Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 45 No. 2 (2024)

A Review on Authentication by Embedding Biometrics in Qr Codes

Archana Y. Chaudhari[1], Jagannath Kulkarni[2], Atharva Ghorpade[3], Shivam Sakore[4], Ujjwala Dube[5] and Anil Kumar Gupta[6]

[1-5] Department of Informtaion Technology, Dr. D.Y.Patil Institute of Technology, Pimpri, Pune, India
[6] C-DAC, Pune , Maharashtra, India.

Abstract. In an age characterized by digital services and the ever-present threat of cyber- attacks, robust and secure authentication methods have never been more analytical. Traditional methods, such as passwords and pins, are prone to various susceptibility, including phishing, brute-force attacks, and user negligence. This vulnerability highlights the pressing need for innovation in the field of authentication. Biometric authentication has proven to be a promising solution that offers the potential for increased security and user benefits, introducing a burst of fresh possibilities into the authentication landscape. However, even biometric systems have faced their own challenges, introducing debates and discussions about privacy and their vulnerability to unauthorized access. In the quest for solutions, a concept like QR code biometric authentication enters the scene, adding a burst of ingenuity and complexity to the discourse. This innovative system employs a cryptographic algorithm to encrypt and decrypt the QR code, creating a perplexing layer of security that baffles potential attackers. The QR code biometric authentication approach eliminates the need for complex passwords, introducing simplicity and efficiency, while simultaneously bursting through the limitations of traditional authentication methods. This paper reviews the literature present in biometric authentication and QR code and help the researcher to gain more knowledge in this field.

Keywords: *cyberattacks, Quick Response code (QR code), cryptography algorithm.*

1 Introduction

The Quick Response code is a matrix barcode invented by Masahiro Hara. It makes use of four input modes numeric, alphanumeric, and byte/binary to store data. Bio- metric Authentication using a QR code represents a perplexing fusion of two distinct yet complementary technologies[1]. This groundbreaking system combines the complex intricacies of biometric authentication with the simplicity and burstiness of QR codes[2]. In an era where security breaches and identification of theft pose persistent threats, this novel approach strives to supply a perplexity of robust solutions[3]. By blending the unique biological traits of individuals with the QR codes, this system offers an intrigu- ing and multifaceted authentication model[4]. It introduces a perplexity of complexity by utilizing biometric data, ensuring that each individual's identity is verified with a high degree of certainty [5]. The concept itself is perplexing, as it combines the intricacies of biometric data analysis and recognition with the burstiness of scanning QR code. This combination promises to offer a more secure and user-friendly method of authenticating individuals and safeguarding sensitive information[6]. In a world where the demand for heightened security and user-friendly experiences coexist, this innovative approach emerges as a perplexing and bursty solution to the authentication challenge of our digital age[7]. The adoption of authentication biometrics is not limited to smartphone unlocking; It is used in various applications, including securing access to corporate net- works, banking operations, border control, and even healthcare systems. Biometrics not only improve security but also provide a better user experience, as they eliminate the need to remember and frequently change passwords or carry a physical access card[8]. This combination gives advantages along with better protection, convenience, privacy protection, and tamper-proof information transmission. It can be employed as a form of multi-aspect authentication. However, sturdy security measures should be in place to guard biometric facts and manage cryptographic keys securely[9]. Users should addi- tionally be educated about the privacy implications and safety features related to suchsystems. By combining biometric data with QR law technology, this design aims to produce a more secure, accessible, and protean authentication system[10].

The structure of this paper is as follows: Section 2 contains works that are related. The proposed method and architecture are described in section 3. Section 4 goes over the Application of the proposed system, while Section 5 presents the conclusion.

2 Literature Survey

In this section, we review the work done in the field of biometric authentication and QR codes. There are recent comprehensive overviews of an adaptive system and surveys that extensively analyzed adaptive biometric authentication system [11].The survey delves into the world of adaptive authentication systems and their challenges, providing a comprehensive understanding. Within its grasp, it encompasses a diverse array of authentication systems that utilize adaptive or context-aware elements, without constraints on the variety of authentication factors they incorporate. Furthermore, it places a special emphasis on investigating biometric features of authentication within these adaptive systems. Physical biometrics are based on physical charac- teristics of the human body which are fingerprints, iris patterns, face recognition, ear shape, palm prints, and vein patterns. Behavioral biometrics depend on patterns of behav- ior or actions, such as keystroke dynamics, gait recognition, and voice recognition[12]. Fingerprint technology is better suited for light security systems, as it is not robust enough for heavy-duty applications. However, it needs to be noted that even in these lighter systems, there is a risk of authentication failure due to possible fingerprint point misident[13]. The touch ID or fingerprint is well-founded than Face ID or other biometrics for reasons that have been touched upon fingerprints are less conditional than facial appearance or changes in voice etc[14]. The fingerprint identifi- cation doesn't depend on a specific camera angle or any other thing. Fingerprint patterns are more rare than facial patterns.[15] In this research, the authors proposed to use fingerprints for the authentication system as shown in figure 1.

