iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** III **Month of publication:** March 2024

DOI: https://doi.org/10.22214/ijraset.2024.59352

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue III Mar 2024- Available at www.ijraset.com

Fraudguard: Innovations in Financial Transaction Security

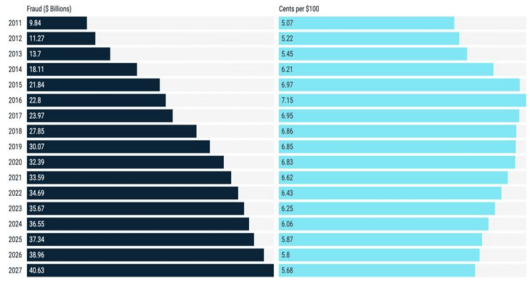
Anupama K[1], Mr. Pramod K[2]
[1]*MCA Scholar,* [2]*Associate Professor, Department of MCA, Nehru College of Engineering and Research Centre, Pambady,*

Abstract: ***This paper discusses the importance of improving authentication and detecting fraud in mobile payments and financial technologies. It examines data analytics, new technologies, and current authentication methods, emphasizing how they enhance security. Taking precautionary steps is crucial in reducing the extensive risks linked to fraud. This study creates a strong structure for safeguarding financial transactions, impacting the course of financial technology, and ensuring financial integrity and user trust amidst evolving payment methods and online threats through the analysis of case studies, industry regulations, and top practices.***

Keywords: fintech, authentication, wireless, biometric, transactions, verification, blockchain, industry, security, regulation, bank, fraud, payments

I. INTRODUCTION

The financial services sector has been transformed by the FinTech industry. However, it is essential to detect fraud and authenticate. According to McKinsey's study, banks are facing a significant risk of fraud. The payments industry has expanded significantly, causing losses for banks. Projected to surpass $31 billion worldwide by 2018. There has been a rise in the use of digital and mobile customer platforms as well as weaknesses within payment services. Today, economic transactions are very common and easily accessible. Fraud is constantly a potential danger. Stringent measures need to be implemented to ensure safety. Safeguard the money that has been earned through hard work. Recent estimates indicate that estimated peak of $5 trillion by 2025.By 2027, an incredible $40 billion is expected to be reached, emphasizing the necessity in search of innovative methods to stop online fraud.From 2011 to 2027, the predicted amount lost to payment fraud is forecasted to exceed $40 billion having more than tripled during this time period.



Fraudulent activity on various types of payment cards results in financial losses for organizations such as payment card issuers, retailers, and transaction and ATM acquirers worldwide. This paper investigates the use of new technologies, regulatory frameworks, and current methods in detecting fraud and ensuring authentication in FinTech and wireless payment sectors. It offers advice, suggestions, and guidance to improve security and trust, predict trends, and encourage growth and sustainability in the FinTech sector.

II. LITERATURE SURVEY

Previous attempts, among other established solutions for detecting click fraud, have utilized AI-driven methods like machine learning (ML) and deep learning (DL). These are designed to shield advertisers from incurring fraudulent click costs that can harm their ad campaigns, with AI technology being utilized to distinguish between valid and invalid ad clicks effectively on both server and user.

In this part, we examine prior research done on the identification and mitigation of click fraud.Our assessment is based on the criteria listed below:

- Case studies that utilized AI methods, such as machine learning and deep learning.
- Research focused on identifying click fraud in the advertising sector, with a specific emphasis on studies related to click fraud detection.
- Carried out within the past decade (2012-2022)
- Expressed in the English language.

