International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

Biometric-Based Payment for Microtransaction Using Elliptic Curve Cryptography

B S Ullas
Dept. of Information Science and Engineering
BNM Institute of Technology, Affilated to VTU
Bengaluru, India

Dr. Jagruthi H
Associate Professor. Dept. of
Information Science and Engineering
BNM Institute of Technology, Affilated to VTU
Bengaluru, India

Kartikey Joshi
Dept. of Information Science and Engineering
BNM Institute of Technology, Affilated to VTU
Bengaluru, India

Shashwath D U
Dept. of Information Science and Engineering
BNM Institute of Technology, Affilated to VTU
Bengaluru, India

Abstract **- A biometric-based payment framework is designed using elliptic curve cryptography (ECC) to enable secure and efficient microtransactions. Fingerprint authentication is employed for user verification, ensuring reliability and eliminating the need for traditional credentials. Encrypted biometric templates and lightweight ECC operations safeguard sensitive data, while the system architecture supports fast processing suitable for low-value transactions. The approach provides strong security with reduced computational cost, making it practical for real-time usage. The prototype demonstrates scalability, affordability, and potential integration with existing digital payment infrastructures.**

Keywords - Biometric Authentication, Microtransaction, Elliptic Curve Cryptography, Secure Payment, Fingerprint Recognition

I. INTRODUCTION

For individuals in the digital economy, secure and convenient payment mechanisms are essential, particularly in the context of low-value transactions where traditional methods may be slow, costly, or vulnerable to fraud. Existing payment systems generally depend on credentials such as passwords, PINs, or card details, which are frequently subject to theft, misuse, or social engineering attacks. To overcome these limitations, this project introduces a biometric-driven payment solution that authenticates users through fingerprint recognition, thereby eliminating the need for manual credentials and reducing the risk of unauthorized access. The system is built upon elliptic curve cryptography (ECC), a lightweight yet robust cryptographic technique that provides strong encryption while consuming fewer computational resources compared to traditional algorithms like RSA. This makes the approach particularly efficient and suitable for real-time microtransactions, where speed and security are equally critical.

Traditional authentication techniques such as passwords or physical tokens provide only limited protection and often burden users with the responsibility of remembering or carrying external credentials. In contrast, biometric authentication leverages unique physiological traits, offering a natural, non-transferable, and tamper-resistant method of identity verification. In this project, fingerprint recognition is employed for user validation, ensuring accurate and reliable authentication with minimal user effort. Unlike conventional payment gateways that can introduce latency due to complex computations or reliance on external servers, the proposed system utilizes ECC-based encryption, which achieves comparable security strength to RSA but with significantly smaller key sizes and faster computations. This efficiency makes the design well-suited for resource-constrained devices such as point-of-sale terminals, mobile phones, and IoT-enabled payment kiosks.

At the heart of the system lies a secure backend architecture integrated with fingerprint modules for template storage, matching, and verification. To protect sensitive biometric data, fingerprint templates are encrypted using ECC prior to storage or transmission, thereby minimizing the risk of exposure during breaches or network attacks. The system also incorporates digital wallet functionalities, enabling users to perform seamless and instant microtransactions while ensuring both confidentiality and integrity of the transaction records. All transaction data is securely logged, ensuring traceability and accountability without compromising user privacy.

The system's performance has been evaluated across several dimensions, including authentication accuracy, encryption and decryption speed, transaction latency, and resource consumption. Experimental results consistently demonstrate low-latency processing, minimal computational overhead, and reliable fingerprint recognition, thereby validating the feasibility of ECC as an ideal cryptographic foundation for microtransaction scenarios. Moreover, by embedding encryption at every stage of the workflow, the design ensures that both user credentials and transaction details remain secure against common cyber threats such as replay attacks,

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

man-in-the-middle attacks, and brute-force attempts.

Beyond its technical reliability, the system is designed with scalability and cost-effectiveness in mind. All hardware components, including fingerprint sensors and ECC-enabled microcontrollers, are affordable, readily available, and compatible with existing digital infrastructures. This

adaptability makes the solution applicable to a wide range of environments, including retail outlets, self-service kiosks, e-commerce platforms, and peer-to-peer payment systems. Furthermore, the modular nature of the design allows for future integration with technologies such as blockchain-based ledgers for immutable transaction logging or privacy-preserving biometric techniques such as homomorphic encryption.

