

Hybrid biometric authentication for banks security improvements

Alyaa A. Abbas *

*General Directorate of Education of Al Muthana
Ministry of Education
Al Muthana
Iraq*

Zahraa Maan Sallal †

*General Directorate of Education of Al Qadisiyah
Ministry of Education
Al Qadisiyah
Iraq*

Abstract

As ATM cards, credit cards, and mobile banking become more convenient, online banking is becoming more popular around the world. Usernames, passwords, CVVs, and OTPs, although traditionally used for authentication, are susceptible to security vulnerabilities. The vulnerabilities of these systems can be exploited at will, resulting in unauthorized access to sensitive financial information. Biometric authentication, particularly the recognition of iris patterns, is proposed as a solution to these security challenges. Through the combination of traditional authentication methods and biometric traits, this system offers an additional layer of security. A secure database stores iris patterns that can be compared to a secure database to verify who is authorized to complete transactions. This provides a dependable solution for modern banking security.

Subject Classification: Primary 93A30, Secondary 49K15.

Keywords: Biometrics parameters, Iris recognition, Security improvement.

1. Introduction

The banking system must keep pace with economic and social progress, while attracting deposits and distributing them in a productive manner. A bank is a service provider that must be able to meet the

* E-mail: programmer.alyaa@gmail.com (Corresponding Author)

† E-mail: Zahraa.m199021@gmail.com

expectations and needs of its customers, as well as ensuring that society's needs are met. With information technology, customer communication is facilitated, speeded up and more effective, resulting in improved performance and innovative services [1]. Banking services are available through various methods, such as POS machines, ATMs, bank websites, and mobile banking. In our opinion, mobile banking is the most convenient. Consumer-provider interactions. In addition to enabling Anywhere Anytime Banking, Mobile Banking is also the easiest and most convenient way to stay in touch with the bank, day or night [2]. Using mobile banking software, you can monitor account balances and the latest transactions, transfer funds between accounts, charge your SIM card, purchase Internet plans, and pay bills using your mobile device. You can also choose the bank you want to use and get other services offered by the software [3]. Furthermore, mobile banking services are available 24 hours a day, 7 days a week. This technology has gained popularity due to its high-quality features, which have attracted many people interested in applying it. Another advantage of mobile banking is that it provides 24-hour access to financial services [4]. Due to software security weaknesses, users are concerned about being attacked by hackers or having their property taken. To reduce the possibility of hackers hacking this software, reliable authentication methods are required for individuals who wish to use it [5].

As fingerprint biometric sensors become universal, mobile banking is adding them. The error rate of this sensor, as well as the security level, is higher than that of facial recognition biometric sensors, which makes them less likely to be hacked.

Due to the growth of the telecommunications and personal computer industries, ATMs have provided new insights to customers and banks. Customers can withdraw money from ATMs by using a plastic card containing an intelligent chip that stores encrypted data about them [6]. Customers have benefited from this technology.

The security concerns of users have increased in recent years, including identity theft, fraud operations, and so on. ATMs currently use only Personal Identification Numbers (PINs) to authenticate users. ATM systems that use PINs do not verify the identity of authorized cardholders since they are only aware of the cardholder's PIN or password [7]. Basically, anyone with a valid PIN can withdraw from ATMs without verifying their identity.

Information security domains have therefore incorporated biometrics for personal identification. A biometric system uses unique features of

individuals, such as their fingerprints, their iris, their hands, their faces, and many others, to ensure their data is secure [8]. In comparison to conventional procedures, biometrics offers a number of advantages. Among these possibilities are theft, loss, copying, and hacking of data such as cards and passwords by third parties and others.

By shoulder surfing, cracking ATM PINs [9], and skimming cards, bank account passwords can be compromised, allowing criminals to take all client funds within the shortest period of time and cause considerable losses. A third party can easily access the account and withdraw money without the client's knowledge in traditional ATM systems, as they require only the PIN code to access the account. Current ATMs require clients to carry their cards and remember their passwords. A client's card could be stolen by a third party if it is accidentally lost as shown in figure 1 [10].