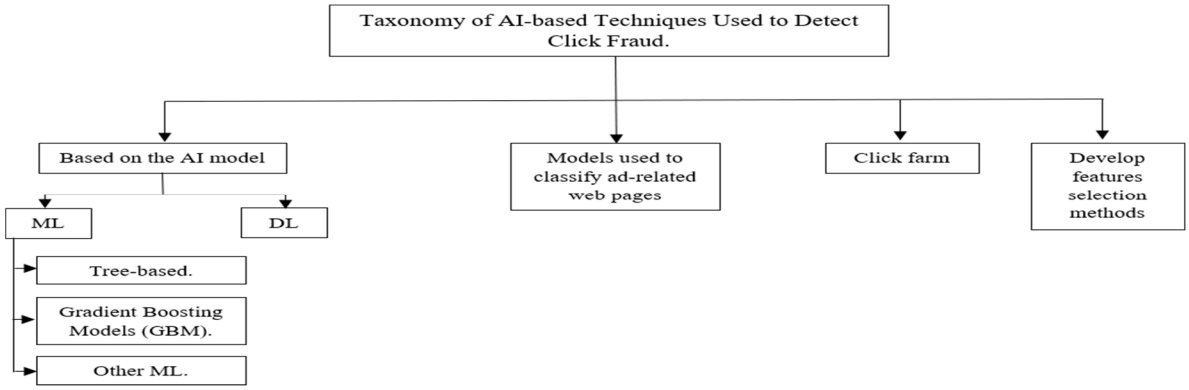


Figure2. Classification of the Literature Review

1) Techniques for detecting click fraud using Machine Learning

a) Tree Based Techniques: Tree-based methods, such as Decision Trees, Random Forests, and Extremely Randomized Trees, are highly effective at pinpointing the sources of clicks for detecting fraud in online advertising. MadTracer by Li et al. and studies conducted by Berrar and Yan & Jiang demonstrate the effectiveness of these systems. These techniques use characteristics such as click profiles and IP analysis to accurately identify fraudulent behavior. Perera et al. present a model that combines user behavior patterns and achieves significant success with different classifiers. Oentaryo and Lim concentrate on extracting features to train machine learning models for identifying click fraud. In general, these studies demonstrate the effectiveness of using tree-based methods to enhance security in mobile payments and financial technologies.

b) Gradient Boosting Model Techniques: The passage describes research using gradient boosting models to identify click fraud in online advertising. Different strategies are examined, such as feature extraction techniques, model integration frameworks, and comparing algorithms. These researches highlight the importance of fundamental statistical techniques, creating relevant features, and thoughtful algorithm choice to tackle issues such as overfitting, complex data, and imbalanced class distribution. Through the use of methods like LightGBM and gradient tree boosting, researchers have made significant progress in improving both the accuracy of fraud detection and the efficiency of the model. In spite of obstacles like restricted feature options, these research projects as a whole help advance the enhancement of click fraud identification techniques.

c) Other ML: Several machine learning models are analyzed for identifying click fraud. Gabryel integrates TF-IDF to weigh features and KNN for classifying clicks, leading to improved results. Almahmoud et al. suggest a model with two stages that combines rule-based and ML-based fingerprints, with KNN achieving high precision. Pan et al. use frequent pattern mining and SVM to effectively identify click fraud. Thejas and colleagues primarily study how to represent temporal click fraud data through AR and MA models, then utilizing LR classification to predict fraud on a large scale with few features. These techniques provide different ways to effectively detect fake clicks in digital marketing.

2) Techniques for Detecting click fraud using Deep Learning

Research is conducted on deep learning (DL) for detecting click fraud. Mouawi and colleagues present the CFC model, which combines unique characteristics with machine learning techniques such as KNN, ANN, and SVM, enabling external tracking through crowdsourcing. Renström and Holmsten utilize unmonitored machine learning with autoencoders, finding that stacked models are successful. Zhang and colleagues create CSBPNN-ABC, which combines backpropagation neural networks with artificial bee colony algorithms to identify mobile ad clicks. By building on past research, they enhance feature selection and introduce a combined ANN-AE model to address bot manipulation, successfully detecting fraud even with imbalanced datasets. These methods improve the detection of click fraud by using deep learning techniques.

3) Models used to classify Ad-related Webpages

Researchers are studying AI models to identify click fraud by classifying pages that have advertisements. Crussell et al. concentrate on fraudulent activity within Android apps, developing MAdFraud to detect fake clicks and impressions within various apps. They utilize RF utilizing characteristics such as request duration and timestamp, detecting 21 fake applications. Iqbal and colleagues present FCFraud to stop devices from participating in click fraud caused by malware by incorporating it into anti-malware programs. FCFraud utilizes past events, examines HTTP packets, and applies ML algorithms (NB, SVM, KNN, C4.5, RF) to spot advertising requests, then implements heuristic methods to prevent fraudulent clicks. These techniques improve the detection of click fraud in different situations.

