Vol 6, Issue 3, March 2026 www.ijesti.com E-ISSN: 2582-9734
International Journal of Engineering, Science, Technology and Innovation (IJESTI)

Biometric-Based Multi-Factor Authentication for Secure Digital Access

Poonam
Research Scholar, Department of Computer Science & Engineering,
CBS Group of Institutions, Jhajjar, Haryana, India.

Dr. Amreesh Kumar Yadav
Assistant Professor, Department of Computer Science & Engineering, CBS Group of Institutions,
Jhajjar, Haryana, India.

ABSTRACT

Authentication is an important security process used to verify the identity of users before allowing access to digital systems, applications, networks, or services. In the present digital environment, traditional authentication methods such as passwords, PINs, and security questions are becoming less effective because they can be stolen, guessed, shared, or hacked through phishing, brute-force attacks, and other cyber threats. To overcome these limitations, biometric authentication and multi-factor verification provide a stronger and more reliable security approach. Biometric authentication uses unique physical or behavioural characteristics such as fingerprint, face, iris, voice, palm print, and keystroke pattern to verify genuine users. Multi-factor authentication adds additional security layers by combining something the user knows, something the user has, and something the user is. The combination of biometrics and multi-factor verification reduces unauthorized access, improves identity protection, and strengthens overall system reliability. Machine learning techniques can further improve authentication performance by detecting suspicious behaviour, classifying genuine and unauthorized users, and reducing false acceptance and false rejection rates. This study focuses on developing secure authentication protocols using biometrics and multi-factor verification to provide better accuracy, privacy, and protection against cyberattacks in modern digital systems.

Keywords: *Biometric Authentication, Multi-Factor Verification, Secure Authentication, Cybersecurity.*

1. INTRODUCTION

Authentication is one of the most important components of information security because it ensures that only genuine and authorized users are allowed to access a digital system, network, application, or service. In the present digital era, where online banking, e-governance, healthcare systems, cloud computing, mobile applications, smart devices, and organizational databases are widely used, the protection of user identity has become a major concern. Traditional authentication methods such as passwords, PINs, and security questions are still commonly used, but these methods are no longer sufficient to provide strong security because they can be easily guessed, stolen, forgotten, shared, or exposed through phishing attacks, brute-force attacks, keylogging, shoulder surfing, and social engineering. As cyber threats are becoming more advanced, there is a growing need for secure authentication protocols that can provide higher accuracy, stronger identity verification, and better protection against unauthorized access. Biometric authentication has emerged as an effective solution because it verifies a person on the basis of unique biological or behavioural characteristics such as fingerprint, face, iris, voice, palm print, signature, or keystroke pattern. These biometric traits are difficult to duplicate and are directly linked with the physical identity of the user, making them more reliable than knowledge-based authentication methods [1]. However, biometric systems also have certain limitations such as false acceptance, false rejection, spoofing attacks, sensor errors, poor-quality input, and privacy concerns. Therefore, using biometrics alone may not be sufficient in highly sensitive security environments. To overcome these limitations,

multi-factor verification is introduced as a stronger approach, where two or more authentication factors are combined to verify the user. These factors generally include something the user knows, such as a password or PIN; something the user has, such as an OTP, smart card, or registered mobile device; and something the user is, such as fingerprint, face, or iris. By combining biometric verification with multi-factor authentication, the security level of the system can be significantly improved because even if one factor is compromised, the attacker still cannot gain access without passing the remaining verification stages. The development of secure authentication protocols using biometrics and multi-factor verification is therefore an important area of research in modern cybersecurity. Such protocols can help reduce unauthorized access, improve user identification accuracy, protect confidential data, and enhance trust in digital services. In addition, machine learning techniques can also be applied to analyze authentication patterns, classify genuine and unauthorized users, detect suspicious behaviour, and improve the overall performance of the authentication system. The present study focuses on developing and analyzing a secure authentication protocol that integrates biometric features with multi-factor verification to provide a reliable, efficient, and user-friendly security mechanism. It also highlights the importance of combining password-based authentication, OTP verification, and biometric recognition to create a layered security system that is more resistant to cyberattacks and identity fraud [2-5]. Thus, the study aims to contribute to the field of information security by presenting a stronger authentication approach suitable for modern digital applications where privacy, accuracy, and secure access control are essential.