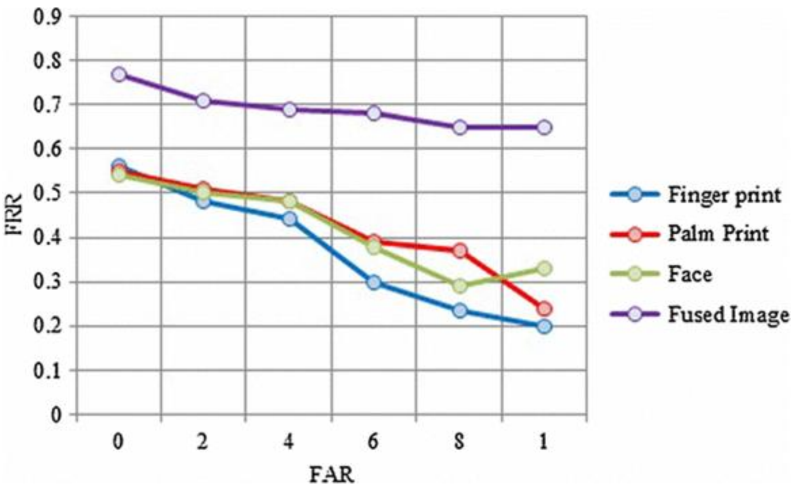

Fig. 1. Various ways of authentication

QR code, or Quick Response code, was developed in 1994 by Masahiro Hara from "Denso Wave," a Japanese corporation. It utilizes four input modes - numeric, alphanumeric, byte/binary, and Kanji/Kana - to adeptly store data. This 2-D matrix barcode is made up of black squares on a white background and can be scanned and read by 2-D digital imaging devices, such as smartphones also third-party apps. For accurate interpretation, QR codes undergo Reed-Solomon error correction. They store information in both the horizontal and vertical elements of the image (Bhardwaj, Garg, & Shekhar, 2022). There are versions of QR codes ranging from Version 1-40. The QR code can store alphanumeric characters from 3000 to 7000. It depends on the information we wantto store in code as shown in table 1.

Table 1. Storage Capacity Of QR Code with Different Input Modes (Bhardwaj et al., 2022)

Input Mode	Maximum Character	Bits/Character
Numeric only	7089	133
Alphanumeric	4296	153
Binary/Byte	2953	8
Kanji/Kana	1817	13

The cryptography is the process of transforming information into an unreadable format. The cryptography contains aspects such as encryption, decryption, cryptographic key, etc. The literature (Bhardwaj et al., 2022) intent of work is to secure QR codes from unauthorized access by allowing only those who have authorization to access it by using cryptography. As in the literature, Fernet presents an impressive encryption solution that strikes the perfect stability between security, speed, and data integrity (Tripathi, Tiwari, Nigam, Gupta, & Verma, 2021). It offers a smart and reliable way to safeguard mobile data from a multitude of threats, ensuring that confidential information remains shielded from prying eyes and possible cyber intrusions (Prashanth, Mohamed, Latha, Hemavathi, & Venkatesh, 2021). And for enhancing the security QR code should be sent via e- mail (Segoro & Putro, 2020) QR Code is used to verify that the logged-in user is the account owner. The code sent via email causes the registration process to change. Detecting whether a QR code has been reproduced by an adversary or tampered with is a critical aspect of maintaining its integrity and ensuring the authenticity of the information it carries (Li et al., 2021). Another methodology proposed to integrate security with QR codes to save text and information(Malallah, Abduljabbar, Shareef, & Al-Janaby, 2023). The traditional method of authentication is not sufficient so to guard against this biometric authentication is proposed in this literature (Ubah et al., 2022). The Arduino board interfacing was developed and it takes the automatic identification of a person once it stored in the system (Dutta et al., 2020). It highlights recent surveys and research on biometric authentication. The research also came up with behavioral and physio- logical patterns. The physiological biometrics and physical features like fingerprints (Chaudhari & Mulay, 2022). The research proves that fingerprint technology is more reliable than others for lighter security and The research also finds the introduction and exploration of the QR code. Explanation of the capabilities and development of the QR code, including different input methods and storage capacities. It touches on the use of cryptography to secure QR codes, with a focus on the Fernet Algorithm. And also, the use of email to enhance QR code security and the significant of detecting tampering or reproduction of QR codes to maintain data integrity and authenticity. In the above research and literature survey the authors reviewed the field of biometric authentication and QR codes. The authors came up with the idea of integrating the fingerprint and QR code to enhance security. The highlights of the literature survey as shown in Table 2.