4) Clickfarm

Additionally, certain research has centered on click farming, a form of click fraud where a substantialamount of inexpensive workers are employed to click on sponsored ad links.Jiangetal.[75] applied PU learning to collect trustworthy negative instances from an unlabelled dataset. They employed weighted logistic regression to assess the impact of extracted features in studying click farming on a major Chinese ecommerce platform and to explore the presence of click farming in stores operating on this platform. Out of various classes such as SVM, RF, and NN, the ensembling method which combined them resulted in the highest accuracy of 97.4%.

5) Develop Feature Selection(FS) Methods

Scientists create methods for selecting features in click fraud data sets. Taneja et al. introduce HDDT with recursive feature elimination, reaching 64.07% accuracy. Thejas and colleagues suggest methods for including features based on metrics and accuracy rankings, improving algorithm performance even without knowing the exact number of features beforehand. They further present Kalman-SMOTE (KSMOTE), combining SMOTE with a Kalman filter in order to maintain class equilibrium. KSMOTE demonstrates superior performance on imbalanced ad click datasets compared to previous algorithms, indicating notable performance enhancements. These methods improve feature selection and tackle data imbalance issues in detecting click fraud.

III. CURRENT AUTHENTICATION METHODS

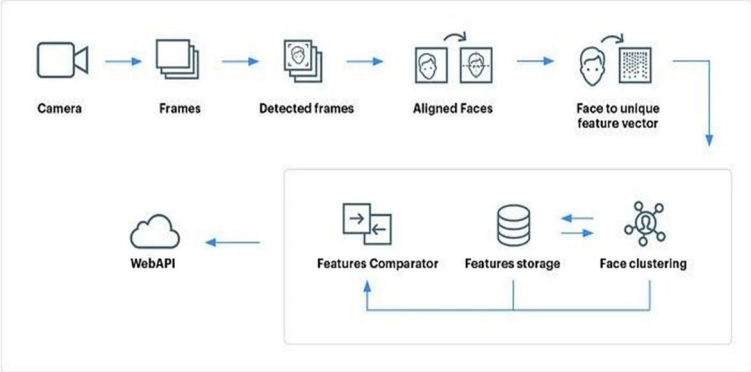
The security of the FinTech and wireless payments sectors is a top priority, and they utilize a range of authentication methods. Passwords, which are easily compromised, are made more secure with two-step verification (2SV) but are still at risk of phishing attacks. Biometric techniques, such as fingerprint and facial recognition, enhance security measures, but worries remain about accuracy and privacy. Token-based systems provide increased security, however, they might not be as convenient. Even with improvements in biometrics, there are still weaknesses that require adherence to industry regulations such as GDPR, EMV, and PCI DSS to protect data security and privacy. Following these regulations helps lower the chance of breaches and cyber-attacks, protecting sensitive data. Biometric systems provide more security against brute-force attacks than passwords.
Figure displays a sample of fingerprint recognition used for authentication

Image provided as input for fingerprint recognition;
(A) is the input image (B) represents the features

In order to prioritize both security and user convenience, it is essential to consistently come up with new ideas and follow rigorous regulations.

IV. EMERGING TECHNOLOGIES

Authentication in FinTech and wireless payments is changing along with advancements in technology. Methods such as fingerprint, facial recognition, SMS OTP, Push Notification Authentication, and eye scanners provide secure identity verification, decreasing the need for complicated passwords [33]. These technologies make use of distinct physical characteristics, improving user convenience. A rise in biometric transactions is occurring as 65% of consumers are knowledgeable about biometrics. Facial recognition uses machine learning to compare facial features to saved data, while fingerprint recognition confirms identity through distinct patterns on fingertips.



The passage emphasizes how biometric authentication, multi-factor authentication (MFA), and blockchain technology are essential in enhancing security and user experience, specifically in mobile payments and FinTech. It highlights the advantages of biometrics in streamlining authentication procedures, while MFA enhances security levels without sacrificing ease of use. Moreover, the text emphasizes the significance of integrating MFA into email platforms to improve security and recommends implementing strong account recovery procedures. It highlights the importance of blockchain in guaranteeing transparency and security in transactions.
Finally, it highlights Apple's Face ID as an instance of advanced biometric authentication and praises financial institutions for effectively incorporating MFA and blockchain to enhance security and user experience in financial transactions.

