International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 13 Issue 8 ǁ August 2025 ǁ PP.121-124

Application of biometric technology in electronic payment security

Abstract
With the widespread adoption of electronic payments, the security risks they face are becoming increasingly severe. This article explores the application value of artificial intelligence, particularly biometric technology, in enhancing payment security. By introducing real-time risk assessment, multi-factor authentication, and behavior analysis, AI effectively addresses the shortcomings of traditional methods. Additionally, the article analyzes the application prospects of multimodal recognition and wearable devices, and points out that data privacy and ethical issues need to be given equal attention. The research provides a reference for building smarter and safer payment systems.
Keywords: *Electronic Payments, AI (Artificial Intelligence), Biometrics*

Date of Submission: 07-08-2025 Date of acceptance: 18-08-2025

I. Security risks faced by electronic payments under technological development

1.1 Proliferation of electronic payments coexists with risks

Electronic payment is the core component that enables the smooth operation of e-commerce. Its essential differences from traditional business trade allow it to occupy an increasingly significant proportion in modern economic development. The digitization of payment methods is an inevitable trend in the development of payment settlement, and a cashless lifestyle is becoming more common[1]. However, the characteristics of virtual online transactions and intangible currency payments bring certain issues of integrity and cash security[2].

In electronic payments, issues such as data forgery and rampant hacking, including destruction, alteration, and erasure, are becoming increasingly severe, with a growing impact on society. At the same time, emerging payment models like small-value, password-free services also pose a risk of fund theft. While technological means create convenience for people, they also bring serious financial risks, including online fraud risk and settlement account management risk. The scope of online fraud is extremely broad, the investigation difficulty is high, the concealment is very strong, the victim group is extensive, causing losses to the economic interests of the people, and it also poses a significant threat to the stability of social and economic development and financial development. At the same time, account management risks also need urgent attention. Criminals often transfer illegal funds through some illegal channels to carry out illegal fundraising activities or evade fund supervision. For example, using someone else's ID, opening empty accounts, false representation, etc[1]. Additionally, if our commercial banks have loose account creation or management policies, it will provide these criminals more possibilities to commit crimes, which will increase the bank's settlement risks.

1.2 Rise of new types of scams

The likelihood of fraud in the financial industry has significantly increased, with criminals using complex advanced AI tools such as DeepFake and machine learning to help them improve their scam success rates. Utilizing advanced deep learning models, DeepFake achieves real-time face swapping, generating images and videos that are almost indistinguishable from real content[3][4][5][6][7]. This incredible sense of realism, while enhancing the credibility of synthetic media, has also been exploited by malicious individuals to venture into dangerous or even illegal territories for greater profit[8][9]. Technologies that drive creative innovation are being used for fraud, including online scams and identity theft, raising serious security concerns [10][11]. In the United States, the FBI's Internet Crime Complaint Center received over 880,000 complaints in 2023 alone, a 22% increase from the previous year, with potential losses exceeding $12.5 billion. Meanwhile, experts predict that identity fraud caused by generative AI will increase annual losses by $2 billion.

Fraud news is constantly emerging. Criminals used deepfake technology and AI voice cloning technology to create very realistic digital replicas of executives in video conferences, deceiving employees of a Hong Kong company into transferring large sums of money into their accounts, earning $25 million. Criminals instructed employees to transfer funds using deepfake avatars of the company's CFO and other officials. Although employees were initially hesitant, the realism and detail of the deepfake, combined with the psychological pressure of direct orders from superiors, led them to refrain from questioning or opposing their superiors. As a result, they authorized

the transactions as instructed, and the scam was ultimately completed.

1.3 Limitations of traditional security measures

In the early days of the rise of electronic payments, authentication was achieved through passwords and SMS verification codes. However, these traditional methods can no longer cope with the ever-evolving attack methods of today's society. Hackers can easily obtain user information and complete fraud by using Trojan programs, phishing websites, and psychological pressure to understand user thoughts. Moreover, some users are accustomed to using simple and repetitive password combinations, increasing the likelihood of criminals obtaining their information and committing financial fraud. Additionally, in cases of repeated passwords, users are very likely to be defrauded of all their funds. In today's society, with the rapid evolution of technology, static verification methods have become increasingly inadequate in addressing the ever-changing security challenges.

At the same time, when it comes to real-time monitoring, identification, and response to fraudulent activities, the existing security systems also have many shortcomings. Most traditional payment systems mainly rely on post-fraud detection and manual review to identify fraudulent activities, lacking the capability for real-time monitoring and analysis of the transaction process. This often means that criminal activities are only discovered after losses have occurred, and sometimes victims need to take the initiative to report to the police for help. This not only delays emergency response time but also increases the difficulty of recovering losses. The lack of a dynamic risk assessment mechanism during payment also prevents the system from adjusting verification intensity based on user behavior patterns, thereby increasing the likelihood of verification actions or defense mechanisms being bypassed by AI. To truly enhance payment security levels, relying solely on traditional methods is clearly no longer sufficient to meet the demands.