In summary, by merging biometric authentication with lightweight cryptographic operations, the project proposes a practical, secure, and user-friendly framework that addresses the inherent challenges of microtransactions. The approach not only enhances user trust, efficiency, and accessibility but also lays a foundation for next-generation payment systems capable of operating securely in diverse digital and mobile ecosystems.

II. LITERATURE SURVEY

The field of secure digital payment has undergone significant evolution with the integration of biometric authentication and lightweight cryptographic mechanisms. A central focus has been enhancing user trust, preventing fraud, and ensuring data privacy in microtransactions.

Devarajan and Sasikaladevi (2020) introduced a biometric-based three-factor mutual authentication scheme, where elliptic curve cryptography (ECC) was applied to strengthen authentication in electronic payment systems, demonstrating improved resistance against replay and impersonation attacks [1]. Similarly, Vincent et al. (2020) proposed an identity-based ECC protocol tailored for mobile payment security, offering lower computational overhead while maintaining strong encryption, making it suitable for resource-constrained devices [2].

Chen and Chen (2023) developed a biometrics-driven mutual authentication and key agreement protocol using ECC within telemedicine systems. Their work highlighted the potential of combining biometric templates with elliptic curve operations to achieve secure and efficient remote authentication [3]. Extending this, Zhai et al. (2024) designed an ECC-based identity authentication scheme optimized for metaverse environments, emphasizing scalability and interoperability across decentralized platforms [4].

Earlier studies also investigated ECC in the context of electronic commerce. Vincent, Folorunso, and Akinde (2010) applied ECC to improve e-payment security, demonstrating its superiority over RSA in terms of speed and reduced key sizes, which are crucial for mobile devices [5]. Al-Zubaidie et al. (2019) conducted a comprehensive survey of ECDSA algorithms, detailing optimizations and real-world applications in financial systems [6]. Complementing this, Solat (2017) reviewed the overall security landscape of electronic payment systems, identifying ECC as a key enabler for lightweight yet robust cryptographic protocols [7].

Ahmed et al. (2021) examined security challenges in next-generation mobile payment platforms, presenting a survey that emphasized biometric authentication combined with ECC as an effective defense against evolving threats such as phishing and man-in-the-middle attacks [8]. Rashidi (2017) provided insights into hardware implementations of ECC, highlighting the role of specialized architectures in accelerating encryption and decryption processes for real-time transactions [9].

Beyond academic research, industry contributions such as the Smart Payment Association's white paper (2013) stressed the importance of biometrics in modern payment applications, outlining deployment strategies for fingerprint and facial recognition in secure financial transactions [10]. Kuraku et al. (2020) explored the integration of AI and big data with biometric authentication for digital payments, enabling real-time fraud detection and enhanced system adaptability [11]. Talib and Salman (2022) further reinforced the value of biometrics by proposing an efficient e-payment model that combined fingerprint recognition with traditional password systems [12].

Agboola and Folorunso (2020) advanced this line of work by presenting a hybrid scheme for e-payment security using ECC, which blended symmetric and asymmetric encryption for enhanced speed without compromising security [13]. Foundational cryptographic research by Miller (1986) first demonstrated the applicability of elliptic curves in cryptography, laying the groundwork for ECC's adoption in payment systems [14]. Building on this foundation, NIST's recommendation (2018) standardized key establishment protocols using ECC, providing a widely accepted framework for secure pair-wise communication in financial systems [15].

Elliptic curve cryptography has gained prominence due to its strong security and efficiency compared to traditional algorithms such as RSA. Vincent et al. [2], [5] demonstrated the effectiveness of ECC in reducing computational overhead while providing robust protection for e-payment systems. Similarly, Agboola and Folorunso [13] proposed a hybrid scheme that integrates ECC to strengthen security for online transactions.

In addition, Al-Zubaidie et al. [6] surveyed efficient implementations of ECDSA, showing its suitability for constrained environments. Rashidi [9] further analyzed hardware implementations of ECC, suggesting that ECC can be optimized for portable devices, a critical requirement for microtransaction systems.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

Biometric authentication has been increasingly used as a replacement for passwords and PINs in mobile and digital payments. Nayak et al. [10] and Talib & Salman [12] explored fingerprint and facial authentication mechanisms, highlighting their role in reducing fraud and improving user convenience.