2. Related Works

A variety of fields are becoming increasingly reliant on biometrics, which entails measuring and analyzing biological features unique to individuals. It bears mentioning that biometrics are a pivotal part of the

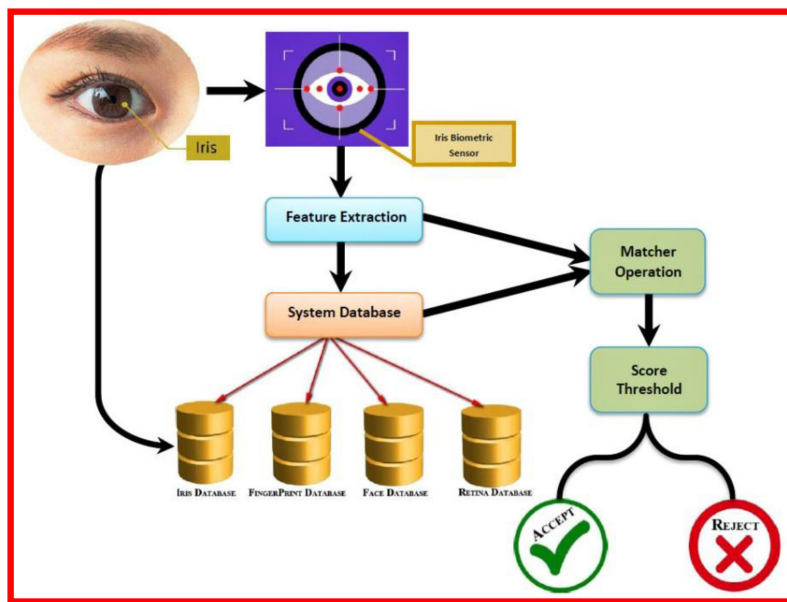


Figure 1

Diagrams for enrolling in and verifying biometric authentication systems

banking industry's explorations [11]. Because of their inherent ability to prevent theft, replica, reproduction, purchase, and forgery, biometric traits are regarded as more innovative than traditional methods such as passwords or identification cards. Because of this increased level of dependability, biometric solutions are seeing considerable interest within the banking sector, indicating improved security [12].

Describe a variety of biometric systems, along with their functional applications, in [13]. In addition, the study concludes that despite biometric recognition systems being effective for overcoming traditional limitations, potential challenges are arising as biometric technology continues to evolve.

A separate endeavor was undertaken by the author [14] aimed at understanding health data obtained from wearable IoT devices. Upon reviewing, discussing, and offering recommendations on using this data as a biometric, the team offered a number of recommendations. The human body is constantly changing, sensors age and deteriorate, selecting a population appropriate for biometric system assessment is difficult, sensor cost has an impact on accuracy, there are no standardized techniques for biometrics, and biometric systems have inadequate security measures [15].

Biometric systems are enhanced through optimization algorithms. The following papers discuss optimization algorithms: [16] applied neural networks to minimize welding challenges, and that approach could be applied to improve biometric system performance and security [17]. Optimizing Shell-and-Tube Heat Exchangers with Copper Oxide and Iranian Refinery Oil Nanofluids. A Pareto frontier curve is generated using algorithms inspired by natural bases that illustrate the cost-efficiency trade-off [18].

A typical two-factor authentication system used by most banks is two-factor authentication. For example, PNB bank requires two passwords for login and two for transaction, SBI bank uses one password for login and one OTP for transaction, etc. Online banking is becoming increasingly popular, so banks need to ensure the security of their users' identities, personal information, and money [19]. The bank should provide secure online services to its customers. To identify genuine users, banks use authentication techniques, and data is transferred from the user's end to the server's end via different cryptographic techniques [20]. The password and user ID are typically checked, since brute force attacks can be used to break them. In order to prevent fraud, banks send an OTP to registered mobile devices as another authentication method. Security also involves

picture authentication, however. Passwords, questions, tags on photos, and one-time passwords are used to authenticate [21]. Transferring data requires hiding data from external users or within the network. Encryption is a method of concealing a message's content by concealing its appearance. Messages that are encrypted are called cipher texts. It is called decryption when cipher texts are converted into plaintext. A message's security is ensured through cryptography. To encrypt or decrypt a message, a 'key' is used. For a message to remain confidential, encryption method and key size must be considered.

An encryption can be either symmetric or asymmetric. When using symmetric key cryptography, the key is the same for both encrypting and decrypting; when using asymmetric key cryptography, the key is the same for both encrypting and decrypting [22]. Encrypting or decrypting information with a public key requires the corresponding private key, and vice versa. Public keys cannot be used to determine private keys in general [23]. The reason why ECDH is used for encrypting data in networks is because it is a combined algorithm [24].

