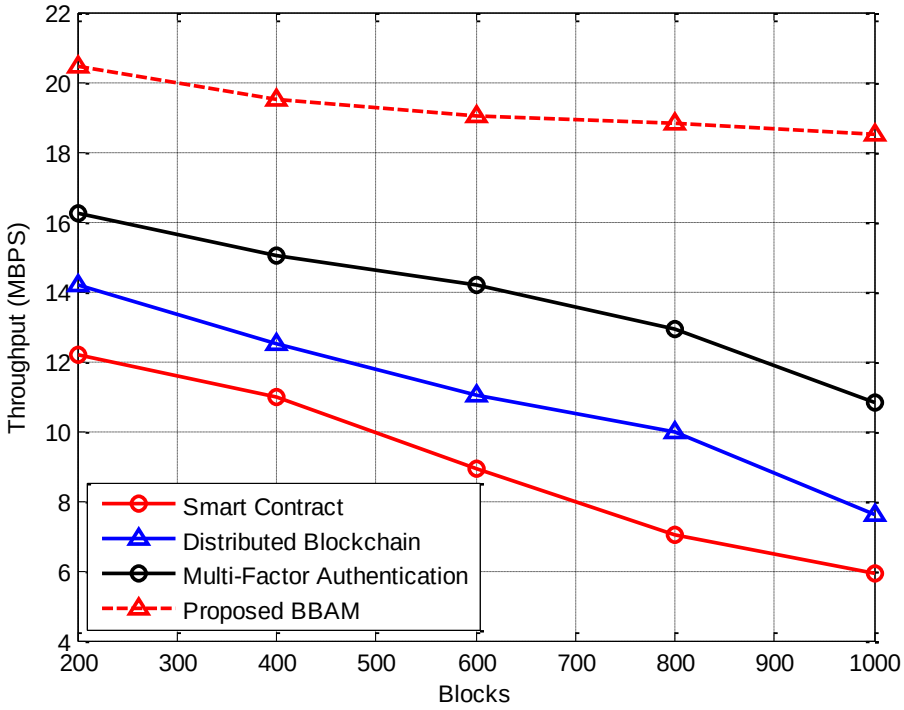

Fig 3: Throughput vs. Blocks in BBAM

Figure 3 shows the results of throughput over various blocks of blockchain for optimal authentication of data in the biometric model. After the process of successful authentication, the efficacy of the system is tested in terms of throughput between the proposed and existing blockchain authentication mechanism. The results of simulation show that the proposed method achieves higher rate of throughput that ensures optimal delivery of data in the network.