1.1 Importance of Secure Authentication

Secure authentication is very important in modern digital systems because it protects sensitive information from unauthorized access. In today's world, people use digital platforms for online banking, shopping, healthcare services, education, government services, cloud storage, social media, and official communication. These systems store personal data, financial details, passwords, identity records, medical information, and confidential documents. If authentication is weak, attackers can easily enter the system and misuse this information. Therefore, secure authentication helps to verify whether the user is genuine before giving access to any digital service.

The importance of secure authentication has increased because cybercrimes such as identity theft, phishing, password hacking, data breaches, and financial fraud are growing rapidly. Traditional password-based systems are not always safe because passwords can be guessed, stolen, shared, or cracked by attackers. A strong authentication system reduces these risks by using advanced methods such as biometric verification, OTP, smart cards, registered devices, and multi-factor authentication. These methods create multiple layers of security and make it difficult for unauthorized users to access the system.

Secure authentication also helps organizations maintain privacy, trust, and data integrity. In banks, it protects financial transactions; in healthcare, it protects patient records; in educational institutions, it secures student data; and in government systems, it prevents misuse of official information. It also helps organizations follow security policies and legal requirements related to data protection. When users know that their accounts and personal data are protected, they develop greater confidence in digital services [6].

In biometric and multi-factor authentication systems, secure authentication becomes even stronger because it combines different verification factors. For example, a user may be required to enter a password, verify an OTP, and provide a fingerprint or face scan. Even if one factor is compromised, the attacker cannot easily pass all verification stages. Thus, secure authentication is essential for preventing unauthorized access, protecting confidential data, reducing cyber threats, and ensuring safe use of digital technologies.

1.2 Limitations of Traditional Authentication

Traditional authentication methods, such as passwords, Personal Identification Numbers (PINs), and security questions, have been widely used for many years to verify the identity of users. Although these methods are simple, inexpensive, and easy to implement, they are no longer sufficient to provide strong security in modern digital environments. The rapid growth of cyber threats, online transactions, cloud computing, mobile applications, and Internet of Things (IoT) devices has exposed several weaknesses in traditional authentication systems.

One of the major limitations of password-based authentication is that users often create weak or easily predictable passwords. Many users choose simple passwords based on names, birthdays, or common words, making them vulnerable to dictionary attacks and brute-force attacks. Even strong passwords may be compromised through phishing attacks, keylogging malware, shoulder surfing, or database breaches. Additionally, users frequently reuse the same password across multiple websites and applications, increasing the risk that a single compromised password can expose several accounts.

PIN-based authentication also has limitations because PINs are generally short and easy to guess or observe. Attackers can obtain PINs through observation, social engineering, or repeated guessing attempts. Similarly, security questions often rely on personal information that may be publicly available or easily discovered through social media and other online sources.

Traditional authentication methods also create usability challenges. Users are expected to remember multiple usernames, passwords, and PINs for different accounts, which often leads to forgotten credentials and frequent password reset requests. This increases administrative costs and reduces user convenience. Furthermore, traditional authentication verifies only the knowledge of secret information and cannot confirm the actual physical identity of the person attempting to log in. If an attacker obtains the correct password or PIN, the system may incorrectly grant access without detecting the unauthorized user [7].

Another important limitation is that traditional authentication methods provide only a single layer of security. Once the password is compromised, the entire authentication process fails. They also offer limited protection against advanced cyberattacks such as credential stuffing, replay attacks, session hijacking, and identity theft. As digital systems continue to evolve, these limitations demonstrate the need for stronger authentication mechanisms that combine biometric verification and multi-factor authentication to improve security, reliability, and user trust.

1.3 Role of Biometric Authentication

Biometric authentication plays an important role in developing secure authentication protocols because it verifies a user on the basis of unique physical or behavioural characteristics. Unlike traditional methods such as passwords, PINs, or security questions, biometric features are directly linked to the identity of a person. These features include fingerprint, face, iris, retina, voice, palm print, hand geometry, signature pattern, and keystroke behaviour. Since biometric traits are naturally present in an individual and are difficult to copy, forget, share, or steal, they provide a stronger level of identity verification than traditional authentication methods.

The main role of biometric authentication is to confirm that the person trying to access a system is the genuine user. In password-based systems, access is granted if the correct password is entered, even if the person entering it is an attacker. However, biometric authentication checks the actual biological or behavioural identity of the user. For example, a fingerprint scanner verifies the fingerprint pattern, a face recognition system checks facial features, and an iris recognition system identifies the unique pattern of the eye. This makes biometric authentication more reliable for preventing unauthorized access.

Biometric authentication also improves convenience for users. Users do not need to remember complex passwords or carry physical tokens every time they log in. A fingerprint scan, face scan, or voice command can provide quick and easy access. This is especially useful in mobile banking, healthcare systems, government services, attendance systems, smart devices, and cloud-based applications. Biometric systems can also reduce problems related to forgotten passwords and repeated password reset requests.

In secure authentication protocols, biometrics can be used as a single authentication method or as one factor in a multi-factor authentication system. When combined with password and OTP verification, biometrics provide an additional security layer. Even if an attacker steals a password or obtains an OTP, access cannot be granted without the user's biometric verification. Therefore, biometrics strengthen multi-factor authentication by adding the factor of "something the user is."

Biometric authentication also supports fraud detection and identity protection. It helps prevent impersonation, fake identity use, unauthorized login, and credential theft. In high-security areas such as banking, defense, healthcare, airports, and official databases, biometric verification ensures that only genuine users are allowed access. However, biometric systems must be designed carefully because they may face challenges such as spoofing attacks, poor-quality input, false acceptance, false rejection, and privacy concerns. Therefore, secure storage of biometric data, encryption, liveness detection, and machine learning-based verification methods are important for improving biometric system reliability [8].

Thus, biometric authentication plays a central role in modern security systems by improving accuracy, reliability, convenience, and protection against unauthorized access. In the development of secure authentication protocols using biometrics and multi-factor verification, biometrics act as a powerful identity verification tool that strengthens overall system security and increases user trust in digital services.

1.4 Combination of Biometrics and MFA

The combination of biometrics and multi-factor authentication is an effective approach for developing secure authentication protocols. Biometric authentication verifies the user through unique physical or behavioural characteristics such as fingerprint, face, iris, voice, palm print, or keystroke pattern, while multi-factor authentication adds extra verification layers using different security factors. These factors generally include something the user knows, such as a password or PIN; something the user has, such as an OTP, smart card, or registered mobile device; and something the user is, such as a biometric trait. When these factors are combined, the authentication system becomes stronger, more reliable, and more difficult for attackers to break.

The main advantage of combining biometrics with MFA is that it reduces the weakness of single-factor authentication. In a password-only system, an attacker can gain access if the password is stolen or guessed. Similarly, OTP-based authentication may also be compromised if the attacker gains control of the user's mobile device or SIM card. However, when biometric verification is added to the authentication process, the system checks the actual identity of the user. Even if an attacker knows the password or receives the OTP, access cannot be granted without matching the user's biometric feature. This creates a layered security mechanism that improves protection against unauthorized access.

In a biometric-based MFA system, authentication may take place in different stages. First, the user enters a password or PIN. Second, the system verifies an OTP sent to the registered mobile number or email. Third, the user provides biometric input such as fingerprint or face scan. If all three factors are successfully verified, the system allows access. If any factor fails, the system denies access or sends an alert. This step-by-step process helps prevent identity theft, account misuse, phishing attacks, credential theft, and fraudulent login attempts.

The combination of biometrics and MFA is especially useful in high-security applications such as online banking, healthcare systems, government portals, cloud services, educational platforms, defence systems, smart offices, and mobile applications. It protects confidential data and ensures that only genuine users can access sensitive services. This approach also improves user trust because users feel more secure when their accounts are protected by multiple verification layers.

Machine learning can further improve the performance of biometric and MFA-based systems. It can analyse login behaviour, detect abnormal access patterns, classify genuine and unauthorized users, and reduce false acceptance and false rejection rates. For example, if a user logs in from an unusual device or location, the system can request additional biometric verification. In this way, biometrics and MFA can work together with intelligent detection techniques to provide adaptive and secure authentication.

Thus, the combination of biometrics and multi-factor authentication provides a strong security framework for modern digital systems. It overcomes the limitations of passwords and OTPs by adding biometric identity verification. This layered approach improves accuracy, reliability, privacy protection, and resistance against cyberattacks. Therefore, biometric-based MFA is considered one of the most effective methods for developing secure authentication protocols in today's digital environment [9].