In [25] the first task is to classify known frauds. Each group of fraudulent cases is visually identified using this process. As a result of signature comparisons, potential hybrid attacks are identified during monitoring. To a certain extent, this can be automated. Fraud attacks change constantly, however [26]. As a result of the visual comparison, suspicious cases can be evaluated when automated methods fail. The detection metrics are then modified based on this information. The goal of monitoring customers is to identify suspicious behavior in real-time so that it can be predicted or even identified early. You can accomplish this by using the fraud detection mechanisms listed above.

3. Proposed Methodology

Here is a diagram that illustrates the essential design of a biometric framework. A password can be overlooked, shared, or watched, among other advantages. The world of today is filled with fast-paced electronic devices and a wide variety of passwords and identifiers. Several applications can be verified quickly, easily, and more economically with biometrics. Furthermore, an easy-to-use framework should be designed. In addition to amplifying devices, camcorders, and scanners that scan unique marks, there are easy and quick solutions available. With the spread of biometric innovations, clients will have less difficulty handling

different confirmation levels and numerous validation cases. There are two main stages to the proposed work:

3.1 *Pre-preparing the Medical Image*

An image-matching calculation depends heavily on finger impression images. Practically speaking, a noteworthy proportion of acquired photos lack quality because of environmental factors or health issues of the client. Low-quality images cause two problems:

- (1) In addition, a great deal of false information may be provided;
- (2) There are a lot of details that are often overlooked. In this context, image pre-processing plays a significant role in the construction of an extraction algorithm.

3.2 *Medical Image Matching*

The calculation is coordinated in two ways.

- (1) There are two records needed to create the Candidate Common Points List.
 - (a) Points of agreement confirmed
 - (b) Points that are unconfirmed or suspicious.
- (2) By comparing the Confirmed Common Points List with the Base picture, we can determine whether the two pictures are similar.

4. An Algorithm for Recognizing Iris Features

4.1 *Registration*

Admins will ask secure resource users to submit eye images. An algorithm is developed for extracting characteristic iris features from the enrolled eye image.

It is possible to extract features in three different ways: segmentation, normalization, and normalization.

- (1) A high-resolution camera and sensor are used to capture images of the iris in medical imaging. To obtain a Fourier transform image, use these equations:

$$G(f_a, f_b) = F(g(a, b)) = \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} G(f_a, f_b) \exp[2\pi i(f_a, f_b)] df_a df_b \quad (2)$$

As its inverse Fourier transform, $G(f_a, f_b)$ is defined as follows:

$$G(a, b) = F^{-1}(G(f_a, f_b)) = \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} G(f_a, f_b) \exp[-2\pi i(f_a, f_b)] da db \quad (2)$$

- (2) The iris is segmented from the rest of the eye in an iris image segmentation.
- (3) Images of the iris are normalized: Using its polar equivalent, an iris can be normalized. A Gabor filter normalizes the iris. Below is an image of the Gabor filter in the Gaussian Window:

$$g_e(a) = \frac{-1}{\sqrt{2\pi\sigma}} e^{\frac{-a^2}{2\sigma^2}} \cos(2\pi\omega_s a) \quad (3)$$

$$g_o(a) = \frac{-1}{\sqrt{2\pi\sigma}} e^{\frac{-a^2}{2\sigma^2}} \sin(2\pi\omega_s a) \quad (4)$$

Based on the Gaussian Window spread as σ illustrated in the figure below, where ω_s is the frequency of the center.

Jacques Daugman created the Gabor filter in two dimensions:

$$g_e(a) = \frac{1}{2\mu\sigma_a\sigma_b} e^{\frac{-1(a^2+b^2)}{2(\sigma_a^2+\sigma_b^2)}} \cos(2\omega_s a + w\omega_s b) \quad (5)$$

$$g_o(a) = \frac{1}{2\mu\sigma_a\sigma_b} e^{\frac{-1(a^2+b^2)}{2(\sigma_a^2+\sigma_b^2)}} \sin(2\omega_s a + w\omega_s b) \quad (6)$$

- (4) The features are encoded: Features are encoded by Local Binary Patterns.
- (5) Finding a match between the features: Feature matching is performed by Daugman using the hamming distance method.

4.2 Verification

To validate, the user must present an ID card. The corresponding share is located by searching the database. A first image of Iris is created by stacking two shares. This image provides a template for creating the iris feature. An iris feature template will be generated by segmenting, normalizing, and extracting features from the user's new eye image. The two feature templates are then matched using a hammering distance.

Matching features indicates a successful verification. It fails if this is not the case. An overview of the authentication process can be found in Figure 3.

