International Journal of Science and Research Archive

eISSN: 2582-8185

Cross Ref DOI: 10.30574/ijsra

Journal homepage: https://ijsra.net/

(Review Article)

AI-enhanced peer to peer payment security

Venkata Mohit Tamanampudi *

AIML/DevOps Automation Engineer, Independent Researcher

International Journal of Science and Research Archive, 2023, 10(01), 1076–1083

Publication history: Received on 16 August 2023; revised on 19 October 2023; accepted on 29 October 2023

Article DOI: https://doi.org/10.30574/ijsra.2023.10.1.0570

Abstract

The use of peer-to-peer payment methods has enhanced the use of payments through technologies that allow users to transfer money directly. However, this innovation has also come with some risks, especially in the security of financial information, requiring high protection levels. This paper aims to discuss using artificial intelligence to improve the security of P2P payment platforms. AI has a robust protection mechanism against crime in transactions through machine learning algorithms in fraud detection, biometrics authentication, and risk assessment. Besides, it looks at future developments such as new trends in AI, potential changes in laws that govern the use of the technology, and the integration of blockchain for enhancing the security infrastructure. Finally, the paper also points out the significance of AI regarding P2P payment security and its importance in increasing user trust and maintaining the credibility of P2P payment systems.

Keywords: AI-driven payment protection; Secure peer-to-peer transactions; Machine learning in payment security; Fraud detection in digital payments; Blockchain and AI security

1. Introduction

P2P payment means the direct cash transfer from one person to another without help from third parties such as banks. It is usually accomplished through a mobile application or any online interface whereby money is transferred from one account to another through linked banks, credit cards, or stored value. Examples of P2P payments include Venmo, PayPal, Cash App, and Zelle, among others.

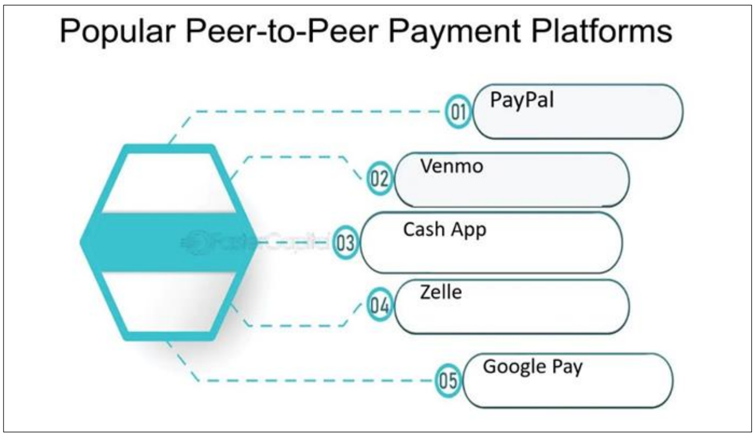


Figure 1 Popular P2P payment platforms

* Corresponding author: Venkata Mohit Tamanampudi

1.1. Security Consideration in P2P Transactions

- **Financial Risks:** Since P2P involves the exchange of personal and or financial details, they are prone to fraud and cybercrimes.
- **User Trust:** This is disastrous for P2P platforms since users lose a lot of money, and security breaches dent the users' confidence in the particular P2P platform.
- **Regulatory Compliance:** Policies on financial regulations and standards should still be followed to preserve user data and the companies' legitimacy.
- **Reputation Management:** A safe payment system makes users trust the platform and continue using it, and new customers are attracted.

1.2. Overview of P2P Payment Systems

With society and the world adopting digitalization, financial transactions have significantly changed. Digital or peer-to-peer (P2P) payments are a fast, safe, and easy way for two individuals to transfer money without using banks. This paper aims to give insight into the historical development, security precautions, current state, and prospects of P2P payments. P2P payments have a long history and development process, from the swap between people to the modern digital options. First, such operations presupposed the direct cash or checks swap between individuals familiar with each other. However, this process has been eased due to technological development, and various P2P payment platforms such as PayPal, Venmo, and Cash App have been developed. Mobile devices have also boosted the use of cards because they are easily used on devices with a few touches on mobile phones.

1.3. How P2P Payments Work

P2P payment systems are used to transfer money from one person to another through electronic means. To do this, a user links their bank account or credit/debit card with these platforms to enable them to transact using the same by sending or receiving money instantly. In the usual scenario, the recipient is selected, the amount is entered, and the transfer is authorized. Some security measures most P2P payment services use include encryption and secure protocols for users' financial data.