V. FUTURE TRENDS AND RECOMMENDATIONS

Regulatory compliance is essential for stability and security due to the fast-paced evolution of the financial technology and payments sectors. Efficient laws and regulations ensure the security of consumers, protect data, and deter unauthorized activities. They establish criteria for protecting data, verifying identities, and preventing fraud, and mandate reporting procedures for security breaches or fraudulent actions.
Regulatory bodies such as FinCEN and EBA consistently adjust to enhance industry defenses against fraud and security vulnerabilities, ensuring businesses adhere to regulations and adhere to essential protocols to avoid financial harm to consumers and businesses. Nevertheless, these rules can require FinTech companies to adhere to certain standards and paperwork, potentially limiting their ability to expand and develop new ideas . Continual collaboration and coordination between industry stakeholders and regulatory agencies are required to maintain a balance between regulation and innovation.
Establishing a robust regulatory framework is essential for instilling trust in the FinTech and payment industries. Regulatory compliance can support industry growth and innovation by promoting security, trust, and protection against financial harm for consumers and businesses. By implementing appropriate regulations, the sector can progress and create new ideas, while also protecting the safety and reliability of financial systems .

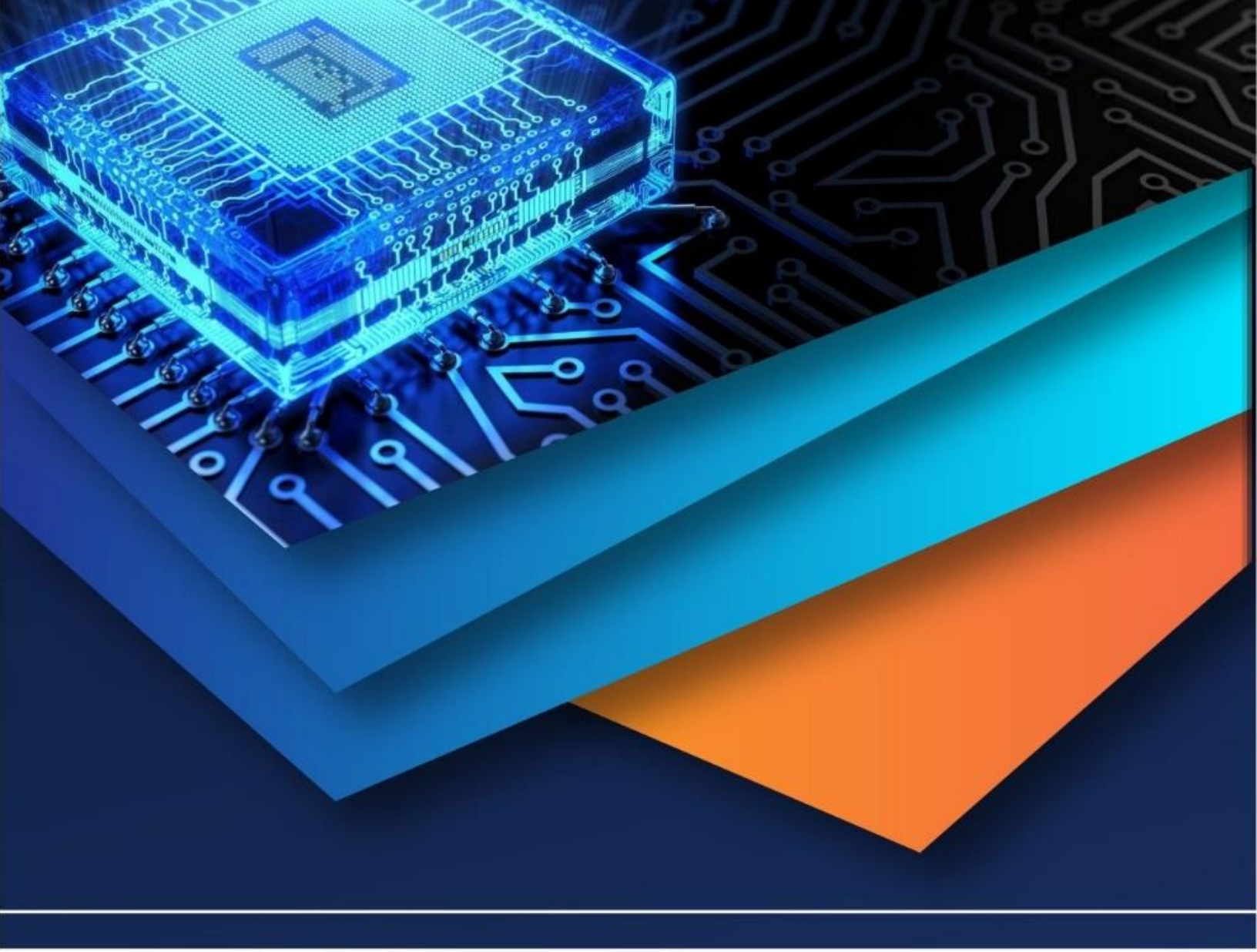
VI. CONCLUSION

The article explores the important function of authentication and fraud detection in the FinTech and wireless payments industries. It points out research results showing different types of fraud and weaknesses in current authentication methods, underlining the pressing necessity for improved security measures. The latest technology like data analytics, machine learning, biometrics, and blockchain are seen as crucial resources in managing financial risks and enhancing security. The article highlights the importance of balancing user ease and strict security measures, promoting adherence to regulations while also encouraging creativity. Moreover, it foresees progress in security solutions with the help of artificial intelligence and neural networks.