Table 2. Literature Survey Table

S/No	Journal (Year)	Title of the paper	Method Used	Findings
1	Science Direct (2023)	The design and evaluation of adaptive biometric authentication systems: Current status, challenges	A review on design and evaluation of adaptive bio-metric authentication systems: Current status, challenges and future direction.	Biometric authentication systems have found extensive use across various scenarios to confirm an individual's identity by relying on physiological and behavioral attributes, offering an alternative to

		and future direction		traditional authentication methods.
2	Science Direct (2022)	Biometric authentication using a deep learning approach based on different level fusion of finger knuckle print and fingernail	Fingerprint technology is better suited for light security systems, Because it isn't robust enough for heavy-duty applications.	The results demonstrated the satisfactory verification execution of the method and its usability in practical applications.
3	IEEE (CISES - 2022)	An Approach for Securing QR code using Cryptography and Visual Cryptography	The proposed method aims to maintain the security of QR code using: encryption, decryption.	The QR code can be secured by the Cryptography.
4	IEEE(CSNT-2021)	The Hybrid Cryptography for Enhancing the Data Security in Fog Computing	Encrypting all the section of the file using any one among the selected algorithms.	Fernet algorithm help to accomplished data integrity and also key information is secure using Fernet encryption.
5	IEEE (ICCCT - 2021)	Enhanced Hybrid Encryption Through Slicing and Merging of Data with Randomization Of Algorithms	The file is encrypted with the AES algorithm.	This application enables a user to encrypt data according to their wish.
6	IEEE (2020)	Implementation of Two Factor Authentication (2FA) and Hybrid Encryption to Reduce the Impact of Account Theft on Android-Based Instant Messaging	QR Code implementation is sent via email.	The attacker cannot read and send messages on behalf of the victim because the attacker does not have any other authentication that the user has.

		(IM) Applications		
7	IEEE (2021)	SCREENID: Enhancing QR Code Security by Fingerprinting Screens	Detecting whether a QR code has been reproduced by an adversary or tampered.	Only QR codes displaying on its specific screen are accepted.
8	IEEE(IT-2023)	QR Code Encryption for improving Bank information and Confidentiality	The methodology is to integrate the security with QR code to save the text bank information.	QR code protection has been proved by using encryption by generating key with the same dimension as the re-sized QR image.
9	IEEE (2022)	Biometrics Authentication Techniques in E Learning Assessment	The biometrics technique is still one of the approaches used to either reduce or stop this malpractice.	The discussion revolved around various biometric techniques and their utilization in the context of e-assessments.
10	IEEE (ICISS-2022)	Smart and Secure Fingerprint Attendance System using Arduino UNO with GSM Alert	The Arduino board interfacing was developed and it takes the automatic identification of a person once it stored in the system.	A secure operation model by hashing biometric information against the looming danger of information leakage.

3 Proposed Methodology

This section describe the proposed dataset & methodology.

3.1 Proposed Dataset

The fingerprint data are crucial within the realm of biometrics technology and security. The fingerprint dataset plays an important role in developing and testing fingerprint recognition systems for authentication and identification purposes. The fingerprint dataset available is FVC2002 (Fingerprint Verification Competition 2002)dataset (Maio, Maltoni, Cappelli, Wayman, & Jain, 2002). In this dataset the images acquired from a range of sensors under different conditions are available. The FVC2002 dataset is commonly utilized for fingerprint recognition algorithms. It consists of four subsets. Another data set is the NIST Special database14, which is element of the National Institute of Standards and Technology database collection. It contains a substantial quantity of fingerprint images. It is used for conducting assessments and appraising fingerprint recognition technologies.

The dataset of the fingerprint is vital for managing and processing for accurate and secure utilization for various applications. To achieve that goal we should try to create our own dataset. In this research, we are going to utilize a fingerprint module and Arduino UNO to collect the fingerprint information stored within the database. In figure 2, we detail the hardware architecture. This is the proposed hardware architecture which consists of an Arduino UNO board and a Fingerprint module R307. The pin configuration of the R307 fingerprint model has 6 pins.