1.4. The Transformative Power of Blockchain and Generative AI for Secure P2P Transactions

The field of P2P payment is experiencing a significant change because of the application of blockchain technology and generative AI in the context of Procure-to-Pay solutions. Thus, blockchain is an effective system of record keeping as it is an immutable database storing information about transactions that cannot be changed. Similarly, generative AI automates tasks and helps in decision-making while offering more efficient ways of bargaining. Altogether, these technologies recast procurement's operational effectiveness and protection principles.

1.5. How Generative AI Strengthens Blockchain Security in P2P

Integrating generative AI with blockchain significantly improves the security measures of decentralized P2P networks. Here's how this synergy improves security:

- **Advanced-Data Analysis:** AI algorithms can work quickly and analyze big data sets, allowing us to identify suspicious or fraudulent activity in the blockchain network quickly.
- **Predictive Capabilities**: Since generative AI is trained on historical transactions and can predict security threats from patterns, one can be able to prevent them.
- **Automated Transaction Verification:** AI validates all the transactions and, therefore, all the records put in the blockchain; this reduces the risk of humans manipulating the data entered into the blockchain.

A study conducted by a top business school reveals how AI improves the security systems in blockchain, thus reducing activities among organizations that adopt the two technologies combined.

1.6. AI in Finance: Transforming Payment Security

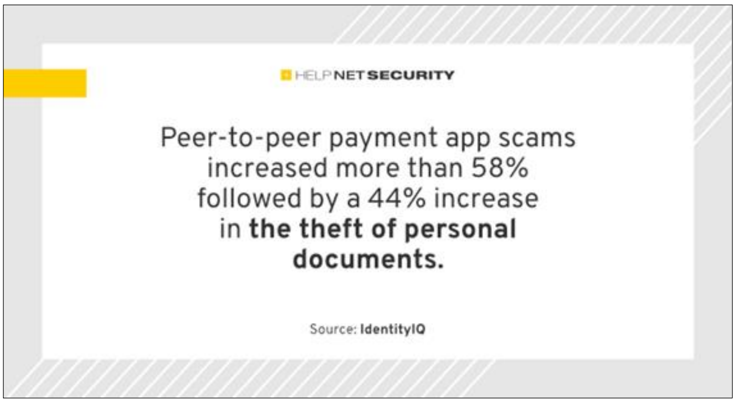
Here's how AI is reshaping the landscape of payment security in the financial sector:

- **Predictive Analytics:** AI algorithms can analyze historical data to predict potential fraud attempts, allowing institutions to implement preventative measures proactively.
- **Natural Language Processing (NLP):** NLP can analyze text-based communications, helping to identify phishing attempts or social engineering attacks.

- **Machine Learning**: Machine learning models can continuously learn from new data, improving their accuracy and efficiency over time. This adaptability is crucial in an environment where fraud tactics are constantly evolving.
- **Edge AI:** By processing data locally on devices, Edge AI can enhance security and reduce latency in payment transactions, which is particularly important for IoT payments.

1.7. AI Technologies in Payment Security

Advanced cyber threats are growing in the present world of the internet and a vast amount of e-commerce. The need for sound and new security measures has become more critical in this environment, which is still evolving for both the business and the consumer. This is where Artificial Intelligence (AI) comes into play—a phenomenon revolutionizing how financial transactions are protected. Unlike traditional security systems, which only act after threats have occurred, AI applies algorithms and real-time data processing to guard vulnerable financial data.



HELPNETSECURITY

Peer-to-peer payment app scams increased more than 58% followed by a 44% increase in **the theft of personal documents.**

Source: **IdentityIQ**

Figure 2 Estimate of personal document theft

For example, an example of AI use was recently illustrated in the case of a high-profile enterprise where AI was instrumental in averting a major cyber-attack on millions of dollars in transactional funds. This case shows the practical use of AI to fight fraud and demonstrates that AI is becoming an integral component of today's payment protection systems. Through the adoption of artificial intelligence in the security of financial institutions, it is not only that the institutions are questioning conventional practice but also setting the pace for safety, efficiency, and reliability in the financial services industry for the future.

Payment security is critical due to the increased risk of fraud and cyberattacks in the digital environment. This is a common scenario, especially given that security solutions today are constantly under pressure from new technology developments. Still, artificial intelligence is gradually making its way into payment fraud prevention and increasing security measures.

2. Comprehensive Defense Mechanisms

Mobile payment security has benefited significantly with the help of Artificial Intelligence (AI). They have more sophisticated algorithms and predictive functions that allow them to provide comprehensive protection against fraud and other unlawful activities.