Taking proactive steps is crucial for maintaining financial integrity and building trust in the industry by investing in secure solutions to safeguard customer data and uphold the reliability of financial service providers. In general, the article highlights how crucial it is to constantly adjust and come up with new ideas in order to navigate the changing world of financial technology, guaranteeing the safety and reliability of online transactions.

REFERENCES

[1] Team, "Banking Fraud Prevention," Itexus, Aug. 18, 2023. https://itexus.com/banking-fraud-prevention-best-practices-success-stories/#gref (accessed Nov. 21, 2023).
[2] Zumstein,D.;Kotowski,W.SuccessFactorsofE-Commerce-DriversoftheConversionRateandBasketValue.InProceedingsofthe 18th International Conference e-Society, Sofia, Bulgaria, 2–4 April 2020; pp. 43–50.
[3] S. Salim, R. Hayden, and R. Wavra, "Using advanced analytics for fraud management | McKinsey," www.mckinsey.com,Sep.26,2018. https://www.mckinsey.com/industries/financial- services/our-insights/combating-payments-fraud-and-enhancing-customer-experience(accessed Nov28,2023).
[4] Aljabri,M.;Alhaidari,F.;Mohammad,R.M.A.;Mirza,S.;Alhamed,D.H.;Altamimi,H.S.;Chrouf,S.M.B. An Assessment of Lexical, Network, and Content-Based Features for Detecting Malicious URLs Using Machine Learning and Deep Learning Models.Comput. Intell. Neurosci. **2022**, 2022, 3241216. [CrossRef] [PubMed]
[5] N. Ratha and J. Connell, "Enhancing Security and Privacy in Biometrics-Based Authentication Systems," Research Gate, Jan.2001. https://www.researchgate.net/publication/220353130_Enhancing_Security_and_Privacy_in_Biometrics-Based_Authentication_Systems
[6] Bala,M.;Verma,D.Acriticalreviewofdigitalmarketing. Int.J.Manag.ITEng.**2018**,8,321–339.
[7] J. McNamee, "Digital bank customers are willing to adopt modern authentication methods for safety's sake," Insider Intelligence, Jun. 03, 2022. https://www.insiderintelligence.com/content/security-data-privacy-digital-consumers-authentication- technologies (accessed Dec. 10, 2023).
[8] A. Hayes, "Blockchain Facts: What Is It, How It Works, and How It Can Be Used," Investopedia, Apr. 23, 2023. https://www.investopedia.com/terms/b/blockchain.asp
[9] Berrar,D.Randomforestsforthedetectionofclickfraudinonlinemobileadvertising. InProceedingsofthe1stInternational Workshop on Fraud Detection in Mobile Advertising (FDMA), Singapore, 4 November 2012; pp.1–10.Available online: http://berrar.com/resources/Berrar_FDMA2012.pdf(accessed on 17 August 2022).
[10] S. Brown, "Machine learning, explained," MIT Sloan, Apr. 21, 2021. https://mitsloan.mit.edu/ideas-made-to- matter/machine-learning-explained



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY