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

# A Study on Secure Digital Authentication Using Biometrics and Machine Learning

**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

The present study entitled "Developing Secure Authentication Protocols Using Biometrics and Multi-Factor Verification" focuses on improving the security, accuracy, and reliability of digital authentication systems. Traditional authentication methods such as passwords and PINs are no longer sufficient because they are vulnerable to guessing, theft, phishing, sharing, and unauthorized misuse. To overcome these limitations, this study proposes a secure authentication framework that combines biometric verification and multi-factor authentication. The proposed system uses multiple parameters such as fingerprint score, face match score, iris match score, password strength, OTP verification, device trust score, liveness detection, login attempts, and location risk score. These factors are used to classify users as genuine or unauthorized. The study also evaluates the performance of different authentication methods with and without machine learning. The results show that single-factor authentication provides lower accuracy, while the combination of password, biometric verification, and OTP achieves the highest accuracy of 99%. Machine learning algorithms such as Logistic Regression, Support Vector Machine, Random Forest, Gradient Boosting, and MLP Neural Network were also applied to improve classification performance. Among these, Logistic Regression and MLP Neural Network showed excellent performance in terms of accuracy, precision, recall, and F1-score. The study concludes that biometric-based multi-factor authentication provides stronger protection against unauthorized access and can be effectively used in banking, healthcare, cloud computing, education, and other sensitive digital systems.

***Keywords:*** *Biometric Authentication, Multi-Factor Verification, Cyber Security, Machine Learning, Secure Authentication.*

## 1. INTRODUCTION

In the present digital age, authentication has become one of the most important elements of information security. Every day, millions of users access online services, mobile applications, banking platforms, healthcare portals, educational websites, government services, cloud storage systems, and social networking platforms. In all these digital environments, it is necessary to confirm whether the person trying to access the system is a genuine user or an unauthorized person [1]. Authentication is the process through which a system verifies the identity of a user before allowing access to protected data, services, or resources. Without proper authentication, confidential information may be exposed to cybercriminals, hackers, and unauthorized users. Therefore, the development of secure authentication protocols is essential for protecting user identity, maintaining privacy, and ensuring the safe use of digital systems.

The rapid expansion of digital technologies has created new opportunities as well as new security risks. Earlier, most services were accessed physically or through limited computer networks. However, today almost every important activity is connected to the internet. People use digital platforms for financial transactions, online shopping, digital payments, telemedicine, e-learning, official communication, and personal data storage. Organizations also depend heavily on digital systems for managing business

operations, customer records, employee data, research documents, and financial information. This increasing dependence on digital platforms has made authentication more critical than ever before. If a system fails to identify users accurately, sensitive information can be stolen, modified, or misused. As a result, strong and reliable authentication mechanisms are required to protect both individuals and organizations.

Traditional authentication methods mainly depend on passwords, PINs, and security questions. These methods are simple and widely used, but they have several weaknesses. Passwords can be forgotten, guessed, stolen, shared, or cracked through brute-force attacks. Many users create weak passwords because they want them to be easy to remember. Some users reuse the same password across multiple websites, which increases the risk of account compromise. If one account is hacked, attackers may try the same password on other platforms. Security questions also have limitations because answers may be easily guessed or discovered through social media and public information. PINs are short and can be observed or stolen. Due to these weaknesses, password-based authentication alone is no longer sufficient for modern security requirements.

Cyber threats have become more advanced with the growth of digital services. Attackers use techniques such as phishing, malware, keylogging, credential stuffing, identity theft, social engineering, and database breaches to gain unauthorized access. Phishing attacks deceive users into entering their passwords on fake websites. Malware can secretly collect login credentials from infected devices. Keyloggers record the keys typed by users and capture passwords. Credential stuffing uses stolen username-password combinations from one service to attack other services. These threats show that traditional authentication systems are highly vulnerable when used alone. Therefore, stronger authentication protocols are needed to reduce the risk of unauthorized access and protect digital identity [2].