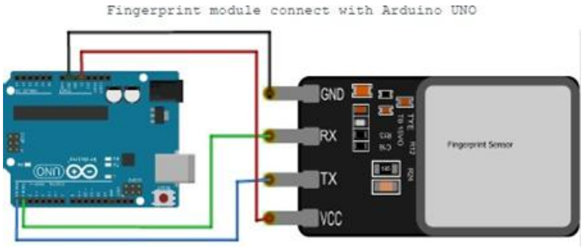

Fig. 2. Hardware Architecture

In Fig.2, we detail the hardware architecture. This is the proposed hardware architecture which consists of an Arduino UNO board and a Fingerprint module R307. The pin configuration of the R307 fingerprint model has 6 pins as describe in table 3.

Table 3. Pin Configuration of R307 fingerprint module.

Pins Number	Pin Name
1	5V
2	GND
3	TX
4	RX
5	Touch
6	3.3V

UNO board. The TX and RX pins are connected for data transmission of the fingerprint.The Arduino UNO board helps to process the fingerprint data by utilizing assistance from the Arduino UNO software. The Arduino Adafruit fingerprint libraryis used for the recognition of the fingerprint. By making sure to properly connect the power and ground connections, in addition to linking the module's TX and RX pins to the Arduino's serial ports, we can easily create a dependable interface. To streamline the process of enrolling fingerprints, you have the option to include a dedicated button. With software and libraries configured, the Arduino can effectively handle features like fingerprint enrollment and verification. This integration provides a simple and effective way to enhance security through biometrics.

3.2 Encryption and Decryption Algorithm

In this project, we are using the Fernet Algorithm for encryption and decryption of the data. The Fernet algorithm is a versatile and trusted symmetric key cryptography method, serving multiple purposes such as secure communication, data storage, and authentication. Its development stemmed from the requirement for a straightforward and efficient solution for encrypting and decrypting data with the additional assurance of data integrity and authenticity. As a favored choice, Fernet is commonly implemented in conjunction with the Python programming language, as it forms a key component of the cryptography library.

Fernet is an excellent choice for implementing data encryption, as it utilizes a symmetric algorithm wherein the same key is used for both encrypting and decrypting data. This key, known as the "secret key," is crucial in ensuring the security of the encrypted data (Tripathi et al., 2021). What sets Fernet apart is its comprehensive approach to security. Along with encryption, it also provides message authentication and integrity checks. This implies that not only is the data encrypted, but it also includes a message authentication code (MAC), making it virtually impossible for anyone to tamper with the data during transmission or storage. One of the most significant advantages of Fernet is its compatibility with web applications and URLs. It utilizes URL-safe base64 encoding for ciphertext and other components, making it a good fit for web-based operations. Additionally, Fernet offers the added benefit of time-based encryption. This feature enables users to set a time-to- live (TTL) for the data that has undergone encryption, ensuring that it automatically expires after a predetermined period.

Steps for implementation of Fernet Algorithmin Python :

1. Generate a secret Key.
2. Encrypt the data using the secret key.
3. Decrypt the data using the same secret key.

3.3 Proposed Architecture

Figure 3 depict the proposed system architecture. The system will work in two phases. In the initial phase, the user can simply register from our own web application for authentication. The individual must input accurate information to avoid errors. The individual must fill the all mandatory details so that it can enhance the security more. Then the individual should proceed with the generation of the QR code. The QR code automatically will be emailed to the user and securely stored in our database.

The heart of this system is a web-based user interface created with Django, HTML, CSS, and JavaScript. Through this interface, users can easily interact with the system, whether it's for enrolling or authenticating. The system also utilizes cutting-edge biometric sensors and that are seamlessly integrated into the user interface, making data collection during enrollment effortless. These sensors capture data of fingerprints which are then processed within the system. Employing feature extraction algorithms, the system extracts crucial information from the collected biometric data for fingerprinting. To ensure secure authentication, the system produces an unparalleled QR code for every individual user based on their biometric data and personal information. This code serves as a reliable identifier for every user.