AI is exceptionally suited for high-volume, real-time data processing, making it possible for the system to recognize patterns and accurately pinpoint fraud cases. For example, a study by Shailendra Mishra at Majmaah University proposed a new cybersecurity technique: Artificial Intelligence for financial sector management (CS-FSM). This method increases the efficiency of cybersecurity systems by strengthening the systems' protection from cyberattacks, thus leading to greater data privacy by 18. 3%; scalability by 17. 2%; risk minimization by 13. 2%; data security by 16. 2%, and evasion of attacks by 11. 2%.

2.1. AI-Based Fraud Detection Systems

The rollout of AI-based fraud-detecting technologies has the potential to revolutionize payment protection. Machine learning algorithms can analyze massive data sets and identify trends and anomalies that depict fraud.

These systems learn from new data and can update themselves with the latest developments in fraud strategies, making them very useful in real-time fraud detection. By applying artificial intelligence, financial institutions, and payment processors will be able to enhance the detection of suspicious transactions and thus decrease fraudulent actions.

2.1.1. Critical factors of the AI-based fraud detection

AI-powered fraud prevention systems consist of several critical components and stages: AI-powered fraud prevention systems consist of several essential components and stages:

- **Data Collection:** As is with any application of artificial intelligence, the data input has to be accurate and of high quality in the case of fraud prevention systems. This system uses transactional and behavioral data from sources to support decision-making and analysis.
- **Understanding Decision-making Behavior**: The next step involves determining the characteristics or patterns of actions that depict the fraud. AI systems analyze the actions of users and differentiate between them and fraudsters.
- **Model Training:** Only when enough data is collected and behavioral patterns are identified are machine learning algorithms tested in real life. Fraud detection is identified using models that are developed based on historical data.
- **Anomaly Detection:** The system depends on the algorithms to notify it of any abnormality in the data. **Continuous Learning:** The reason is that fraudulent strategies may evolve, and a machine learning model has to be trained with new data and patterns from time to time.
- **Alerts and Reports:** If the system identifies data that are different from standard patterns of the authorized users, the system alerts users of such activity and produces reports that can be used for further examination.

Therefore, the AI-driven fraud prevention model needs a lot of data, model training, and continual learning to meet payment security needs.

2.2. Biometric Authentication

Besides identifying fraudulent activities, AI systems are now changing customer authentication overall. By processing different types of data and their behavioral characteristics, AI improves the security and credibility of the customer identification process. This improved accuracy in authentication, coupled with increased security, is essential to ensure that only the rightful users are granted access and to minimize or eradicate fraudulent transactions. Biometric identification using artificial intelligence is reliable for identifying individuals during financial transactions. Fingerprints, facial recognition, and voice recognition are among the biometric features unique to an individual and, hence, very reliable in authentication. AI systems can also analyze biometric data and check this data against templates to ensure the user is genuine.

Passwords and PINs can be easily hacked or bypassed. In contrast, biometrics allow AI to offer users a good and secure interface while ensuring that a third party cannot imitate their identity.

2.3. Anomaly Detection and Behavioral Analysis

With the help of advanced algorithms, AI systems can analyze large volumes of transactional data and customer behavior to identify signs that reflect fraudulent transactions. In this way, AI can set the parameters of normal behavior and look for unusual transactions.

For instance, if a customer tends to buy a large quantity of products, the AI system can notify the management of possible fraud. Further, AI can assess the risk linked to a transaction using other details like device details, location, and transaction history. With the help of AI, it is possible to detect and analyze the anomalies and inefficient behavior of payment systems and, therefore, prevent fraud.

2.4. Cybersecurity and Threat Intelligence

AI improves cybersecurity and threat intelligence and strengthens payment security. It handles and analyzes large volumes of data, such as network traffic and system logs, and feeds from threat intelligence sources to help identify and prevent cyber threats.

If AI can identify patterns of emerging malicious activity, such as malware infections or attempts at illegitimate access, risks can be addressed immediately. In addition, AI can help identify and mitigate new threats that may emerge in the future concerning payment systems' security.