Biometric authentication has emerged as a powerful solution to many limitations of traditional authentication. Biometrics refers to the measurement and use of unique physical or behavioural characteristics of a person for identification or verification. Common biometric traits include fingerprints, face patterns, iris structures, voice features, palm prints, retina patterns, hand geometry, and behavioural features such as typing rhythm or walking style. Unlike passwords or PINs, biometric traits are directly connected to the individual. A fingerprint or iris pattern cannot be easily forgotten or shared like a password. This makes biometric authentication more convenient and secure in many situations. Biometric systems are now used in smartphones, laptops, banking applications, airports, offices, healthcare systems, and government identity programs.

Fingerprint recognition is one of the most commonly used biometric methods. It verifies a person by analyzing the unique patterns of ridges and valleys on the fingertip. Since fingerprint patterns are different for each individual, they provide a strong basis for identity verification. Facial recognition is another widely used biometric technology. It identifies a user by analyzing facial features such as the distance between the eyes, shape of the nose, jawline, and overall facial structure. Iris recognition uses the unique patterns in the colored part of the eye and is considered highly accurate. Voice recognition identifies a user based on vocal characteristics such as tone, pitch, and speaking pattern. Each biometric method has its own advantages and limitations, but all of them aim to make authentication more secure and user-friendly.

One of the major advantages of biometric authentication is that it reduces dependence on memorized secrets. Users do not need to remember complex passwords or carry additional tokens in many biometric systems. This improves convenience and reduces the burden on users. Biometrics also provides better accountability because access is linked to the actual physical or behavioural identity of the user. In workplaces, biometric attendance systems reduce proxy attendance. In banking and mobile payments,

biometric verification helps prevent unauthorized transactions. In healthcare systems, biometrics can help ensure that only authorized doctors, staff, or patients access sensitive medical records. These applications show that biometrics can play an important role in strengthening identity verification [3].

However, biometric authentication is not completely free from challenges. Biometric systems may face spoofing attacks, sensor errors, privacy concerns, and false recognition problems. Spoofing occurs when attackers try to fool the biometric system using fake fingerprints, photographs, masks, recorded voices, or other artificial samples. Sensor quality can also affect accuracy. Poor lighting may reduce the performance of face recognition systems, while dirty or damaged fingers may affect fingerprint scanning. Biometric systems may sometimes wrongly accept an unauthorized person or wrongly reject a genuine user. These errors are known as false acceptance and false rejection. In addition, biometric data is sensitive because it is permanently linked to a person. If a password is stolen, it can be changed, but if biometric data is compromised, it cannot be easily replaced. Therefore, biometric authentication must be designed carefully with strong protection mechanisms.

To overcome the weaknesses of single-factor authentication, multi-factor authentication has become an important security approach. Multi-factor authentication, also called MFA, verifies the identity of a user by using two or more different authentication factors. These factors are generally divided into three main categories: something the user knows, something the user has, and something the user is. Something the user knows includes passwords, PINs, or answers to security questions. Something the user has includes a mobile phone, smart card, hardware token, OTP device, or registered email account. Something the user is includes biometric traits such as fingerprint, face, iris, or voice. By combining different factors, MFA creates multiple layers of security.

The main strength of multi-factor authentication is that it does not depend on a single method of verification. Even if one factor is compromised, the attacker still needs to pass the remaining factors. For example, if a password is stolen, the attacker may still need an OTP sent to the registered mobile number and biometric verification from the genuine user. This layered approach makes unauthorized access much more difficult. MFA is widely used in banking, email services, cloud platforms, corporate networks, online payment systems, and government portals. It has become an important defence mechanism against identity theft and account takeover attacks.

The integration of biometrics with multi-factor authentication provides a strong and reliable authentication model. In such a system, biometric verification can be combined with passwords, OTPs, smart cards, device verification, or behavioural analysis. For example, a user may first enter a username and password, then verify an OTP received on a registered mobile device, and finally complete fingerprint or face recognition. Only after all these steps are successfully completed will the system grant access. This type of authentication protocol increases confidence that the person accessing the system is the genuine user. It also reduces the chances of unauthorized access because an attacker must compromise multiple independent security factors [4].