2. RELATED REVIEWS

Rajeh et al. (2026) examined the security challenges associated with smart home environments, where devices such as smart televisions, refrigerators, and locks had been connected to the Internet for improving daily convenience. The study highlighted that communication through public channels had exposed user data to several security threats, making privacy protection a major concern. The authors proposed a lightweight authentication scheme that combined biometric data with cryptographic techniques to provide secure access with low computational overhead. The scheme had enabled mutual authentication among users, gateways, and smart devices. Formal analysis using the Real-or-Random model had demonstrated its resistance against polynomial-time adversaries, while informal analysis had shown protection against attacks such as eavesdropping and fault analysis. The performance results indicated low memory use, CPU consumption, execution time, and communication cost. Therefore, the study suggested that the proposed scheme had offered an efficient, robust, and practical solution for securing smart home networks.

Sharma and Kumar (2026) examined the security challenges of wireless sensor networks and emphasized that WSNs had required decentralized authentication authority for secure, transparent, and efficient data migration among network nodes. The study had noted that WSNs were highly vulnerable to network attacks because of their limited sensor resources, including low processing power, restricted storage, and limited bandwidth. To address these issues, the authors had proposed the CurveGuard Multifactor Authentication Protocol (CGMFAP), which included user and sensor registration, login, password renewal, biometric renewal, and revocation phases. They had also introduced an Enhanced Elliptic Curve Integrated Encryption Scheme using redefined key matrix negotiation and matrix multiplication for secure communication. The use of a hyper-chaotic Lorenz generator had further improved diffusion and resistance against attacks. Through BAN logic analysis, the protocol had been found secure, efficient, and capable of reducing computational and communication overhead in WSN operations.

de Jesus Sousa and Gondim (2025) had examined the growing significance of the Internet of Drones (IoD) in response to the increasing use of unmanned aerial vehicles across sectors such as military operations, rescue services, agriculture, and entertainment. They had explained that IoD systems involved multiple drones operating in different flight zones to perform specific tasks, mainly real-time data collection and communication with users through mobile devices. The authors had emphasized that,

because these systems transmitted sensitive information through public communication channels, privacy and security concerns had become critical. They had argued that authentication protocols were necessary to ensure secure communication and to prevent attacks such as replay and man-in-the-middle attacks. The study had proposed a biometric and elliptic curve cryptography-based user authentication scheme for IoD. Its security analysis and AVISPA verification had shown resistance to known attacks while providing anonymity, authenticity, untraceability, and improved computational performance.

Alshehri (2025) introduced a Multi-Factor Authentication System that was designed to enhance data security in IoT-based healthcare devices. The study explained that the proposed system had integrated several advanced algorithms, including the Multi-Factor Authentication Algorithm, Biometric Template Protection Algorithm, Dynamic Risk-Based Authentication Algorithm, Adaptive Biometric Fusion Algorithm, and Context-Aware Access Control Algorithm. It was reported that these algorithms had worked together to provide strong, adaptive, and context-aware authentication for healthcare environments. The comparative analysis indicated that the proposed system had consistently performed better than existing authentication methods. The ablation study further showed that each algorithm had contributed significantly to the overall effectiveness of the framework. The study suggested that the combined approach had strengthened user authentication and improved protection against security threats. Overall, the work highlighted that the proposed system had offered a promising solution for emerging data security challenges in IoT healthcare systems.

Arpitha et al. (2024) examined the role of secure authentication in IoT-based healthcare systems, particularly in the Telecare Medicine Information System (TMIS). The study highlighted that the transmission of sensitive patient information through insecure Internet channels had created serious privacy and security challenges. It was observed that mutual authentication between patients and medical servers was essential for protecting medical data and ensuring system reliability. The researchers proposed a three-factor authentication scheme based on passwords, smart cards, and biometrics. Elliptic Curve Cryptography (ECC) was used because it offered strong security with a smaller key size, while biometric verification was strengthened through Fuzzy Extractor technology. The scheme also enabled registered users to change passwords without revealing their identity to the server. Security verification was carried out using BAN logic. The study concluded that the proposed method provided privacy protection, mutual authentication, session key agreement, and lower computation and communication costs compared with existing techniques.

Ayeswarya and Singh (2024) examined the significance of authentication systems in strengthening security against unauthorized access and impersonation attacks. They observed that conventional authentication mechanisms had often failed to provide continuous protection, which increased system vulnerability. The study highlighted Continuous Authentication Systems (CAS) as an effective approach for adapting dynamically to changing security threats. The authors reviewed recent developments, trends, and challenges related to CAS design and implementation. They reported that supervised learning methods, especially score-level fusion techniques, had been widely used in CAS classification. However, they noted that comparative studies on different biometric combinations, such as physiological, behavioural, and multimodal biometrics, had remained limited. The review further indicated that most studies had focused mainly on accuracy measures like FRR, FAR, and EER, while usability, scalability, and security had received less attention. The authors suggested that real-world evaluation was necessary for improving CAS effectiveness.

Chen and Chen (2023) stated that the Telecare Medicine Information System (TMIS) had emerged as an important medical model that used communication and information technologies for remote diagnosis, treatment, and healthcare services. They explained that, because TMIS operated through an insecure public Internet environment, several mutual authentication and key agreement protocols had been developed to protect patient privacy. The authors reviewed the scheme proposed by Ostad-Sharif et al.

and reported that it had suffered from limitations related to strong authentication, inefficient password change, and vulnerability to offline password-guessing attacks. To address these weaknesses, they proposed a biometrics-based mutual authentication and key agreement protocol for TMIS by using one-way hash functions and elliptic curve cryptography. They further claimed that the proposed scheme had been formally verified under the random oracle model and had shown resistance against known attacks. Their findings indicated reduced computation cost and communication overhead.

Pahlevi et al. (2022) stated that the rapid development of the Internet of Things had expanded across various sectors, while the number of IoT devices was expected to reach 75 billion by 2025. They observed that this growth had not been accompanied by adequate security improvements, which made IoT devices vulnerable to cyber-attacks such as brute force and sniffing attacks. The authors explained that authentication mechanisms could reduce such threats, but their implementation on IoT devices remained difficult because most devices had limited computational capacity. They argued that conventional authentication methods were not suitable for constrained IoT environments. Therefore, they proposed a secure mutual authentication protocol based on two-factor authentication using RFID and fingerprint with the MQTT protocol. The study included registration and authentication processes. The findings indicated that the proposed protocol achieved optimal FAR and FRR at an 80% threshold and showed resistance against brute force and sniffing attacks.

Yang et al. (2021) reviewed the role of biometrics in improving security within Internet of Things (IoT) environments, where a large number of smart devices required continuous interaction with users and other devices. The study indicated that biometrics had offered significant possibilities for enhancing both usability and security in IoT systems. The authors had mainly focused on two major aspects, namely authentication and encryption. In relation to authentication, they discussed biometric-based authentication systems and classified them according to various biometric traits and the number of traits used. Regarding encryption, they examined biometric-cryptographic systems that had combined biometric features with cryptographic techniques to strengthen IoT security. The review also identified several challenges related to the application of biometrics in IoT and discussed possible solutions. Overall, the study had contributed to understanding current research trends and future directions in biometric-based IoT security.

Tarannum et al. (2020) examined multimodal biometrics as an emerging approach for ensuring distributed data security. The study stated that single-user and multi-user data authentication had become important in commercial and e-governance applications. It was observed that earlier biometric security systems mainly focused on securing single-user data and were often dependent on static initialization parameters and fixed multimodal biometric features. The authors further indicated that traditional multimodal biometric authentication schemes did not adequately consider dynamic changes in integrity verification. To address these limitations, they proposed a multi-user multimodal authentication framework for large image data. The framework used iris, facial, and fingerprint features to identify the unique integrity of users for authentication and security. The study also introduced an integrity computational algorithm and encryption technique to strengthen data verification. The findings showed that the proposed model achieved improved integrity verification with nearly 7% computational integrity bit change and 5% runtime efficiency.

Banerjee et al. (2019) had examined the development of remote user authentication schemes and observed that researchers had been continuously attempting to strengthen authentication protocols since the concept was first introduced in 1981. The study had highlighted that many scholars had incorporated advanced security features to improve user authentication mechanisms. Banerjee et al. had particularly reviewed the scheme proposed by Turkanovic et al. (2014), which had used smart cards for authenticating

users in an IoT-based wireless sensor network environment. The authors had argued that the earlier scheme could not resist several possible security attacks and had contained various security weaknesses. To address these limitations, they had proposed an enhanced biometric-based user authentication technique. Their proposed protocol had not only overcome the flaws of the earlier scheme but had also reduced computational overhead. The study had further verified mutual authentication and session key secrecy through the ProVerif simulation tool.

3. CONCLUSION

Secure authentication has become an essential requirement in the modern digital world because users, organizations, and institutions depend heavily on online systems for communication, banking, healthcare, education, cloud storage, government services, and business operations [9]. Traditional authentication methods such as passwords, PINs, and security questions are no longer sufficient to protect sensitive data because they can be guessed, stolen, shared, or compromised through phishing, brute-force attacks, keylogging, and social engineering. These weaknesses show the need for advanced authentication mechanisms that can provide stronger identity verification and better protection against unauthorized access [10].

Biometric authentication offers an effective solution because it verifies users through unique physical or behavioural characteristics such as fingerprint, face, iris, voice, palm print, and keystroke pattern. Since these traits are directly connected with the identity of a person, they are more difficult to duplicate or misuse compared to traditional passwords. However, biometrics alone may also face challenges such as spoofing attacks, false acceptance, false rejection, sensor errors, and privacy concerns. Therefore, combining biometrics with multi-factor authentication provides a more secure and reliable approach.

The integration of biometric verification with multi-factor authentication creates a layered security system. In this system, the user may be required to provide a password, verify an OTP, and complete biometric recognition before gaining access. Even if one factor is compromised, the remaining factors continue to protect the system. This reduces the chances of identity theft, unauthorized login, account misuse, and data breaches. Such a system is especially useful in high-security areas like banking, healthcare, government portals, cloud services, mobile applications, and organizational networks.

Machine learning can further strengthen authentication protocols by analyzing user behaviour, detecting suspicious login patterns, and classifying genuine and unauthorized users more accurately. It can also help reduce false acceptance and false rejection rates, making the system more efficient and user-friendly. Thus, the development of secure authentication protocols using biometrics and multi-factor verification provides a strong framework for improving digital security [11].

In conclusion, biometric-based multi-factor authentication is a powerful and reliable method for protecting modern digital systems. It overcomes the limitations of traditional authentication by combining identity-based verification with multiple security layers. The proposed approach improves accuracy, reliability, privacy, and resistance against cyberattacks. Therefore, secure authentication protocols using biometrics and multi-factor verification are highly important for ensuring safe access control and building user trust in the digital environment.

REFERENCES

1. Rajeh, Z. M., Alhomdy, S. A., Thabit, F., & Maodah, K. A. (2026). A secure authentication scheme for smart home environments: a biometric-driven approach. *Frontiers in Computer Science*, *8*, 1669659.
2. Sharma, S., & Kumar, B. (2026). Enhancing Security in Wireless Sensor Networks through Curve Guard Multifactor Authentication Protocol. *IETE Journal of Research*, 1-18.

3. de Jesus Sousa, M., & Gondim, P. R. L. (2025). A multi-factor user authentication protocol for the internet of drone's environment. *Peer-to-Peer Networking and Applications*, *18*(2), 69.
4. Alshehri, H. (2025, March). Developing Multi-Factor Authentication and Biometric Verification Protocols for Enhancing Data Security in IoT Healthcare Devices. In *2025 17th International Conference on Computer and Automation Engineering (ICCAE)* (pp. 367-373). IEEE.
5. Arpitha, T., Chouhan, D., & Shreyas, J. (2024). Anonymous and robust biometric authentication scheme for secure social IoT healthcare applications. *Journal of Engineering and Applied Science*, *71*(1), 8.
6. Ayeswarya, S., & Singh, K. J. (2024). A comprehensive review on secure biometric-based continuous authentication and user profiling. *IEEe Access*, *12*, 82996-83021.
7. Chen, Y., & Chen, J. (2023). A biometrics-based mutual authentication and key agreement protocol for TMIS using elliptic curve cryptography. *Multimedia Tools and Applications*, *82*(11), 16009-16032.
8. Pahlevi, R. R., Suryani, V., Nuha, H. H., & Yasirandi, R. (2022, August). Secure two-factor authentication for iot device. In *2022 10th International Conference on Information and Communication Technology (ICoICT)* (pp. 407-412). IEEE.
9. Yang, W., Wang, S., Sahri, N. M., Karie, N. M., Ahmed, M., & Valli, C. (2021). Biometrics for internet-of-things security: A review. *Sensors*, *21*(18), 6163.
10. Tarannum, A., Rahman, Z. U., Rao, L. K., Srinivasulu, T., & Lay-Ekuakille, A. (2020). An efficient multi-modal biometric sensing and authentication framework for distributed applications. *IEEE Sensors Journal*, *20*(24), 15014-15025.
11. Banerjee, S., Chunka, C., Sen, S., & Goswami, R. S. (2019). An enhanced and secure biometric based user authentication scheme in wireless sensor networks using smart cards. *Wireless Personal Communications*, *107*(1), 243-270.