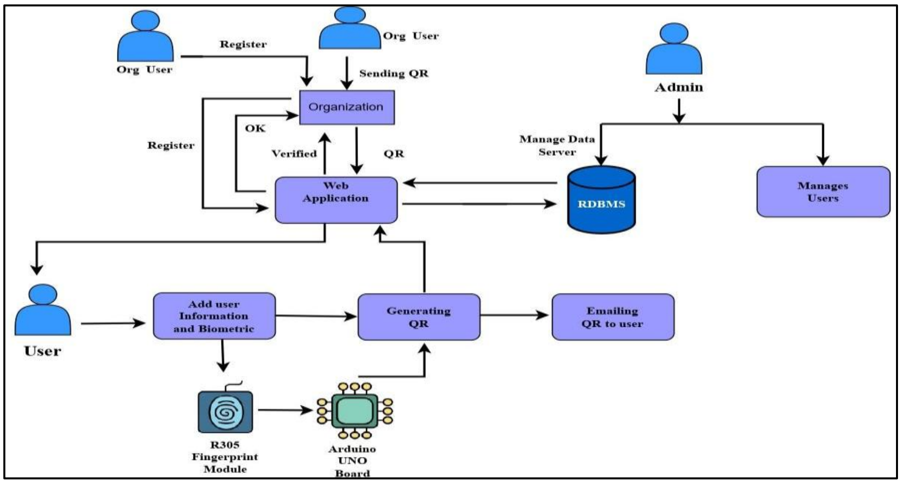

Fig. 3. Proposed System Architecture

4 Applications

The proposed system has many applications in the in the real world.

- The system offers robust managing entry and ensuring safety measures to organizations, grant-ing entrance only to authorized personnel in restricted areas. Additionally, it aids in accurate employee scheduling and monitoring of attendance.
- Financial institutions canenhance transaction security by implementing biometric authentication for customer identity verification.
- In the healthcare sector, the system safeguards electronic health records and upholds the privacy of patient data. Governments can utilize biometric authentication for various services, including passport issuance, voting, and identity verification.
- In educational institutions, such as schools and universities, it has the potential to ensure secure student attendance.
- The integration of biometric authentication opens up endless capabilities for app developers to safeguard user information.

- From mobile banking and password managers to online retailers and guest check-insat hotels and resorts, the possibility of increased security is immense.
- Enhanced Pro- tection for E-Commerce Biometric authentication adds an additional security measure for online retailers, ensuring secure customer logins and payments.
- Protecting critical infrastructure is crucial, and incorporating biometric authentication measures is key to safeguarding facilities like electricity generation facilities and data centers.

5 Conclusion

Our research yielded invaluable insights. The system proved being promising technology, enhancing security, user acceptance, and adaptability across various industries. The journey doesn't end here. We see a future where the system continues to evolve, adapting to new threats and opportunities, and we encourage further exploration and innovation within this field.

Closing this gap is crucial as it would provide valuable insights into the durability of the system and its suitability for widespread, long-term adoption. Future research should focus on conducting in-depth assessments, exploring techniques for mobile and wearable devices, and considering continuous authentication methodologies. Additionally, the acquisition of large-scale datasets and the establishment of standardized evaluation protocols specific to adaptive biometric authentication systems will contribute to a more thorough understanding of system feasibility and effectiveness.

References

1. Bhardwaj, C., Garg, H., & Shekhar, S. (2022). *An Approach for Securing QR code using Cryptography and Visual Cryptography*. Paper presented at the 2022 International Conference on Computational Intelligence and Sustainable Engineering Solutions (CISES).

2. Chaudhari, A., & Mulay, P. (2019). Algorithmic analysis of intelligent electricity meter data for reduction of energy consumption and carbon emission. *The Electricity Journal, 32*(10), 106674. doi:https://doi.org/10.1016/j.tej.2019.106674

3. Chaudhari, A. A., & Mulay, P. (2019). SCSI: Real-Time Data Analysis with Cassandra and Spark. In M. Mittal, V. E. Balas, L. M. Goyal, & R. Kumar (Eds.), *Big Data Processing Using Spark in Cloud* (pp. 237-264). Singapore: Springer Singapore. Saravanakumar, S., & Thangaraj, P. (2019). A computer aided diagnosis system for identifying Alzheimer's from MRI scan using improved Adaboost. Journal of medical systems, 43(3), 76.

4. Kumaresan, T., Saravanakumar, S., & Balamurugan, R. (2019). Visual and textual features based email spam classification using S-Cuckoo search and hybrid kernel support vector machine. Cluster Computing, 22(Suppl 1), 33-46.

5. Saravanakumar, S., & Saravanan, T. (2023). Secure personal authentication in fog devices via multimodal rank-level fusion. Concurrency and Computation: Practice and Experience, 35(10), e7673.