Developing secure authentication protocols using biometrics and multi-factor verification requires careful planning and design. A protocol must be secure, accurate, efficient, user-friendly, and privacy-preserving. Security means the system should resist attacks such as replay attacks, spoofing attacks, phishing, brute-force attacks, and man-in-the-middle attacks. Accuracy means the system should correctly identify genuine users and reject unauthorized users. Efficiency means the authentication process should not take too much time or require excessive computational resources. User-friendliness means the system should be easy to use and should not create unnecessary difficulty for genuine users. Privacy preservation means the system should protect biometric data and personal information from misuse.

A secure biometric-based MFA system usually includes several important steps. First, the user registers with the system by providing basic identity information and biometric samples. During registration, the biometric data is captured and converted into a digital template. This template should be securely stored using encryption or other protection techniques. The system should avoid storing raw biometric images because they may create privacy risks. During login, the user provides required credentials such as password, OTP, or biometric input. The system then compares the new biometric sample with the stored template. If the match is successful and other authentication factors are verified, access is granted. If any factor fails, access is denied or additional verification may be required.

Security of biometric data is a very important concern in authentication protocol development. Biometric templates must be protected from theft, tampering, and unauthorized use. Encryption can be used to secure biometric templates during storage and transmission. Hashing, template protection, secure channels, and privacy-preserving techniques can also be applied. Access to biometric databases should be strictly controlled. Systems should also follow the principle of minimum data collection, which means only necessary biometric information should be collected and stored. Users should be informed about how their biometric data is used, stored, and protected. Transparency and consent are important for building user trust in biometric authentication systems.

Another important aspect of authentication protocol development is performance evaluation. The effectiveness of biometric and MFA systems can be measured using different parameters such as accuracy, precision, recall, F1-score, false acceptance rate, false rejection rate, authentication time, and security strength. False acceptance rate represents the chances of an unauthorized user being wrongly accepted by the system. False rejection rate represents the chances of a genuine user being wrongly rejected. A good authentication system should have low false acceptance and false rejection rates. It should also authenticate users quickly without reducing security. Machine learning and artificial intelligence can be used to improve biometric matching, detect suspicious behaviour, and enhance authentication accuracy.

The use of biometrics and MFA is especially important in sectors where data security is critical. In banking and financial services, secure authentication helps protect accounts, online transactions, and payment systems. In healthcare, it protects patient records, medical history, and hospital management systems. In education, it can secure online examination systems, student portals, and digital learning platforms. In government services, biometric MFA can support secure digital identity, welfare distribution, and citizen service portals. In corporate environments, it helps protect confidential files, internal networks, and employee systems. In smart devices and Internet of Things environments, secure authentication prevents unauthorized control of connected devices [5].

Despite its benefits, the implementation of biometric and multi-factor authentication must address social, ethical, and technical issues. Some users may be concerned about privacy and misuse of biometric data. Others may face difficulty using biometric systems due to physical disabilities, age-related changes, or sensor limitations. Environmental conditions may also affect biometric recognition. Therefore, authentication protocols should be inclusive and flexible. Alternative verification methods should be available for users who cannot use a particular biometric method. Systems should also be designed to avoid discrimination, bias, and unequal access. Ethical use of biometric data is necessary for the long-term success of these technologies.

The future of authentication is moving toward more intelligent, adaptive, and continuous security systems. Instead of verifying users only at the time of login, future systems may continuously monitor user behaviour, device patterns, location, and interaction style to detect unusual activity. Behavioural

biometrics such as keystroke dynamics, mouse movement, touchscreen gestures, and walking patterns may become more common. Artificial intelligence may help identify fraud attempts in real time. At the same time, privacy-enhancing technologies will become necessary to protect user rights. The combination of biometrics, MFA, artificial intelligence, encryption, and secure protocol design can create highly reliable authentication systems for the future.

In conclusion, developing secure authentication protocols using biometrics and multi-factor verification is an important step toward strengthening digital security. Traditional password-based systems are no longer sufficient because they are vulnerable to theft, guessing, phishing, and misuse. Biometric authentication offers a stronger method of identity verification by using unique human characteristics, while multi-factor authentication adds additional layers of protection. When biometrics and MFA are combined, they provide a more secure, reliable, and user-friendly authentication framework. Such systems can reduce unauthorized access, protect sensitive data, improve trust in digital services, and support secure online activities across different sectors. However, successful implementation requires proper attention to privacy, accuracy, usability, data protection, and ethical concerns. Therefore, this study focuses on the development of secure authentication protocols that integrate biometric technology with multi-factor verification to provide effective protection against modern cyber threats and ensure safe access to digital systems [6].