5. Biometrics Issues

Biometric systems are beneficial, but they are also vulnerable to hacking since they require strong correlation between users and their data. The following are some problems with biometric systems.

Non-Revocability: Unlike a password or PIN, biometric information stored in a database cannot be changed or revoked.

- **Privacy Compromiser:** It has become increasingly important for users to maintain secrecy. An identity's privacy can be compromised in three ways:
 1. Invading biometric privacy: Lost biometric templates can be retrieved by referring to the stored template. The first image of the fingerprint must be created to create fingerprints from saved minutiae points.
 2. The confidentiality of biometric information must be maintained: Biometric traits are simultaneously enrolled in a variety of biometric systems by the same user. Due to this, it is possible to negotiate biometric layouts and use them to log into another biometric system.
 3. Privacy-preserving user identification: A multi-biometric database can crossmatch biometric systems using template data for the same client.

5.1 *Sensors used in biomedicine*

Optical sensors are used to capture images of unique finger impressions. Light passing through a phosphor layer reflects off the finger to create the image of the fingerprint. A high-frequency sound wave penetrates the epidermis of the skin with ultrasound sensors. Piezoelectric transducers produce sound waves. It is possible to estimate the unique mark from the estimation of the reflected waves. Fingers placed on chips create electrical charges between their surfaces and silicon plates. An electrical charge is bigger on the capacitance plates than on the unique finger impression surfaces because a small distance separates them.

5.2 *Estimating biometric authentication system performance*

Hamming distances are calculated from biometric template queries and database features. An image of the same individual usually has a Hamming distance of about 0 when feature vectors are calculated from the images.

As a result, when two feature vectors differ by approximately 0.5 Hamming distance, they are generally regarded as belonging to different users. Identifying your biometric recognition infrastructure's false acceptance rate (FAR), false rejection rate (FRR), and equal error rate (EER) will provide insight into its accuracy. Future chapters will employ this method to evaluate performance.

6. **Assessing the performance of the system**

Biometric layouts are less stable than passwords or encryption keys. It is not uncommon for the same client to have a wide range of results when taking biometric tests at different times. As a result, matches are always made on a probabilistic basis. It is necessary to match secret keys and tokens. Blunders caused by insufficient coordination fall into two categories.

6.1 *Acceptance that is not true*

Imposters may be accepted as legitimate clients if their formats resemble genuine ones.

6.2 *A falsely Rejected*

It is possible for a client who is already certified to be rejected during validation if they provide poor quality biometrics. It appears that this rejection was a false rejection. Additionally, the framework can make less frequent blunders, such as -

6.3 *Failure to enlist (FTE)*

The number of people with messy fingerprints is estimated to be around 4%. People whose hands are frequently used, including seniors and workers, have been harmed. The poor edge structure of these clients prevents them from being enlisted into the database, therefore they cannot be validated. Biometric frameworks should include error-handling components.

6.4 Failure to verify (FTA):

I liked the biometrics when I enlisted. Highlights during confirmation cannot, however, be deciphered by the framework. You may notice fingerprints if you are overexerting, have late damage, or sweat excessively. Frozen, sore, or frosty throats can be debated. When False Rejection occurs during the coordinating process, it differs from False Rejection during the selection process.

7. Results and Discussion

The text’s results section analyzes several access control systems. The proposed system includes authentication, authorization, accounting, and authentication models. The results include a comparison table of the two systems and visual representations of the login and registration forms. Comparison of the existing and proposed systems can be found in Table 1. The proposed system will handle the user interface as in the following figures 2, 3 and 4:

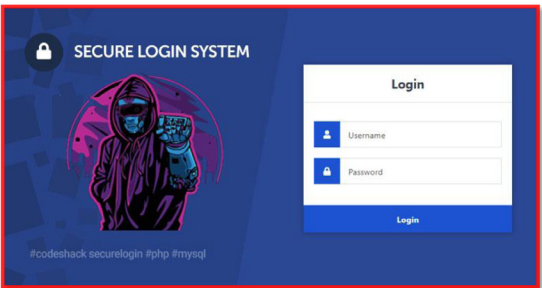


Figure 2

An overview of the proposed system’s interface



Figure 3

A proposed system for logging in and registering

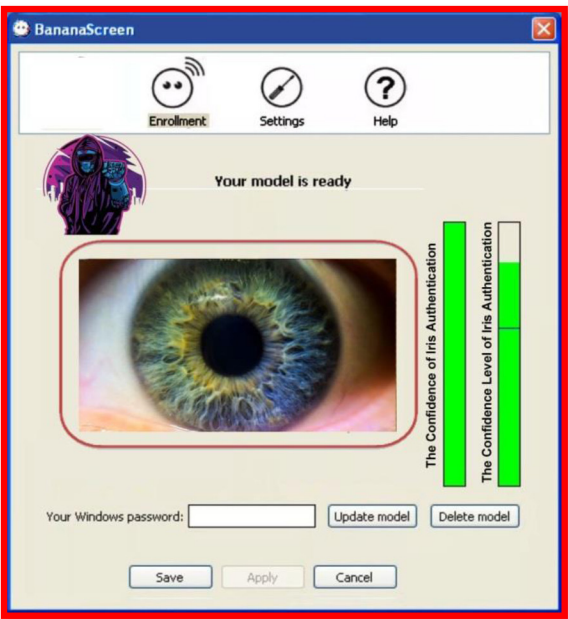


Figure 4
Scanning the iris of the eye

Table 1
Comparing the existing system with the proposed system

Designs	A Fine-Grained Approach to Access Control	Authentication as a means of protecting privacy
Implementation of the System	Decide	Confirmation
A proposal for a system	Bank system that is flexible and agreed upon	A model of accounting that includes complete verification and approval

8. Discussion and Conclusion

Biometric authentication has several advantages over conventional password-based authentication, according to the document’s conclusion. As a result, biometric traits, such as iris patterns, are unique, stable, and practically impossible to replicate, as opposed to passwords and pins. Unlike fingerprints and facial recognition, the iris recognition technology utilized in the proposed system is more accurate and reliable. With iris

recognition, security is enhanced and environmental or physical factors are less likely to impact it. According to the conclusion, image processing, segmentation, feature extraction, and feature matching are employed as part of the implementation process. Authentication is made secure using these processes. The document addresses potential challenges as well, including the irrevocability of biometric data. A compromised biometric template cannot be reset, unlike a password, making its protection essential. As part of the discussion, encryption and secure storage are stressed as ways to prevent misuse of personal information.

References

- [1] G. Gorgani, "The effect of e-banking on bank customers' deposits," *International Journal of Humanities and Cultural Studies*, vol. 1, no. 1, pp. 2231–2246 (2016).
- [2] L. Sharma and M. Mathuria, "Mobile banking transaction using fingerprint authentication," in *2018 2nd International Conference on Inventive Systems and Control (ICISC)*, IEEE, 2018, pp. 1300–1305. Accessed: Dec. 20 (2024).
- [3] A. Roy, N. Memon, and A. Ross, "Masterprint: Exploring the vulnerability of partial fingerprint-based authentication systems," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 9, pp. 2013–2025 (2017).
- [4] M. M. S. Rani and K. R. Euphrasia, "Data security through QR code encryption and steganography," *Advanced Computing: An International Journal (ACIJ)*, vol. 7, no. 1/2, pp. 1–7 (2016).
- [5] R. Bala, "Technology Infrastructure Management in Banks 2020–Agenda for Future," vol. 6, pp. 416–423 (2020).
- [6] A. M. S. E. Saad, "A Systematical Review Study to Investigate the Use of Biometric Security Techniques in Automatic Teller Machines: Insight from the Past 15 Years," in *2019 1st International Informatics and Software Engineering Conference (UBMYK)*, IEEE, 2019, pp. 1–4. Accessed: Dec. 20 (2024).
- [7] H. Lasisi and A. A. Ajisafe, "Development of stripe biometric based fingerprint authentications systems in Automated Teller Machines," in *2012 2nd International Conference on Advances in Computational Tools for Engineering Applications (ACTEA)*, IEEE, 2012, pp. 172–175. Accessed: Dec. 20 (2024).