6. Thangavel, S., & Selvaraj, S. (2023). Machine Learning Model and Cuckoo Search in a modular system to identify Alzheimer's disease from MRI scan images. Computer Methods in Biomechanics and Biomedical Engineering: Imaging & Visualization, 11(5), 1753-1761.

7. Saravanakumar, S. (2020). Certain analysis of authentic user behavioral and opinion pattern mining using classification techniques. Solid State Technology, 63(6), 9220-9234.

8. Chaudhari, A. Y., & Mulay, P. (2022). Cloud4NFICA-Nearness Factor-Based incremental clustering algorithm using Microsoft Azure for the analysis of intelligent meter data *Research Anthology on Smart Grid and Microgrid Development* (pp. 423-442): IGI Global.

9. Dutta, R., Tamang, T., Paul, P., Kumar, N., Chetri, C., & Dutta, P. K. (2020). *Smart and Secure Fingerprint Attendance System using Arduino UNO with GSM Alert*. Paper presented at the 2020 3rd International Conference on Intelligent Sustainable Systems (ICISS).

10. Heidari, H., & Chalechale, A. (2022). Biometric authentication using a deep learning approach based on different level fusion of finger knuckle print and fingernail. *Expert Systems with Applications*, *191*, 116278.

11. Li, Y., Chen, Y.-C., Ji, X., Pan, H., Yang, L., Xue, G., & Yu, J. (2021). *Screenid: Enhancing qrcode security by fingerprinting screens.* Paper presented at the IEEE INFOCOM 2021-IEEE Conference on Computer Communications.

12. Maio, D., Maltoni, D., Cappelli, R., Wayman, J. L., & Jain, A. K. (2002). *FVC2002: Second fingerprint verification competition.* Paper presented at the 2002 International conference on pattern recognition.

13. Malallah, F. L., Abduljabbar, A. I., Shareef, B. T., & Al-Janaby, A. O. (2023). *QR Code Encryption for improving Bank information and Confidentiality.* Paper presented at the 2023 27th International Conference on Information Technology (IT).

14. Prashanth, C., Mohamed, M., Latha, K., Hemavathi, S., & Venkatesh, D. (2021). *Enhanced Hybrid Encryption Through Slicing and Merging of Data with Randomization of Algorithms.* Paper presented at the 2021 4th International Conference on Computing and Communications Technologies (ICCCT).

15. Ryu, R., Yeom, S., Herbert, D., & Dermoudy, J. (2023). The design and evaluation of adaptive biometric authentication systems: Current status, challenges and future direction. *ICT Express*.

16. Segoro, M. B., & Putro, P. A. W. (2020). *Implementation of Two Factor Authentication (2FA) and Hybrid Encryption to Reduce the Impact of Account Theft on Android-Based Instant Messaging (IM) Applications.* Paper presented at the 2020 International Workshop on Big Data and Information Security (IWBIS).

17. Sekaran, R., Munnangi, A. K., Ramachandran, M., & Gandomi, A. H. (2022). 3D brain slice classification and feature extraction using Deformable Hierarchical Heuristic Model. Computers in Biology and Medicine, 149, 105990-105990.

18. Ramesh, S. (2017). An efficient secure routing for intermittently connected mobile networks. Wireless Personal Communications, 94, 2705-2718.

19. Sekaran, R., Al-Turjman, F., Patan, R., & Ramasamy, V. (2023). Tripartite transmitting methodology for intermittently connected mobile network (ICMN). ACM Transactions on Internet Technology, 22(4), 1-18.

20. Tripathi, S., Tiwari, R. K., Nigam, R., Gupta, N. K., & Verma, B. (2021). *The hybrid cryptography for enhancing the data security in fog computing.* Paper presented at the 2021 10th IEEE International Conference on Communication Systems and Network Technologies (CSNT).

21. Ubah, A. E., Onakpojeruo, E. P., Ajamu, J., Mangai, T. R., Isa, A. M., Ayansina, N. B., & Al-Turjman, F. (2022). *Biometrics Authentication Techniques in E-Learning Assessment.* Paper presented at the 2022 International Conference on Artificial Intelligence of Things and Crowdsensing (AIoTCs).

22. A. S. Kumar, J. V. M. L. Jeyan, J. N. T, S. Annamalai and N. V. Kousik (2023) *Lossless Video Compression Using Reinforcement Learning in UAV Applications*, International Conference on Data Science and Network Security (ICDSNS), Tiptur, India, 2023, pp. 1-6, doi: 10.1109/ICDSNS58469.2023.10245784.