II. Application of artificial intelligence and biometric technology in payment security

2.1 AI-driven real-time risk assessment

AI models can analyze transaction data in real-time, identify abnormal behaviors, and improve the accuracy of fraud detection. For example, JPMorgan uses machine learning algorithms to analyze transaction patterns and flag potential fraudulent activities. The system builds detailed purchase profiles for each customer. Banks can detect any behavior that deviates from normal consumption, which may indicate illegal activities. The system updates evaluation models based on historical data and ultimately selects the appropriate model to assess the risk of each transaction. At the same time, the AI-driven system adjusts the intensity of dynamic defense mechanisms in real-time to adapt to new and different threats.

To identify suspicious activities, Citigroup has also taken corresponding measures. The group uses AI to sift through large datasets. The group's AI system can assess the risk level of transactions in real-time, using a series of tagged data to detect potential fraud. This approach not only improves the efficiency and accuracy of fraud detection but also significantly reduces the probability of false positives.

In Europe, HSBC uses AI-driven tools to prevent and detect payment fraud. The AI system analyzes millions of transactions, identifies patterns, and flags anomalies that may indicate fraudulent activity. With the help of this tool, HSBC can stop unauthorized transactions before they occur, thereby protecting customers' assets and reputation.

These examples illustrate a broader trend in the banking industry: the shift towards predicting fraud. By harnessing the power of AI, banks can stay one step ahead of fraudsters and anticipate fraudulent activities in advance. By building complex models that AI can learn from, banks can not only respond to fraud but also predict it ahead of time, thereby creating a more resilient and robust financial ecosystem in the face of growing cyber threats.

2.2 Integrated application of biometric technology

Biometric authentication has received considerable attention. Authentication can use behavioral biometrics, such as gestures, keystroke dynamics, and signatures, or unique features like fingerprints and facial characteristics. By using feature extraction methods, training and testing models can be developed with the help of AI and machine learning. Current research findings indicate that behavioral biometric authentication is regarded as an effective technology in the field of digital payments by users and security stakeholders. Biometric technology creates favorable conditions for people to conduct business activities, making them easier to carry [12].

Mastercard once used behavioral biometrics to try to detect impostors, examining how specific users type and swipe on the app. The app monitors this information as part of each transaction, with algorithms considering unique data points on the backend, such as the rhythm of password entry, how users hold their devices, and how they move their mouse. Experts say there are subtle but clear differences between the behavior of trusted users and that of impostors.

2.3 Combination of multi-factor authentication and AI

As payment risks become increasingly complex and fraud techniques more sophisticated, single-factor authentication methods can no longer provide sufficient security assurance. Multi-Factor Authentication (MFA) establishes a stronger and more complex layer of protection in the payment process by combining various verification methods, such as biometrics, device fingerprints, and behavioral feature analysis. When users conduct transactions, the system not only recognizes physiological features such as facial recognition and fingerprints, but also references device information (such as the unique code of commonly used phones, IP addresses, etc.) and behavioral habits (such as typing rhythm, sliding patterns, etc.) to determine whether the operation is performed by the user themselves, by others, or even by AI. The advantage of multi-dimensional verification is that even if one link is compromised, the overall system still possesses defensive capabilities, thereby effectively reducing the risk. For example, in a system that requires both password and fingerprint verification, if someone with malicious intent knows the password but still cannot pass the fingerprint recognition, then the fraud cannot succeed.

With the application of artificial intelligence technology in authentication, multi-factor authentication has become more intelligent and dynamic. For example, with Mastercard, the "Decision Intelligence" system scores each payment based on contextual information at the time of the transaction. This scoring is based on hundreds of millions of data points, including the cardholder's past spending behavior, geographical location, and more. The system can determine the reliability of a transaction within tens of milliseconds and automatically reject suspicious transactions when necessary. These AI tools continuously evolve through autonomous learning. They not only speed up the judgment process but also identify abnormal patterns that are difficult for humans to detect. For example, it can determine whether a user's occasional high spending is normal behavior or potential fraudulent activity. Compared to static rule-based judgments, AI can dynamically adjust authentication methods based on risk levels. This ensures transaction security while optimizing user experience.

III. Future Outlook: The Trend of AI and Payment Security Integration

3.1 The application prospects of emerging technologies

Digital payments are constantly evolving, and electronic payment methods are becoming increasingly diverse. Emerging technologies are driving the transformation of identity verification methods from traditional to intelligent and personalized approaches. Multimodal biometric recognition technology has emerged as the most effective solution to enhance verification accuracy and resistance to attacks. Compared to single fingerprint or facial recognition, multimodal recognition combines various biometric features (such as fingerprints, irises, facial expressions, voice, etc.), significantly improving the system's accuracy in detecting fraudulent activities. Since these characteristics are unique to each individual and personalized features are difficult to forge, biometric recognition has a higher capability to prevent theft and tampering compared to PIN codes or passwords, significantly reducing the risk of identity theft.