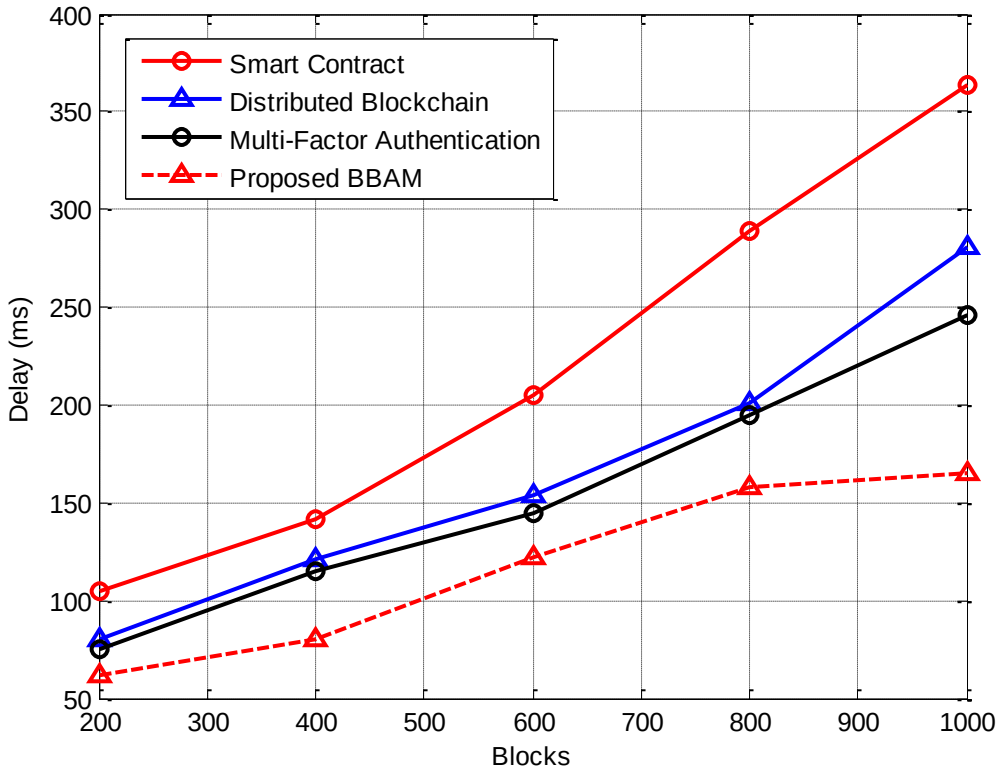

Fig 4: Delay vs. Blocks in BBAM

Figure 4 shows the results of delay over various blocks of blockchain for optimal authentication of data in the biometric model. After the process of successful authentication, the efficacy of the system is tested in terms of delay between the proposed and existing blockchain authentication mechanism. The results of simulation show that the proposed method achieves reduced rate of delay that ensures faster delivery of data in the blockchain network.

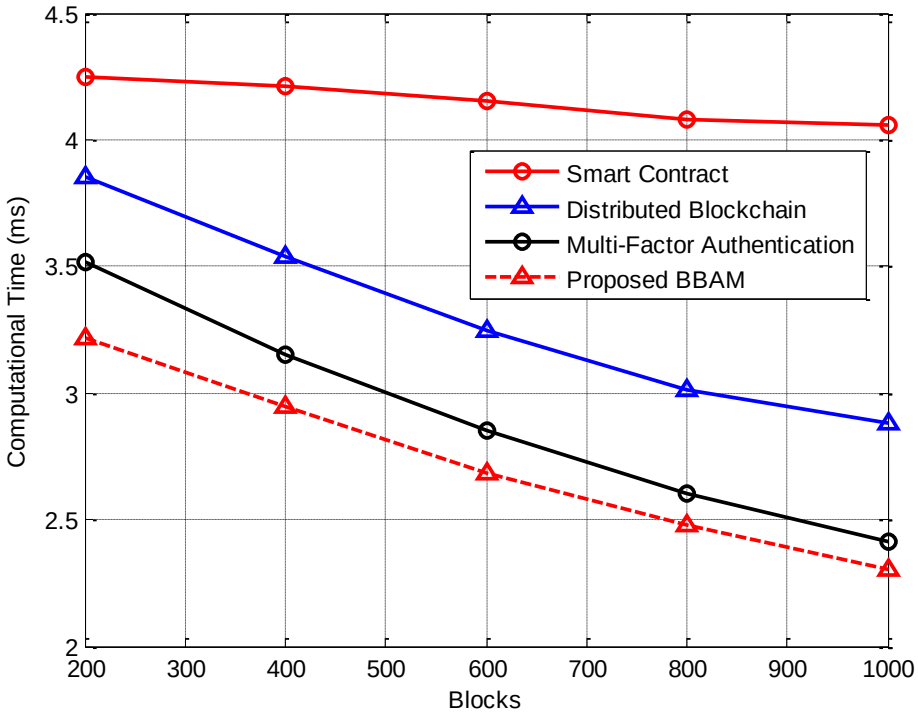

Fig 5: Computational time (ms) vs. Blocks in BBAM

Figure 5 shows the results of computational time over various blocks of blockchain for optimal authentication of data in the biometric model. After the process of successful authentication, the efficacy of the system is tested in terms of computational time between the proposed and existing blockchain authentication mechanism. The results of simulation show that the proposed method achieves reduced rate of computational time that ensures faster delivery of data in the blockchain network.