Kuraku et al. [11] emphasized the integration of biometrics with AI and big data to enhance real-time fraud detection, while the Smart Payment Association [10] discussed the adoption of biometrics in payment cards and mobile wallets. However, these studies also note challenges such as privacy risks, spoofing attacks, and the need for error-tolerant systems.

The combination of biometric authentication with ECC has been proposed to achieve both strong user verification and lightweight cryptographic security. Devarajan and Sasikaladevi [1] introduced a three-factor mutual authentication scheme that leverages ECC for securing biometric transactions. Similarly, Chen and Chen [3] proposed a biometrics-based mutual authentication and key agreement protocol for telemedicine systems, demonstrating ECC's capability to protect sensitive biometric exchanges.

More recent research by Zhai et al. [4] applied ECC-based identity authentication in emerging environments like the metaverse, which has implications for next-generation financial ecosystems.

Several broader surveys provide a holistic perspective on the challenges and advancements in secure payment systems. Solat [7] presented a comprehensive survey of electronic payment security, identifying fraud prevention and user trust as central issues. Ahmed et al. [8] analyzed next-generation mobile payment security, including biometrics and lightweight cryptography. Finally, NIST guidelines [15] remain the standard reference for ECC-based key establishment, ensuring that new frameworks align with international standards.

Collectively, these works highlight that biometric authentication, when combined with ECC, offers a highly efficient, scalable, and secure solution for modern digital payment ecosystems. This combination is particularly well-suited for microtransactions, where lightweight computation and strong protection against fraud are essential.

III. COMPARATIVE ANALYSIS

The use of Elliptic Curve Cryptography (ECC) in securing electronic and biometric-based payment systems has received considerable attention over the last two decades. Table 1 (to be added later in your final paper) can summarize the contributions, strengths, and limitations of the reviewed works. Here, we provide a comparative discussion highlighting the evolution of techniques, their effectiveness, and the research gaps that remain.

Early contributions such as Miller's seminal work on elliptic curves [14] laid the mathematical foundation for ECC-based cryptographic applications. Building on this, Vincent et al. [5] and Solat [7] identified ECC as a lightweight yet secure cryptographic alternative to RSA in the context of e-payment systems. Their findings established the relevance of ECC for constrained devices, but they primarily focused on theoretical security benefits without extensive validation in large-scale real-world payment infrastructures.

Subsequent studies introduced biometric integration into ECC-driven payment schemes. Devarajan and Sasikaladevi [1] proposed a three-factor authentication system, combining biometrics, passwords, and smart cards with ECC. Their scheme addressed insider threats and replay attacks effectively but was computationally heavier than traditional ECC models. Similarly, Chen and Chen [3] advanced this idea by developing a biometrics-based mutual authentication and key agreement protocol for telemedicine information systems. Their approach demonstrated resilience against impersonation and man-in-the-middle attacks, although usability concerns such as biometric failure rates were not deeply analyzed.

With the rise of mobile and digital payments, Vincent et al. [2] and Agboola and Folorunso [13] developed identity-based and hybrid ECC schemes to enhance flexibility and minimize overhead. These approaches improved on traditional public-key infrastructures by reducing certificate management challenges. However, scalability in high-volume payment systems was not fully explored.

Recent research has shifted towards emerging environments and advanced payment ecosystems. Zhai et al. [4] extended ECC-based authentication into metaverse platforms, underlining its adaptability beyond conventional payments. Likewise, Kuraku et al. [11] examined the synergy of biometrics, AI, and big data in digital transactions, highlighting real-time fraud detection as a critical advancement. Talib and Salman [12] reinforced this direction by demonstrating efficient biometric-driven payment models tailored for practical deployment.

Complementing these domain-specific contributions, general surveys and standards have enriched the field. Al-Zubaidie et al. [6] provided an in-depth survey of ECDSA, emphasizing algorithmic improvements relevant for signature-based payment protocols. Rashidi [9] analyzed hardware implementations of ECC, a perspective crucial for payment terminals and IoT-enabled devices. Furthermore, global guidelines such as NIST recommendations [15] and the SPA white paper [10] provided standardization and best practices, ensuring interoperability and regulatory alignment.