- [8] M. Karnan, M. Akila, and N. Krishnaraj, "Biometric personal authentication using keystroke dynamics: A review," *Applied Soft Computing*, vol. 11, no. 2, pp. 1565–1573 (2011).
- [9] L. O’Gorman, "Comparing passwords, tokens, and biometrics for user authentication," *Proceedings of the IEEE*, vol. 91, no. 12, pp. 2021–2040 (2003).
- [10] D. Pradeep, M. Naveena, K. Sharmi, and N. Yogi, "Security Enhancement for ATM Machine Using Mobile Application and IoT Technology," in *2024 5th International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV)*, IEEE, 2024, pp. 673–679. Accessed: Dec. 20 (2024).
- [11] R. W. Taylor, E. J. Fritsch, J. Liederbach, M. R. Saylor, and W. L. Tafoya, *Cyber Crime and Cyber Terrorism*. Pearson, New York, NY, 2019. Accessed: Dec. 20 (2024).
- [12] M. Umanailo, R. Hamid, and A. R. S. Putra, "Cybercrime case as impact development of communication technology that troubling society," *International Journal of Scientific & Technology Research*, vol. 8, no. 9, pp. 1224–1228 (2019).
- [13] T. Sabhanayagam, V. P. Venkatesan, and K. Senthamarai Kannan, "A comprehensive survey on various biometric systems," *International Journal of Applied Engineering Research*, vol. 13, no. 5, pp. 2276–2297 (2018).
- [14] S. Khan, S. Parkinson, L. Grant, N. Liu, and S. McGuire, "Biometric Systems Utilising Health Data from Wearable Devices: Applications and Future Challenges in Computer Security," *ACM Computing Surveys*, vol. 53, no. 4, pp. 1–29 (Jul. 2021), doi: 10.1145/3400030.
- [15] T. V. Bakunova, E. A. Trofimova, and E. V. Lapteva, "Biometrics as a method of information security in the banking sector digitalization," in *International Scientific and Practical Conference on Digital Economy (ISCDE 2019)*, Atlantis Press, 2019, pp. 929–934. Accessed: Dec. 20 (2024).
- [16] F. Casino, T. K. Dasaklis, and C. Patsakis, "A systematic literature review of blockchain-based applications: Current status, classification and open issues," *Telematics and Informatics*, vol. 36, pp. 55–81 (2019).
- [17] N. Ansaripour, A. Heidari, and S. A. Eftekhari, "Multi-objective optimization of residual stresses and distortion in submerged arc welding process using Genetic Algorithm and Harmony Search," *Proceedings of the Institution of Mechanical Engineers, Part C: Journal of*

- Mechanical Engineering Science*, vol. 234, no. 4, pp. 862–871 (Feb. 2020), doi: 10.1177/0954406219885977.
- [18] O. A. Daniali, D. Toghraie, and S. A. Eftekhari, “Thermo-hydraulic and economic optimization of Iranol refinery oil heat exchanger with Copper oxide nanoparticles using MOMBO,” *Physica A: Statistical Mechanics and its Applications*, vol. 540, p. 123010 (2020).
 - [19] J. Lee, J. Woo, C. Lee, and K. Joo, “A software development methodology for secure web application,” *International Journal on Advanced Science, Engineering and Information Technology*, vol. 9, no. 1, pp. 336–341 (2019).
 - [20] M. Wazid, S. Zeadally, and A. K. Das, “Mobile banking: Evolution and threats: Malware threats and security solutions,” *IEEE Consumer Electronics Magazine*, vol. 8, no. 2, pp. 56–60 (2019).
 - [21] M. V. Prakash, P. A. Infant, and S. J. Shobana, “Eliminating vulnerable attacks using one time password and passtext analytical study of blended schema,” *Universal Journal of Computer Science and Engineering Technology*, vol. 1, no. 2, pp. 133–140 (2010).
 - [22] P. Rani and R. Sharma, “Intelligent transportation system for internet of vehicles based vehicular networks for smart cities,” *Computers and Electrical Engineering*, vol. 105, p. 108543 (2023).
 - [23] P. Rani and R. Sharma, “IMFOCA-IOV: Intelligent Moth Flame Optimization based Clustering Algorithm for Internet of Vehicle,” in *2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, IEEE, 2023, pp. 1–6. Accessed: Nov. 09 (2024).
 - [24] R. Bose, S. Chakraborty, and S. Roy, “Explaining the workings principle of cloud-based multi-factor authentication architecture on banking sectors,” in *2019 Amity International Conference on Artificial Intelligence (AICAI)*, IEEE, 2019, pp. 764–768. Accessed: Dec. 20, 2024. R. A. Leite, J. L. D. Comba, and J. L. D. Comba, “Eva: Visual analytics to identify fraudulent events,” *IEEE Transactions on Visualization and Computer Graphics*, vol. 24, no. 1, pp. 330–339 (2017).
 - [25] P. Rani, S. Verma, S. P. Yadav, B. K. Rai, M. S. Naruka, and D. Kumar, “Simulation of the lightweight blockchain technique based on privacy and security for healthcare data for the cloud system,” *International Journal of E-Health and Medical Communications (IJEHMC)*, vol. 13, no. 4, pp. 1–15 (2022).

Received July, 2024