In addition, with the popularity of smartwatches and smart bands, authentication methods based on wearable devices are gradually emerging. Devices like smartwatches and bands are embedded with fingerprint recognition and heart rate monitoring, and more advanced ones even include skin conductance sensors. These embedded functions can be used for continuous user identity verification. Smartwatches and bands not only enable "contactless payment," but also offer very convenient user experiences, significantly improving user satisfaction. Users do not need to remember passwords or carry physical cards; they can complete authorization with just a touch, a voice command, or a facial scan. This "light interaction" model not only improves customer satisfaction but also reduces transaction interruptions caused by cumbersome verification processes, and to some extent, it can handle situations where the network is unstable during transactions. As technology matures, these methods are expected to become one of the mainstream payment methods in the future.

3.2 Data privacy and ethical challenges

Although AI can assist in fraud detection, providing convenience and ensuring the safety of people's funds, it also has its limitations. During the autonomous learning process of machine learning models, if they happen to learn biased historical data, AI might incorrectly associate legitimate transactions with fraud. In such cases, AI-driven systems could make errors in marking certain statistics or locations, leading to legitimate transactions being misidentified as fraud. This raises serious concerns about fairness and trust.

Because the progress of AI is relentless, the possibility of fraud also increases with the advancement of AI's autonomous learning. AI algorithms can become increasingly accurate in simulating biometric features through training, allowing them to impersonate or gain unauthorized access to systems. For example, AI-based voice synthesis technology can replicate someone's voice to such an extent that it can successfully deceive voice recognition systems. Similarly, facial recognition systems can be tricked by AI-generated deepfake images or masks.

In the face of these risks, adopting a method that combines multi-factor authentication and biometrics may help prevent fraud and the data breaches it causes to some extent. For example, combining fingerprint

recognition with passwords adds extra layers of security to behavioral analysis and biometrics, reducing the likelihood of successful fraud.

3.3 Establishment of policies and industry standards

To address the fairness and trust issues raised by AI as a fraud detection method, experts suggest that the final layer of fraud detection measures can often benefit from human judgment. In this regard, a hybrid model seems to be a better choice. AI brings speed and scale, while humans bring nuance and accountability. Mastercard's Chief Data Officer, Andrew Reiskind, agrees with this. In the company's AI governance program, employees can oversee all AI-driven operations and solutions.

Even though AI can already replace humans in some tasks in today's society, we still need to adhere to a people-centered approach. Advanced technology can not only improve efficiency and produce excellent products, but it should also ensure that its technology complies with ethical standards and legal regulations.

References

[1] Zhang, X, N. (2021), Research on Payment Risk Prevention under New Technologies [J]. Heilongjiang Finance,2021, (06):58-59.
[2] Cao, Q., &Hou, J, R. (2015), The application of electronic payments in robots[J]. Rubber and Plastics Technology and Equipment,2015,41(18):14-15. DOI: 10.13520/j.cnki.rpte.2015.18.007.
[3] Ke, Z., & Yin, Y. (2024). Tail Risk Alert Based on Conditional Autoregressive VaR by Regression Quantiles and Machine Learning Algorithms. arXiv preprint arXiv:2412.06193.
[4] Sharma, M., & Kaur, M. (2022). A review of Deepfake technology: an emerging AI threat. Soft Computing for Security Applications: Proceedings of ICSCS 2021, 605-619.
[5] Chadha, A., Kumar, V., Kashyap, S., & Gupta, M. (2021). Deepfake: an overview. In Proceedings of second international conference on computing, communications, and cyber-security: IC4S 2020 (pp. 557-566). Springer Singapore.
[6] Whyte, C. (2020). Deepfake news: AI-enabled disinformation as a multi-level public policy challenge. Journal of cyber policy, 5(2).
[7] Qin, Y., Mitra, N., Wonka, P. (2020). How Does Lipschitz Regularization Influence GAN Training? Computer Vision – ECCV 2020. ECCV 2020. Lecture Notes in Computer Science, vol 12361. Springer, Cham. https://doi.org/10.1007/978-3-030-58517-4_19
[8] Arshed, M. A., Mumtaz, S., Ibrahim, M., Dewi, C., Tanveer, M., & Ahmed, S. (2024). Multiclass AI-Generated Deepfake Face Detection Using Patch-Wise Deep Learning Model.Computers, 13(1), 31.
[9] Giudice, O., Guarnera, L., & Battiato, S. (2021). Fighting deepfakes by detecting gandct anomalies. Journal of Imaging, 7(8), 128.).
[10] Singh, S., Sharma, R., & Smeaton, A. F. (2020). Using GANs to synthesise minimum training data for deepfake generation. arXiv preprint arXiv:2011.05421.
[11] Zong,K.,etal.(2025). Detection of AI Deepfake and Fraudin Online Payments Using GAN-Based Models.arXivpreprintarXiv:2501.07033.
[12] Komarraju,A.K.,et, al. (2024). Enhancing Digital Payment Security with Biometric Authentication and AI: A Big Data Approach. International Journal of Engineering and Computer Science. DOI: 10.18535/ijecs/v13i04.4811