Overall, the comparative review suggests that while ECC has become a cornerstone of secure payment systems, its integration with biometrics and AI is still maturing. The literature demonstrates strong resistance against common cryptographic attacks, but challenges remain in balancing

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

security, efficiency, and usability. In particular, practical deployment in large-scale ecosystems (e.g., mobile-first markets, IoT-based microtransactions) requires further optimization. Future research should address biometric error tolerance, privacy-preserving storage, and hardware acceleration of ECC to ensure widespread adoption.

IV. PROPOSED SURVEY INSIGHTS

The survey of existing literature reveals a strong movement toward integrating biometric authentication with elliptic curve cryptography (ECC) for secure payment systems. While many studies address biometric-based payments [10]–
[12] and others focus on ECC-enabled cryptographic protocols [2], [5], [6], the combination of both approaches tailored to microtransaction environments remains relatively underexplored.

From the reviewed works, the following insights are drawn:

1. Lightweight Security is Crucial

ECC consistently outperforms RSA in terms of computational cost and key size, making it ideal for mobile devices and IoT-driven payment systems. Hardware-oriented surveys [9] show ECC's adaptability to constrained environments, which aligns with the requirements of microtransactions.

2. Biometric Authentication Enhances User Trust

Biometric mechanisms such as fingerprint, iris, and face recognition increase usability and fraud resistance. However, privacy concerns and spoofing risks persist, which necessitate secure biometric template storage and encryption [10], [12].

3. ECC–Biometric Integration is Promising but Limited in Adoption

Few studies [1], [3], [13] have combined ECC with biometrics in authentication frameworks, mostly targeting healthcare or general e-payments rather than microtransactions. This indicates a gap in scalable, low-latency, and cost-effective biometric payment solutions specifically for small-value transactions.

4. Future Payment Ecosystems Require Hybrid Approaches

The combination of ECC for cryptographic efficiency, biometrics for strong authentication, and AI-driven anomaly detection [11] represents a holistic model for next-generation secure payments. International standards such as NIST's recommendations [15] remain crucial to ensure interoperability and compliance in real-world deployment.

V. FUTURE DIRECTIONS

Although the reviewed literature demonstrates significant progress in securing payment systems through biometrics and elliptic curve cryptography (ECC), several avenues remain open for future research. One promising direction is the integration of blockchain technology with biometric authentication and ECC. Blockchain's decentralized ledger can strengthen transaction integrity and provide non-repudiation in microtransaction environments, making payments more transparent and tamper-resistant.

Another critical area is privacy-preserving biometrics. Emerging techniques such as homomorphic encryption and secure multiparty computation allow biometric templates to be verified without exposing raw data, thereby reducing risks of identity theft and enhancing user trust.

With the proliferation of smart devices, the deployment of biometric-ECC payment models in IoT ecosystems and mobile wallets is another natural extension. Lightweight implementations are especially important for devices with constrained processing power, ensuring that security does not compromise efficiency.

Finally, future studies could explore hybrid authentication mechanisms that combine multiple biometric traits with ECC-based cryptography. Such approaches can improve resilience against spoofing attacks while maintaining the lightweight characteristics required for microtransactions.

In addition, future research should investigate regulatory compliance and standardization of biometric-ECC payment systems. Establishing global benchmarks for interoperability and legal frameworks will be essential for widespread adoption across banking, retail, and mobile commerce sectors.

VI. CONCLUSION

This survey has examined the intersection of biometric authentication and elliptic curve cryptography (ECC) in the context of secure digital payments, with a particular emphasis on the challenges and opportunities surrounding microtransactions. The analysis underscores that ECC provides not only computational efficiency but also strong cryptographic guarantees, making it particularly well-suited for resource-constrained platforms such as mobile devices, IoT-enabled payment kiosks, and point-of-sale terminals. On the other hand, biometric authentication introduces a more intuitive, reliable, and user-centric mechanism for verifying identities, addressing the long-standing vulnerabilities of password or PIN-based systems that are susceptible to theft, duplication, and user fatigue.

The comparative review of existing approaches highlights both strengths and limitations. On the positive side, ECC-based biometric systems demonstrate improved authentication accuracy, faster transaction processing, and reduced computational overhead compared to traditional cryptographic solutions. These advantages directly align with the performance requirements of low-value, high-frequency digital payments. However, notable limitations persist, including privacy concerns regarding biometric template storage, potential interoperability challenges across heterogeneous platforms, and the limited adoption of such

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

frameworks in real-world microtransaction ecosystems. These challenges emphasize the importance of integrating advanced privacy-preserving methods, such as homomorphic encryption or secure multiparty computation, and ensuring compatibility with existing financial infrastructures.

Overall, the findings of this survey suggest that biometric-based payment systems leveraging ECC hold substantial potential to transform the way digital microtransactions are conducted. By ensuring both security and usability, these systems provide a promising pathway toward secure, low-cost, and efficient payment solutions. Looking ahead, continued innovation in blockchain integration for immutable transaction records, privacy-preserving biometric techniques, and large-scale IoT deployment can further strengthen the reliability and scalability of such systems. Ultimately, the convergence of biometrics and ECC lays the groundwork for a robust, future-ready framework that could redefine digital commerce, particularly in scenarios where speed, trust, and security are paramount.

REFERENCES

[1] M. Devarajan and S. Sasikaladevi, "Biometric-Based Three-Factor Mutual Authentication Scheme for Electronic Payment System Using Elliptic Curve Cryptography," *Malaysian Journal of Computer Science*, Special Issue 1, pp. 39–60, 2020.

[2] O. R. Vincent, T. M. Okediran, A. A. Abayomi-Alli, and O. J. Adeniran, "An Identity-Based Elliptic Curve Cryptography for Mobile Payment Security," *SN Computer Science*, vol. 1, no. 2, pp. 1–10, 2020.

[3] Y. Chen and J. Chen, "A Biometrics-Based Mutual Authentication and Key Agreement Protocol for TMIS Using Elliptic Curve Cryptography," *Multimedia Tools and Applications*, vol. 82, pp. 16009–16032, 2023.

[4] H. Zhai, M. Deng, and H. Wu, "Elliptic Curve Cryptography-Based Identity Authentication Scheme Suitable for Metaverse Environment," *Symmetry*, vol. 16, no. 7, article 891, 2024.

[5] O. R. Vincent, O. Folorunso, and A. Akinde, "Improving E-Payment Security Using Elliptic Curve Cryptosystem," *Electronic Commerce Research*, vol. 10, no. 1, pp. 27–41, 2010.

[6] M. Al-Zubaidie, Z. Zhang, and J. Zhang, "Efficient and Secure ECDSA Algorithm and Its Applications: A Survey," *arXiv preprint arXiv:1902.10313*, 2019.

[7] S. Solat, "Security of Electronic Payment Systems: A Comprehensive Survey," *arXiv preprint arXiv:1701.04556*, 2017.

[8] W. Ahmed, A. Rasool, N. Kumar, et al., "Security in Next-Generation Mobile Payment Systems: A Comprehensive Survey," *arXiv preprint arXiv:2105.12097*, 2021.

[9] B. Rashidi, "A Survey on Hardware Implementations of Elliptic Curve Cryptosystems," *arXiv preprint arXiv:1710.08336*, 2017.

[10] Smart Payment Association (SPA), "Biometrics for Payment Applications," White Paper, Nov. 2013.

[11] C. Kuraku, H. K. Gollangi, and J. R. Sunkara, "Biometric Authentication in Digital Payments: Utilizing AI and Big Data for Real-Time Security and Efficiency," *Educational Administration: Theory and Practice*, vol. 26, no. 4, pp. 954–964, 2020.

[12] A. A. Talib and A. D. Salman, "An Efficient Electronic Payment Using Biometric Authentication," *Iraqi Journal of Computers, Communications, Control & Systems Engineering (IJCCCE)*, vol. 22, no. 3, pp. 50–59, 2022.

[13] A. A. Agboola and O. Folorunso, "An Improved Hybrid Scheme for E-Payment Security Using Elliptic Curve Cryptography," *International Journal of Information Technology*, vol. 12, no. 4, pp. 999–1007, 2020.

[14] V. S. Miller, "Use of Elliptic Curves in Cryptography," *Advances in Cryptology — CRYPTO'85 Proceedings*, Lecture Notes in Computer Science, vol. 218, pp. 417–426, 1986.

[15] NIST, "Recommendation for Pair-Wise Key Establishment Using Elliptic Curve Cryptography (SP 800-56A Rev. 3)," National Institute of Standards and Technology, 2018.