5. Conclusions

In this paper, we develop a blockchain based security model for the Biometric Blockchain Authentication Model to secure the data and avoids data leakage. The model is designed in such a way that it verifies and secures the entire data in block ledgers. The experimental validation is conducted to test the efficacy of authentication. The results of simulation show that the proposed authentication model achieves higher degree of security than other methods.

BBAM authentication is successfully implemented on the Ethereum blockchain using a core operation of the system. As demonstrated in the evaluations, BBAM beats conventional authentication methods with minimal performance impact. Inevitably, BBAM authentication process takes longer than that of current systems. For larger systems and more templates, the time it takes to authenticate may rise as well. This weakness is reduced by implementing deep optimization techniques for node communication. Because the BBAM uses a distributed ledger technology, it has the intrinsic constraint that its security and dependability depend on the number of nodes. Consider the number of nodes while deploying BBAM to reduce this. In order to improve BBAM, we plan to extend the template segmentation method, integrate the distributed file system, and implement an improved routing on inter-node communications.

References

[1] Joseph, T., Kalaiselvan, S. A., Aswathy, S. U., Radhakrishnan, R., &Shamna, A. R. (2021). A multimodal biometric authentication scheme based on feature fusion for improving security in cloud environment. *Journal of Ambient Intelligence and Humanized Computing*, *12*(6), 6141-6149.

[2] El-Rahiem, B. A., El-Samie, F. E. A., & Amin, M. (2021). Multimodal biometric authentication based on deep fusion of electrocardiogram (ECG) and finger vein. *Multimedia Systems*, 1-13.

[3] Velliangiri, S., Manoharn, R., Ramachandran, S., & Rajasekar, V. R. (2021). Blockchain Based Privacy Preserving Framework for Emerging 6G Wireless Communications. *IEEE Transactions on Industrial Informatics*.

[4] Adekunle, S. E. (2021). An Innovative Approach in Electronic Voting System Based on Fingerprint and Visual Semagram. *International Journal of Information Engineering & Electronic Business*, *13*(5).

[5] Nahar, M. N., Alsadoon, A., Prasad, P. W. C., Giweli, N., &Alsadoon, O. H. (2021). An enhanced one-time password with biometric authentication for mixed reality surgical Tele-presence. *Multimedia Tools and Applications*, *80*(7), 10075-10100.

[6] Vaya, D., &Hadpawat, T. (2021). Enhanced fingerprint authentication using blockchain. *Blockchain 3.0 for Sustainable Development*, *10*, 123.

[7] Sarier, N. D. (2021). Multimodal biometric authentication for mobile edge computing. *Information Sciences*, *573*, 82-99.

[8] Huang, Y. B., Hou, H., Chen, T., Li, H., & Zhang, Q. Y. (2021). Long sequence biometric hashing authentication based on 2D-SIMM and CQCC cosine values. *Multimedia Tools and Applications*, 1-27.

[9] Sujarani, R., Manivannan, D., Manikandan, R., &Vidhyacharan, B. (2021). Lightweight Bio-Chaos Crypt to Enhance the Security of Biometric Images in Internet of Things Applications. *Wireless Personal Communications*, 1-21.

[10] Wang, W., Qiu, C., Yin, Z., Srivastava, G., Gadekallu, T. R., Alsolami, F., & Su, C. (2021). Blockchain and PUF-based Lightweight Authentication Protocol for Wireless Medical Sensor Networks. *IEEE Internet of Things Journal*.

[11] Preneel, B. (1994). Cryptographic hash functions. *European Transactions on Telecommunications*, *5*(4), 431-448.

[12] Delac, K., &Grgic, M. (2004, June). A survey of biometric recognition methods. In *Proceedings. Elmar-2004. 46th International Symposium on Electronics in Marine* (pp. 184-193). IEEE.

[13] Gayathri, R., &Ramamoorthy, P. (2012). A fingerprint and palmprint recognition approach based on multiple feature extraction. *European Journal of Scientific Research. ISSN*, 514-526.