2.4.1. The Advantages of AI in P2P Payment Security

By implementing AI-driven monitoring systems to enhance payment security, businesses can enjoy several key advantages:

- **Real-Time Protection:** Artificial intelligence in a business organization constantly tracks vast volumes of transactional and behavioral data to identify fraudulent activities at their early stages. This is important in preventing fraudsters and reducing the losses incurred.
- **Scalability:** Adopting machine learning systems makes it easy to scale when the business expands as the systems are scalable. Despite rising transaction traffic, there have been no decreases in security, and AI solutions do not need more employees.
- **Cost Efficiency:** One of such strategies is the effective use of AI. Organizations will not need to employ staff to carry out manual fraud detection, thus saving personnel to focus on other essential duties. Also, AI solutions increase efficiency, which leads to the prevention of losses from fraud.
- **High Accuracy Over Time:** While fraudsters adapt new schemes, AI models can continue learning to enhance their abilities to identify fraud. For this reason, the training and adaptation of this AI continue to occur to ensure its efficiency in the fight against new threats. Besides fraud mitigation, AI solutions also improve customer reputation by creating a sense of trust that goes further than conventional marketing.

3. AI-Powered Solutions in Practice

Everything considered, it is clear that the application of Artificial Intelligence in fraudulent transactions has the following benefits. However, what advantages are there to including new AI-based systems?

- **Card Fraud Detection:** Card fraud losses were estimated to be $32 in 2021. This makes it a common problem, as companies spend 34 billion on cyber risks yearly. The main weakness of cards is that fraudsters use bots to accomplish their goals. Machines can also watch for suspicious activity to separate bots from users, especially in IP addresses and behavior.
- **Fake Account Detection**: Automated accounts are problematic because they interfere with genuine product reviews, share phony information, and thus mislead consumers and skew analytical data. Therefore, it is clear that using AI-backed systems in the authorization phase improves the system's security without hampering the entrance of legitimate new members. AI-based payment protection is highly valued nowadays by businesses globally, and it results in the proper implementation of as many solutions as possible that allow for the prompt detection of fraud cases and +enhance payment security. For example:
    - Rakuten France continued to be attacked and required constant protection, so it had to hire more employees. Such an approach eliminated the problem, thus making an AI-based solution the best.
    - VISA is one of the biggest payment service providers, and the company started using VISA Advanced Authorization; AI algorithms could process all the obtained data. This integration helped save the company $25 billion in potential fraud.
    - US Bank, RBC, and Santander have incorporated the AI platform Personetics, which, based on behavioral analysis, counters fraud and safeguards users' information.

4. The Limitations of AI

As with any technology, AI has limitations. It is good at pattern detection, anomaly recognition, and fraud prevention. AI systems work based on patterns and correlation analysis of vast databases but do not possess the complete understanding, creativity, and situational awareness inherent to human intelligence. This gap can render AI systems easily exploitable by highly advanced attacks and other forms of fraud that may be beyond the ability of the AI to recognize.

4.1. Emerging Threats and Adversarial Attacks

Threats are constantly evolving, and criminals are becoming more creative in their attacks on payment systems and even implementing adversarial attacks on AI. Such attacks involve changing inputs to deceive the AI model into considering fraudulent activities as usual. The downsides of these systems include that they may not quickly detect new threats once they are left to operate independently of human control. Human analysts can understand cybercriminals' motives and subtle patterns of intentions and, therefore, can quickly respond to new threats by modifying security strategies.

4.2. Ethical Issues and Prejudiced Decision Making

AI algorithms rely on past data for their predictions and results. If this training data is biased, discriminative patterns may be learned and incorporated into the decision-making system. In payment security, such algorithms may be biased and financially disadvantage some people while disadvantaging others by not detecting suspicious activities or approving legitimate transactions.

Humans need to supervise AI systems to prevent them from deepening social bias. Experts can advise on ethical concerns, and algorithm outputs can be controlled and modified in case of bias towards any particular segment in payment security.

4.3. Unforeseen System Failures and False Positives

Sophisticated AI systems can also fail or produce false alarms at once. Such issues can lead to identifying genuine transactions as fraudulent, creating inconveniences for users and reducing confidence in the payment system. However, responding to such problems as soon as possible can be complex without controls. This allows human experts to examine flagged transactions, work on suspicious cases, and make decisions relying on contextual information that an AI algorithm cannot identify. They can also reduce false favorable rates, making the payment process much more manageable while enforcing enough security.

4.4. Accountability and Legal Compliance

In an AI-based payment security environment, there are issues related to liability and the law. AI systems may perform actions with legal consequences or requirements or are against the law. Without human intervention, accountability cannot be given, and compliance with the law cannot be enforced. Finally, human supervision of AI systems guarantees that the systems provide ways of checking and explaining their actions to make decisions. This reduces the chances of prejudice, cheating, and non-compliance with the law and other regulations, thus protecting both the user and the service provider.

5. The Indispensable Role of Human Involvement

Payment security is also increased with the help of AI, but human interference is also crucial. Human experts bring valuable assets, which include decision-making, context awareness, moral reasoning, and the ability to learn about newer threats. Through integration with AI systems, they can always be on the lookout for the best security measures to ensure the payment ecosystem is secure, efficient, and adaptive to future threats.

5.1. Adaptive Learning: AI's Continuous Evolution

Another benefit of applying AI in payment security is that it develops and evolves its capabilities more and more. AI systems are not static; they are created with machine learning algorithms to mitigate advanced fraud schemes. This is well illustrated by fraudsters constantly evolving their modus operandi to evade these traditional security measures. The AI systems can understand each attempted breach or anomaly in the existing system and hence develop better ways of detecting such attacks in the future; it improves the overall security of payment systems.

Nonetheless, there is a lot of talk about how helpful AI's learning abilities are in the long run. It is essential to understand that, like any other line of work, AI systems need continuous management and updates as they improve with the data and experience they receive. The efficiency of the learning abilities of AI depends on the constant feed of large volumes of good-quality data sets and the constant tuning of algorithms to meet emergent threats and changes in consumer behavior. Lenders must dedicate resources to maintaining and enhancing AI solutions to counter ever-emerging cybersecurity threats.

5.2. The Future of AI in Payment Security

In the future, AI will continue to be the critical solution in payment security. Here are some expected trends:

- **Advanced Biometrics**: AI will expand the use of more complex forms of biometric authentication, such as voice recognition, facial recognition, and even gait analysis.
- **Quantum-Resistant Cryptography:** While quantum computing threatens modern cryptography, AI will play a crucial role in creating and implementing quantum-safe cryptography.
- **Federated Learning:** This AI approach helps train strong fraud detection models without sharing customers' data, a significant concern in the open banking environment.

- **Explainable AI:** As the systems continue to become sophisticated, there will be a need for 'explainable AI' in payment security so that human beings can understand and oversee the security decisions made by the AI systems.

5.3. Anticipated Changes in Regulatory Standards

Stricter Compliance Requirements: This may lead to the enhancement of more strict rules and regulations by the regulatory bodies on data protection and fraud control in P2P transactions. Standardization of Security Protocols: There may be a shift in policy where all P2P platforms are made to exhibit a certain level of security to which all have to adhere.

- **Focus on Consumer Protection:** The focus on protecting consumers from scams and unauthorized transactions will be higher, thus enhancing security measures among the platforms.
- **Cooperation Between Regulators and Tech Companies**: Promotion of collaborative relations between the regulatory bodies and the technology suppliers in developing frameworks that offer security while at the same time supporting innovation.

5.4. Embracing AI for Unprecedented Security in Digital Finance

Incorporating AI in payment security systems is a significant advancement in the fight against fraud and the safety of payments. These new applications of AI, in combating fraud, identifying customers, and managing risk, enhance operations efficiency while upholding the credibility of online financial services. Payment security in connection with AI means a more secure, efficient, and reliable payment system in a rapidly progressing digitalization world.

Nevertheless, the path continues after the AI technologies are deployed. AI's value is based on its ongoing development and respect for customer privacy and data protection. To this end, financial institutions must rely on these intelligent systems more than ever to shield their customers from emerging cyber threats.

6. Conclusion

With features such as fraud detection, biometric authentication, anomaly detection, and cybersecurity measures, AI offers payment security a fresh future. AI in payment systems helps prepare payment systems for new fraud techniques, provides users with a secure experience, and minimizes the probability of fraud.

However, the successful use of AI in payment security depends on privacy, ethical issues, partnership, and integration into the payment system. Thus, AI can mean a turning point in payment security, the constant development and emergence of new technologies with cautious application to further enhance the payment security level.

References

[1] The Role of Artificial Intelligence in Fraud Detection and Payment Security. (2024, April 3). https://tranzzo.com/blog/the-role-of-artificial-intelligence-in-fraud-detection-and-payment-security

[2] Szymanski, B., & Szymanski, B. (2024, May 15). P2P Payments — A Brief Overview of Peer-to-Peer Payments. PAYCRON -. https://www.paycron.com/blog/p2p-payments-the-evolution-security-and-future-of-peer-to-peer-payments

[3] The AI Revolution in Payment Security: Safeguarding Digital Transactions. (2024, August 27). https://ozow.com/blog/the-ai-revolution-in-payment-security-safeguarding-digital-transactions#:~:text=AI%20is%20revolutionising%20payment%20security,decisions%20to%20thwart%20fraudulent%20activities.

[4] Magnates, F. (2023, June 19). Can AI Revolutionize Payment Security? https://www.linkedin.com/pulse/can-ai-revolutionize-payment-security-financemagnates

[5] Luong, T. (2024, April 12). AI: The Keystone of Modern Payment Security Architecture - SmartDev. SmartDev. https://www.smartdev.com/ai-the-keystone-of-modern-payment-security-architecture/

[6] Bionducci, L., Botta, A., Gathinji, C., Jain, R., Bruno, P., Denecker, O., Nadeau, M.-C. and Sattanathan, B. (2023). The 2023 McKinsey Global Payments Report | McKinsey. [online] www.mckinsey.com. Available at: https://www.mckinsey.com/industries/financial-services/our-insights/the-2023-mckinsey-global-payments-report.

[7] Chui, M., Hazan, E., Roberts, R., Singla, A., Smaje, K., Sukharevsky, A., Yee, L. and Zemmel, R. (2023). Economic Potential of Generative AI | McKinsey. [online] www.mckinsey.com. Available at: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-economic-potential-of-generative-ai-the-next-productivity-frontier#key-insights.

[8] J.P.Morgan (2023). AI Boosting Payments Efficiency & Cutting Fraud | J.P. Morgan. [online] www.jpmorgan.com. Available at: https://www.jpmorgan.com/insights/payments/payments-optimization/ai-payments-efficiency-fraud-reduction.

[9] Kadar, T. (2024). Wired-In: AI in Payments: Balancing Security with User Experience. [online] resources.northrow.com. Available at: https://resources.northrow.com/wired-in-payments-in-ai-balancing-security-with-user-experience [Accessed 12 Apr. 2024].

[10] Maynard, N. (2022). AI in Financial Fraud Detection: Key Trends, Competitor Leaderboard & Market Forecasts 2022-2027. [online] www.juniperresearch.com. Available at: https://www.juniperresearch.com/research/fintech-payments/fraud-identity/ai-financial-fraud-detection-trends-report/

[11] Mishra, S. (2023). Exploring the Impact of AI-Based Cyber Security Financial Sector Management. Applied Sciences, [online] 13(10), p.5875. doi:https://doi.org/10.3390/app13105875.

[12] squaremile (2023). How AI Is Revolutionising Mobile Payments Security. [online] Square Mile. Available at: ttps://squaremile.com/article/ai-mobile-payments-security/ [Accessed 12 Apr. 2024].

[13] Technologies, C. (2023). Generative AI Revolution: Top 10 Use Cases in Banking and Payments | Cigniti. [online] Cigniti. Available at: https://www.cigniti.com/blog/top-ten-use-cases-generative-ai-banking-payment-industry/ [Accessed 12 Apr. 2024].

[14] Vanini, P., Rossi, S., Zvizdic, E. and Domenig, T. (2023). Online Payment fraud: from Anomaly Detection to Risk Management. Financial Innovation, 9(1). doi:https://doi.org/10.1186/s40854-023-00470-w.

[15] Zaytsev, A. (2023). Case Study: Harnessing AI for Financial Security at Visa. [online] AIX. Available at: https://aiexpert.network/case-study-harnessing-ai-for-financial-security-at-visa/ [Accessed 12 Apr. 2024].

[16] Zou Yanting and Ali, M. (2023). Artificial Intelligence, Digital Finance, and Financial Inclusion: A Conceptual Framework. Emerald Publishing Limited eBooks, pp.77–85. doi:https://doi.org/10.1108/978-1-83753-304-620231006.

[17] Oyeniyi, J. Combating Fingerprint Spoofing Attacks through Photographic Sources.

[18] Bhadani, U. (2020). Hybrid Cloud: The New Generation of Indian Education Society.

[19] Bhadani, U. A Detailed Survey of Radio Frequency Identification (RFID) Technology: Current Trends and Future Directions.

[20] Bhadani, U. (2022). Comprehensive Survey of Threats, Cyberattacks, and Enhanced Countermeasures in RFID Technology. International Journal of Innovative Research in Science, Engineering and Technology, 11(2).

[21] Nasr Esfahani, M. (2023). Breaking language barriers: How multilingualism can address gender disparities in US STEM fields. International Journal of All Research Education and Scientific Methods, 11(08), 2090-2100. https://doi.org/10.56025/IJARESM.2024.1108232090