## 2. RELATED REVIEWS

**Jothimani et al. (2026)** had proposed a secure health data access system by integrating an AI-based centralized patient data management system with fingerprint biometric authentication. The study had focused on improving healthcare data security through a hybrid authentication technique that combined ORB descriptors and minutiae-based fingerprint features. These features had been fused at the feature level before being processed by a CNN classifier. The system had been designed to support scalability, secure communication, encrypted data transfer, and real-time authentication through a microservices architecture. The SOCOFing fingerprint dataset had been used for testing, and the CNN model had been evaluated through cross-validation against a baseline SVM classifier. The findings had indicated that the CNN outperformed the SVM in accuracy, precision, recall, and F1-score. The study had further reported low authentication time and reduced false acceptance and rejection rates, confirming the effectiveness of the hybrid biometric approach.

**Haleem et al. (2026)** examined the security challenges associated with the rapidly expanding Internet of Things (IoT), which had connected physical and virtual objects to enable automated services without direct human involvement. The study stated that the centralized architecture of IoT had created serious security concerns, including single points of failure, privacy risks, weak transparency, data integrity issues, and vulnerabilities across sensors, gateways, platforms, and infrastructure. The authors emphasized that effective IoT security had required strong mechanisms such as authentication, privacy protection, data integrity, resistance to malicious attacks, usability, and scalability. The survey had focused on biometrics and blockchain as two important approaches for strengthening IoT security. It further reviewed recent developments in IoT-based biometric systems, including authentication protocols, encryption methods, and privacy measures. The study also highlighted that combining blockchain with biometrics had offered a promising decentralized framework for improving transparency, security, and trust in IoT environments.

**Mohammed et al. (2025)** proposed an innovative multi-modal biometric authentication framework that had integrated deep learning techniques with zero-trust architecture principles to strengthen network access control. They explained that the framework had used a three-tier fusion strategy at feature, score,

and decision levels by combining facial, fingerprint, and iris recognition modalities. The authors reported that ResNet-50-based CNNs had been applied for facial recognition, CNN-based minutiae extraction for fingerprints, and 2D Gabor wavelets with deep learning features for iris analysis. Using LFW, CelebA, FVC2004, NIST SD14, CASIA Iris V4, and UBIRIS v2 datasets, the framework had achieved 99.47% authentication accuracy, 0.02% FAR, and 0.15% FRR. It had also reduced fraudulent access attempts by 68% and improved authentication time to 235 ms. The study concluded that the proposed model had offered a scalable, efficient, and secure solution for high-security network authentication environments.

**Lee et al. (2025)** had examined zero-trust architecture as an important advancement in cybersecurity and had highlighted the growing relevance of continuous authentication within this framework. The study had indicated that traditional static authentication mechanisms were insufficient to address modern network security threats, particularly identity spoofing and credential theft. It had further observed that previous studies had mainly emphasized either device-to-device authentication or user authentication, while both users and devices required equal attention in secure authentication systems. The researchers had also pointed out that user authentication fatigue remained a major challenge in continuous authentication practices. To address these issues, the study had proposed an unconsciously continuous authentication protocol based on zero-trust principles and behavioural biometrics. The protocol had used keystroke dynamics to continuously assess user trust levels and update communication keys. The findings had shown that the proposed protocol was robust and had achieved satisfactory experimental performance.

**Arman et al. (2024)** examined the growing challenges of identity authentication that had emerged due to the rapid expansion of smart technologies and digital services. The study stated that biometric credentials had increasingly been adopted for verification because they offered several advantages over traditional authentication methods. It further highlighted that the protection of biometric data privacy had become essential in different application contexts. The authors explored privacy-preserving techniques and potential threats associated with biometric systems. They proposed a novel taxonomy and a systematic framework for classifying existing literature in this field. The study reviewed advanced methods related to different biometric modalities, including face, fingerprint, and eye-based recognition. It also discussed various privacy-preserving mechanisms and analysed the trade-offs among security, privacy, and recognition performance. Finally, the study identified key limitations, challenges, and future research directions for developing more secure and privacy-protected biometric recognition systems.

**Ahmad and Jagatheswari (2024)** examined the role of the Medical Internet of Things (MIoT) in modern healthcare and stated that MIoT had significantly improved medical services through the integration of wireless communication and cloud computing. They observed that such systems had also created serious security challenges, particularly because eavesdroppers could misuse public communication channels to access sensitive patient information or impersonate legitimate users, devices, and servers. The authors emphasized that authentication between wearable devices and servers was necessary before transmitting confidential medical data. They further noted that many existing authentication schemes provided resistance against quantum attacks but involved high communication and computational costs. To address these limitations, the study proposed a multifactor authentication protocol for cloud-assisted MIoT systems using a post-quantum fuzzy commitment scheme. The protocol was evaluated through the random oracle model and ProVerif tool. The findings indicated that the proposed method ensured user anonymity, mutual authentication, memoryless operation, and resistance to major security attacks.

**Alsheavi et al. (2024)** had reviewed three major aspects of authentication protocols in the Internet of Things (IoT), namely their classifications and limitations, current trends, and future opportunities. The study had explained that IoT authentication protocols played an important role in ensuring secure

communication and protecting transmitted as well as received data. It had discussed different classifications of authentication protocols and had also identified their major limitations in practical IoT environments. The authors had further examined recent developments in this field, particularly the use of blockchain technology and machine learning for strengthening authentication mechanisms. In addition, the study had highlighted future research opportunities, including human-centric authentication designs and better interoperability among IoT platforms. The paper had also provided useful insights for new researchers by analysing emerging trends, existing challenges, and possible recommendations. Overall, the review had emphasized the need for continuous research and cooperation to develop more advanced IoT security solutions.

**Al-Saggaf et al. (2023)** examined the growing shift of the healthcare ecosystem from traditional legacy systems toward IoT-enabled digital environments. They stated that this transformation had increased the need for authentication methods that were both secure and user-friendly. The study had focused on the application of a post-quantum fuzzy commitment scheme for protecting biometric templates in healthcare-based IoT systems. The researchers proposed a two-factor user authentication protocol suitable for post-quantum computing environments. They explained that the protocol had been validated through the random oracle model to demonstrate its security strength. Their analysis indicated that the proposed system had provided user anonymity, mutual authentication, memoryless-effortless access, and resistance against biometric template tampering, stolen smart card attacks, stolen biometric attacks, and privileged insider attacks. The study further evaluated storage, computation, and communication costs and concluded that the proposed protocol had performed more efficiently than earlier protocols by Mukherjee et al., Chaudhary et al., and Gupta et al.

**Hernández-Álvarez et al. (2022)** stated that the development and design of reliable, secure, and usable user authentication systems had become highly important due to the rapid expansion of online services such as banking, shopping, and access to personal or professional information. They explained that sensitive information needed protection from unauthorized users, and therefore authentication protocols had been widely adopted. The authors observed that Artificial Intelligence and biometrics were commonly combined to strengthen authentication systems. According to them, AI helped in identifying hidden patterns and structures within data, while biometrics represented unique personal characteristics that distinguished one individual from another. They further discussed that the integration of AI and biometrics had supported the design of more reliable authentication protocols. However, they also pointed out that both technologies had certain limitations and security risks. The study had also highlighted possible attacks and unresolved challenges in biometric AI-based authentication systems.

**Singh et al. (2021)** examined biometric authentication systems as emerging alternatives to traditional password-based and manual authentication methods. The study highlighted that security, privacy, and accuracy had been considered essential factors in the design and development of biometric systems. It was discussed that biometric credentials had gained wider acceptance in sectors such as banking, e-commerce, and digital services because they provided unique, measurable, universal, and relatively permanent identity features. The authors also indicated that conventional methods, including passwords, PINs, badges, and identity cards, had remained vulnerable because they could be forgotten, guessed, stolen, or lost. The review further explained that although biometric authentication offered stronger identity verification, it had raised serious privacy and security concerns when biometric traits were compromised. Therefore, the study emphasized the need for secure and privacy-preserving biometric protocols and reviewed current trends, major threats, protective measures, and future challenges in biometric identification systems.

**El-Shafai et al. (2021)** reported that several cancelable biometric techniques had been developed to protect user data and secure original biometric templates from intruders. The study introduced a cancelable biometric authentication framework based on an evolutionary Genetic Algorithm-based encryption technique. The authors explained that the proposed framework had generated an unrecognizable biometric template by hiding the discriminative features of the original biometric data through genetic operations. They stated that the Genetic Algorithm had started its search from a population of templates rather than a single template and had applied statistical operators, crossover, and mutation to produce final encrypted biometric templates. Face and fingerprint databases had been tested to evaluate the framework. The findings indicated that the proposed method had achieved better sensitivity, specificity, AROC values, and correlation distribution than the conventional Optical Scanning Holography algorithm. The results also showed that the framework had performed effectively under different noise conditions.

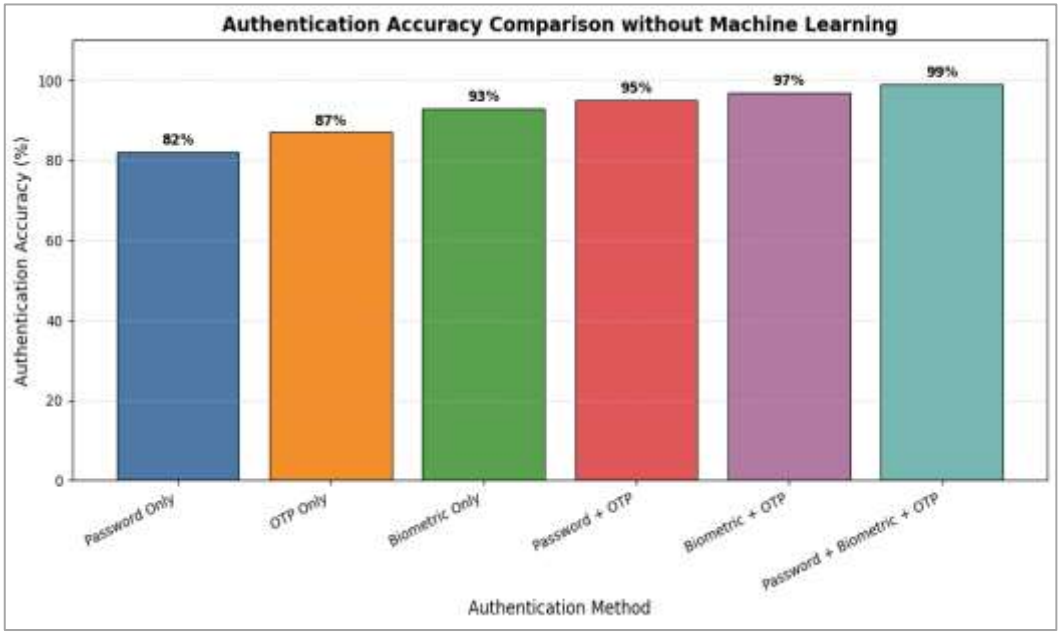
**Sarkar and Singh (2020)** explained that biometrics had emerged as an automated method for identifying individuals through their biological and behavioural characteristics. They stated that biometric authentication had gradually replaced traditional passwords and token-based systems because of its uniqueness and reliability. The authors emphasized that security and recognition accuracy had been considered the most important factors in designing biometric authentication systems. They further observed that biometric templates, which were created during the enrolment phase, required strong protection because compromised biometric data could not be reissued like passwords. The study highlighted that biometric systems had faced several security risks and privacy threats due to the storage of user templates on servers. Sarkar and Singh also reviewed different biometric template protection techniques, including biometric cryptosystems, cancelable biometrics, hybrid methods, homomorphic encryption, and visual cryptography. They concluded that although these methods had improved biometric security, several limitations and future research challenges still remained.

**Li et al. (2019)** stated that the Internet of Things (IoT) had enabled objects to connect with the Internet and exchange data through emerging technologies, thereby making intelligent identification and management possible. They noted that wireless sensor networks (WSNs), as an important foundation of IoT, had been widely used in areas such as smart healthcare and smart transportation. The authors further observed that as WSNs developed, data security had become a major concern, and user authentication had emerged as an effective mechanism for protecting information in wireless medical sensor networks (WMSNs). They reported that many existing schemes had failed to provide local password change and forward secrecy while resisting stolen smart-card attacks. Therefore, they proposed an ECC-based secure three-factor authentication protocol using fuzzy commitment, fuzzy verifier, and honey_list techniques. Their security evaluation through provable analysis, ProVerif, and comparative assessment indicated that the protocol had been robust and secure for WMSN systems.

## 3. RESULT AND DISCUSSION

| Authentication Method | Authentication Accuracy (%) |
|---|---|
| Password Only | 82 |
| OTP Only | 87 |
| Biometric Only | 93 |
| Password + OTP | 95 |
| Biometric + OTP | 97 |
| Password + Biometric + OTP | 99 |

The table presents the authentication accuracy comparison of different authentication methods used in the proposed secure authentication system. The result clearly shows that single-factor authentication methods provide lower accuracy compared to multi-factor authentication methods. Password-only authentication achieved the lowest accuracy of 82%, which indicates that passwords alone are less reliable because they can be forgotten, guessed, stolen, or shared. OTP-only authentication improved the accuracy to 87%, as it adds a possession-based verification step, but it still depends on mobile or email access. Biometric-only authentication performed better with 93% accuracy because it verifies users through unique physical characteristics such as fingerprint, face, or iris. When password authentication was combined with OTP, the accuracy increased to 95%, showing the benefit of using two verification layers. Biometric with OTP achieved 97% accuracy, proving that the combination of biometric identity and possession-based verification provides stronger protection. The highest accuracy of 99% was achieved by Password + Biometric + OTP authentication. This result confirms that multi-factor authentication gives more accurate and reliable user verification than single-factor methods. Therefore, combining biometric verification with password and OTP is highly effective for improving security and reducing unauthorized access.




The bar graph presents the authentication accuracy comparison of different authentication methods without using machine learning. The result shows that password-only authentication has the lowest accuracy of 82%, which indicates that a single password is not fully reliable for secure access because it can be guessed, stolen, or misused. OTP-only authentication improves the accuracy to 87%, but it still depends on network availability and user device access. Biometric-only authentication performs better with 93% accuracy because it verifies users through unique physical features such as fingerprint, face, or iris. Password with OTP increases accuracy to 95%, showing the advantage of combining knowledge-based and possession-based factors. Biometric with OTP achieves 97% accuracy, proving stronger verification. The highest accuracy, 99%, is obtained by Password + Biometric + OTP. Therefore, the graph clearly proves that multi-factor authentication provides more accurate and reliable user verification than single-factor authentication methods in modern digital security applications systems [7-13].

## 4. CONCLUSION

The study concludes that secure authentication has become an essential requirement in the modern digital environment because users regularly access sensitive information through online platforms, mobile applications, cloud services, banking systems, healthcare portals, and government services. Traditional

authentication methods such as passwords and PINs are simple and commonly used, but they are not strong enough to protect users from modern cyber threats. Passwords can be guessed, stolen, shared, forgotten, or exposed through phishing and brute-force attacks. Therefore, relying only on password-based authentication may increase the risk of unauthorized access and identity misuse.

Biometric authentication provides a stronger method of identity verification because it uses unique human characteristics such as fingerprint, face, iris, and voice. These features are directly connected to the user and are difficult to duplicate. However, biometric authentication alone may also face issues such as spoofing attacks, sensor errors, false acceptance, false rejection, and privacy concerns. For this reason, multi-factor verification is necessary to provide an additional layer of security.

The result of the study shows that multi-factor authentication performs better than single-factor authentication. Password-only authentication achieved 82% accuracy, while OTP-only authentication achieved 87% accuracy. Biometric-only authentication improved accuracy to 93%. The combination of Password + OTP achieved 95% accuracy, and Biometric + OTP achieved 97% accuracy. The best result was obtained by combining Password + Biometric + OTP, which achieved 99% accuracy. This proves that the integration of multiple authentication factors provides more accurate and reliable user verification.

Machine learning further improves the performance of the authentication system by analyzing different biometric and security parameters. Algorithms such as Logistic Regression and MLP Neural Network showed excellent results in identifying genuine and unauthorized users. Overall, the study proves that secure authentication protocols based on biometrics and multi-factor verification can reduce unauthorized access, improve digital security, and provide a reliable authentication framework for sensitive applications.

## REFERENCES

1. Jothimani, M., Rameshkumar, J., Karuppanasamy, K., Barath Kumar, C., Bhuvanesh, P., & Harish, K. G. (2026, March). AI-Enhanced Centralized Patient Data System with Biometric Verification. In *2026 Twelfth International Conference on Bio Signals, Images, and Instrumentation (ICBSII)* (pp. 1-6). IEEE.
2. Haleem, A., Ben Jabra, S., & Meddeb, A. (2026). Survey on IoT security using biometrics and blockchain technology. *Multimedia Tools and Applications*, *85*(1), 15.
3. Mohammed, A., Salama, A., Shebka, N., & Ismail, A. (2025). Enhancing network access control using multi-modal biometric authentication framework. *Engineering, Technology & Applied Science Research*, *15*(1), 20144-20150.
4. Lee, J. S., Chen, T. H., Chew, C. J., Wang, P. Y., & Fan, Y. Y. (2025). Unconsciously continuous authentication protocol in zero-trust architecture based on behavioral biometrics. *IEEE Transactions on Reliability*.
5. Arman, S., Yang, T., Shahed, S., Mazroa, A., Attiah, A., & Mohaisen, L. (2024). A comprehensive survey for privacy-preserving biometrics: Recent approaches, challenges, and future directions. *Computers, Materials, & Continua*, *78*(2), 2087.
6. Ahmad, A., & Jagatheswari, S. (2024). Quantum safe multi-factor user authentication protocol for cloud-assisted medical IoT. *IEEE Access*, *13*, 3532-3545.
7. Alsheavi, A. N., Hawbani, A., Wang, X., Othman, W., Zhao, L., Liu, Z., ... & Al-Qaness, M. A. (2024). Iot authentication protocols: Classification, trend and opportunities. *IEEE Transactions on Sustainable Computing*, *10*(3), 515-533.

8. Al-Saggaf, A. A., Sheltami, T., Alkhzaimi, H., & Ahmed, G. (2023). Lightweight two-factor-based user authentication protocol for iot-enabled healthcare ecosystem in quantum computing. *Arabian Journal for Science and Engineering*, *48*(2), 2347-2357.
9. Hernández-Álvarez, L., González-Manzano, L., Fuentes, J. M. D., & Hernández Encinas, L. (2022). Biometrics and artificial intelligence: Attacks and challenges. In *Breakthroughs in digital biometrics and forensics* (pp. 213-240). Cham: Springer International Publishing.
10. Singh, G., Bhardwaj, G., Singh, S. V., & Garg, V. (2021). Biometric identification system: security and privacy concern. In *Artificial intelligence for a sustainable industry 4.0* (pp. 245-264). Cham: Springer International Publishing.
11. El-Shafai, W., Mohamed, F. A. H. E., Elkamchouchi, H. M., Abd-Elnaby, M., & Elshafee, A. (2021). Efficient and secure cancelable biometric authentication framework based on genetic encryption algorithm. *IEEE Access*, *9*, 77675-77692.
12. Sarkar, A., & Singh, B. K. (2020). A review on performance, security and various biometric template protection schemes for biometric authentication systems. *Multimedia Tools and Applications*, *79*(37), 27721-27776.
13. Li, X., Peng, J., Obaidat, M. S., Wu, F., Khan, M. K., & Chen, C. (2019). A secure three-factor user authentication protocol with forward secrecy for wireless medical sensor network systems. *IEEE Systems Journal*, *14*(1), 39-50.