[14] Oravec, M. (2014, September). Feature extraction and classification by machine learning methods for

biometric recognition of face and iris. In *Proceedings ELMAR-2014* (pp. 1-4). IEEE.

[15] Mansour, A., Sadik, M., Sabir, E., & Azmi, M. (2016, October). A context-aware multimodal biometric authentication for cloud-empowered systems. In *2016 International Conference on Wireless Networks and Mobile Communications (WINCOM)* (pp. 278-285). IEEE.

[16] Masala, G. L., Ruiu, P., & Grosso, E. (2018). Biometric authentication and data security in cloud computing. In *Computer and network security essentials* (pp. 337-353). Springer, Cham.

[17] Khatri, S. K., &Vadi, V. R. (2017, August). Biometrie based authentication and access control techniques to secure mobile cloud computing. In *2017 2nd International Conference on Telecommunication and Networks (TEL-NET)* (pp. 1-7). IEEE.

[18] Ahmad, A., Paul, A., Khan, M., Jabbar, S., Rathore, M. M. U., Chilamkurti, N., & Min-Allah, N. (2017). Energy efficient hierarchical resource management for mobile cloud computing. *IEEE Transactions on Sustainable Computing*, *2*(2), 100-112.

[19] Sarier, N. D. (2017, May). Privacy preserving multimodal biometric authentication in the cloud. In *International conference on green, pervasive, and cloud computing* (pp. 90-104). Springer, Cham.

[20] Nair, V. S., Reshmypriya, G. N., Rubeena, M. M., &Fasila, K. A. (2017, March). Multibiometric cryptosystem based on decision level fusion for file uploading in cloud. In *2017 International Conference on Recent Advances in Electronics and Communication Technology (ICRAECT)* (pp. 29-32). IEEE.

[21] Mansour, A., Sadik, M., & Sabir, E. (2015, November). Multi-factor authentication based on multimodal biometrics (MFA-MB) for Cloud Computing. In *2015 IEEE/ACS 12th International Conference of Computer Systems and Applications (AICCSA)* (pp. 1-4). IEEE.

[22] Vidya, B. S., & Chandra, E. (2019). Entropy based Local Binary Pattern (ELBP) feature extraction technique of multimodal biometrics as defence mechanism for cloud storage. *Alexandria Engineering Journal*, *58*(1), 103-114.

[23] Abed, L., Clarke, N., Ghita, B., &Alruban, A. (2018, November). Securing cloud storage by transparent biometric cryptography. In *International Conference on Security for Information Technology and Communications* (pp. 97-108). Springer, Cham.

[24] Kundu, S., & Sarker, G. (2016, January). A new RBFN with modified optimal clustering algorithm for clear and occluded fingerprint identification. In *2016 2nd International Conference on Control, Instrumentation, Energy & Communication (CIEC)* (pp. 125-129). IEEE.

[25] Arrawatia, S., Mitra, P., & Kishore, B. (2017). Critical literature survey on iris biometric recognition. *Int J Sci Res Sci Technol*, *3*(6), 600-605.

[26] Jia, W., Zhang, B., Lu, J., Zhu, Y., Zhao, Y., Zuo, W., & Ling, H. (2017). Palmprint recognition based on complete direction representation. *IEEE Transactions on Image Processing*, *26*(9), 4483-4498.

[27] Veeraiah, D., Mohanty, R., Kundu, S., Dhabliya, D., Tiwari, M., Jamal, S.S., Halifa, A. Detection of Malicious Cloud Bandwidth Consumption in Cloud Computing Using Machine Learning Techniques (2022) Computational Intelligence and Neuroscience, 2022, art. no. 4003403

[28] Dhanikonda, S.R., Sowjanya, P., Ramanaiah, M.L., Joshi, R., Krishna Mohan, B.H., Dhabliya, D., Raja, N.K. An Efficient Deep Learning Model with Interrelated Tagging Prototype with Segmentation for Telugu Optical Character Recognition (2022) Scientific Programming, 2022, art. no. 1059004