ISSN: 2755-0214

Journal of Economics & Management Research

SCIENTIFIC Research and Community

Review Article

Open Access

Customer Authentication in Mobile Banking-MLOps Practices and AI-Driven Biometric Authentication Systems

Sumanth Tatineni

Devops Engineer, Idexcel Inc

ABSTRACT

The intersection of customer demands, security, and innovative services in the diverse mobile banking space calls for continuous adaptation by financial institutions. Small challenges such as on-demand customization and scalability are addressed through merging technologies, which is important for smaller institutions undergoing IT modernization. Despite the slow pace of ML adoption in banking, those leveraging ML experience increased their success in this competitive landscape. This article looks at the role of MLOps in overcoming challenges posed by evolving data volumes and complexities in deploying and developing ML models within financial institutions. As online banking authentication holds an important role in securing financial transactions, a historical overview of authentication methods, from biometrics to tokens, creates a chance to delve into the transformative potential of AI-driven biometric authentication. With the increase in mobile banking fraud, the need to safeguard sensitive customer data is met with radical technology. The article examines the varied authentication methods employed in online banking applications and depicts the potential of biometrics, majorly behavioral biometrics, to improve security and user experience. The rise of online mobile banking systems introduces both convenience and security concerns, thus prompting a closer look at the adoption of biometrics to mitigate fraud risks and improve the seamless authentication process throughout the user session. Customers increasingly demand quick and easy mobile payments, so biometrics has become a key fraud prevention and detection solution. By running in the background and eliminating setup authentication and risk-based authentication, behavioral biometrics significantly reduces fraud, thus addressing the limitations of traditional authentication methods like email verification and passwords. The article navigates the evolving mobile banking security space, highlighting the important role of MLOps and the potential of AI-driven biometric authentication in meeting the dual objectives of improving customer experience and strengthening severity protocols.

***Corresponding authors**

Sumanth Tatineni, Devops Engineer, Idexcel Inc.

Received: December 05, 2022; **Accepted:** December 12, 2022; **Published:** December 19, 2022

Keywords: Online banking, Customer Data Protection, Machine learning Operations (MLOps), Security Protocols, User Experience, Online Banking Authentication

Introduction

The ongoing COVID-19 pandemic has reshaped the global space and accelerated the digital transformation era for banks, thus bringing online and mobile banking to the forefront. As the pandemic prompts limitations on assisted services globally, financial institutions actively advocate for mobile banking registration to meet customers' common banking needs. A 2020 mobile banking survey by J.D. Power depicted a notable surge, with 37% of retail banking customers using mobile banking more frequently than ever [1].

Nonetheless, this digital shift has brought about challenges, mainly regarding security. The increased reliance on mobile banking applications has attracted an increase in security threats. Kaspersky's 2020 Q2 statistics on I.T. threat evolution reported over 1.2 million malicious mobile installers, with nearly 39,000 linked to mobile banking Trojans. This depicts the urgency for stronger security measures to safeguard sensitive information and ensure a secure banking environment [2]. To respond to these challenges, financial institutions recognize the role of secure authentication systems with biometrics leading in digital banking security platforms.

Traditional knowledge-based authentication methods like PINS, one-time passwords, and passwords can be forgotten, stolen, or compromised. Microsoft affirmed that 44 million exposed user accounts were a s result of weak passwords, and Google's findings on password reuse vulnerabilities highlight the need for a stronger authentication approach. Biometric verification, given reliable authentication through features such as fingerprint recognition and facial scans, is important in the financial industry security [3]. Biometrics plays a huge role in securing online banking, boosting customer trust, and enhancing the overall brand reputation of banking institutions.

In this era where technological advancement is rapid, data has become important for organizational success. Leveraging computational techniques such as ML, the banking sector is due to experience improved end-user services, personalized customer experiences, and enhanced fraud prevention [4]. This article looks into the intersection of mobile banking, biometric authentication, and the potential of ML, thus exploring how these technologies collectively contribute to a seamless, secure, and customer-centric financial space.

Significance and Background of Customer Authentication in Mobile Banking

The urgency for a secure and seamless authentication system has been amplified by the increased digital transformation

brought about by the pandemic. The pandemic has catalyzed the adoption of online and mobile banking. Recognizing this shift, financial institutions turn to biometrics for a more user-friendly and secure authentication solution. In addition, with technological advancements, the role of ML in the banking sector has become more pronounced. Banks cater to a diverse clientele, from individuals to large corporations, thus leveraging machine learning to process huge volumes of data quickly, which surpasses human-rule-based systems.

ML's impact has increased, with one leading European bank using ML models fueled by huge datasets and cloud computing to prevent fraud proactively [5]. The dynamic consumer behaviors and needs challenge banks relying on outdated model outputs. This article delves into the role of MLOps as a solution to empowering banks to deploy real-time models that adapt to this changing dynamic, thus offering helpful insights, especially as digital-only banks rise – which ensures relevance in retail banking through personalized experiences and services [6].

While MLOps adoption in the banking industry remains low and often overlooked until scale challenges arise, it presents a chance for first movers to gain a strategic advantage. Adopting MLOps empowers banks to meet evolving needs and regulations, thus future-proofing their businesses and positioning themselves as financial institutions offering top-tier experiences for consumers. This is a proactive approach for mobile banking security to deal with authentication challenges, mainly biometric technology in safeguarding financial transactions [7].

Why Banks Need MLOps for Digital Transactions

The importance of MLOps regarding mobile banking is in the set for best practices that reliably and efficiently deploy ML models to production. With data volumes growing and constant model updates in mobile banking operations being unnecessary to ensure relevance, MLOps is an important framework. The challenges posed by the surge of data science are clear, mainly in larger organizations with multiple divisions using various data management tools.

MLOps, similar to DevOps, applied its techniques and tools to machine learning, thus addressing challenges like inert model management, slow application deployments, and inefficient processes within the banking sector. Similar to the impact of DevOps on IT teams, MLOps can revolutionize how ML models deploy and operate [8]. By automating pipeline development and governance processes and integrating advanced data management tools, MLOps facilitates a smooth, automated sequence for structuring, deploying, and managing ML models in banking with continuous feedback loops at each stage.

Additionally, cross-team collaboration is important in MLOps, thus involving multidisciplinary teams like ML engineers, data scientists, financial analysts, and I.T. operations. This collaborative approach removes silos within organizations, thus promoting scale, efficiency, and long-term business value in the increasingly evolving mobile banking security landscape. Moreover, as financial institutions utilize large volumes of historical data to train ML algorithms for predicting outcomes and uncovering patterns, the management of new data scaling and velocity of ML algorithms becomes more complex.

Stale models trained on outdated data bring about the risk of inaccurate predictions. MLOps comes in as a solution specifically designed to address these challenges, thus enabling ML at scale and ensuring the continuous accuracy and relevance of predictive models in mobile banking [9]. Technically, MLOps is a systematic approach for financial institutions that offers lifecycle management solutions for machine learning models. As AI plays an important role in banking projects, MLOps provides the needed structure to navigate challenges and effectively streamline the management and deployment of machine learning models [10].

- **MLOps Practices for Banking:** MLOps transforms the traditional technique to machine learning operations, ensuring an efficient and continuous process that adapts to the evolving financial services scope, thus providing a scalable and secure foundation for AI-driven advancements in banking. MLOps improve patching speed, upgrades, updates, and code quality [11]. Extending DevOps principles to MLOps becomes important to manage the dynamic nature of data and machine learning model updates, thus aligning seamlessly with the business processes relevant to the financial sector [12]. MLOps revolves around four major tenets that collectively promote the foundational need for CI/CD for machine learning.
- **Model Deployment:** This incorporates a well-defined and, at times, automated process for designing, developing, and releasing models to production. Looking at SDLC processes, this practice highlights repeatable steps, thus allowing scalable, measurable, and repeatable deployment by data scientists.
- **Model Monitoring:** This is a post-deployment tenet and thus is important in monitoring ring model performance and accuracy. It is necessary to detect when a model becomes stale and promptly identify suboptimal results due to new real-world data like shifts in consumer behavior like those seen during the COVID-19 pandemic [13].
- **Model Training and Retraining:** This tenet addresses the variability in model accuracy over time or when predefined intervals elapse. The need to retrain models using updated datasets is important for optimizing models to target outcomes, as heightened by the need for prompt updates during the COVID-19 pandemic-induced changes in consumer behavior [14].
- **Automation:** This principle stands for delivering machine learning at scale. Automation is important in mobile banking security, especially as reliance on ML increases, depicting the unsustainable manual efforts required for development, delivery, monitoring, and retraining [15]. Automation allows data scientists to focus on improving models and enhancing insights, performance, and user experiences, similar to the role of DevOps pipelines in business applications.
- **Customer Segmentation and Personalization:** Despite substantial AI investments, banks still need help translating predictive insights from their ML models into strong customer personalization programs and campaign strategies. Common challenges include narrow ML model slopes, inconsistent customer data, and reliance on on-off use cases, limited knowledge sharing, and difficulty replicating models. Banks should enhance their capability to develop a comprehensive suite of ML models to excel in personalized engagement at every stage [16]. Currently, most models focus on isolated moments with short-term, product-centric goals, such as boosting mortgage applications, instead of identifying the drivers of customer lifetime value. MLOps ensures that the models adhere to best practices in data analysis, feature selection, and model training, thus promoting an all-around approach to personalization.

Benefits of MLOps in Banking

- **Seamless Automation:** ML empowers banks to smoothly automate the integration of AI/ML models into applications across all digital channels and points where customers interact. This ensures an enhanced overall customer experience [17]. In addition, MLOps helps automate application versioning and drift, thus ensuring replicable and consistent results at scale.
- **Reduced Costs:** MLOps reduces costs significantly, especially those related to AI/ML integration in self-managed environments. This is attained by strong traceability, version control, implementation of CI/CD pipelines, and continuous code checks.
- **Effortless Scaling:** MLOps empowers financial institutions and banks to establish highly flexible and agile application deployment infrastructures. This allows data team steams to concentrate on critical tasks with minimal I.T. involvement, thus ensuring easy scaling as demands evolve [18].
- **Effective Governance:** With facilitated code sharing and enabling the reproducibility of application codes with traceable version control across various data modeling scopes, MLOps ensures effective governance. Through rules-based automation in productionizing models, MLOps promotes automated deployments, thus streamlining AI/ML model governance.
- **Scalability:** While MLOps is mostly overlooked in industries such as banking, scalability becomes a challenge, and its relevance grows as banks prioritize efficiently in critical customer points. As the banking industry increasingly leans towards AI/ML and edge technologies for optimal customer experiences, MLOPs become important for managing, monitoring, and optimizing ML lifecycles.

AI-Driven Biometric Authentication in Banking

As the fintech industry transforms quickly, heightened security measures and improved customer experiences have become necessary. Banks increasingly turn to biometric technology as the main solution to these needs. Biometric authentication, characterized by its reliance on unique behavioral or physical characteristics, becomes a secure form of identity verification. The difficulty in falsifying or replicating biometric characteristics contributes to its reputation as a resilient authentication method [19].

Nonetheless, it is important to understand the need for robust protection of biometric data, as compromise could have major consequences, unlike passwords or other replaceable authentication methods. Biometric authentication removes traditional reliance on cards, keys, or passwords. Instead, it leverages distinctive attributes such as voice patterns to validate one's identity. Implementing biometric security in mobile banking involves collecting unique biometric data incorporating 3 primary categories [20].

- Morphological biometrics – attributes associated with the body's physical structure such as eye, face shape, or fingerprint scanned using specialized software.
- Biological biometrics – attributes of molecular or genetic levels such as blood, DNA, or other elements obtained from bodily fluids.
- Behavioral biometrics – Attributes based on unique behavioral patterns like speaking or walking.

The operation of biometric technology within banking follows a standardized process such as

- Data collection is where hardware scanners with custom software capture biometric data based on the selected security type, ranging from tiny scanners integrated into mobile phones to standalone professional devices.
- The connected software processes the collected biometric data, thus converting it into digital format. The system then matches this digital representation against an existing database [21]. The collected biometric data is encrypted and converted into a coded language graph, safeguarded from unauthorized access.
- If the data samples coincide, access to the system gets granted. If not, the user is denied access, or a system operator is alerted. This smooth process replaces traditional identification methods like passwords.

- **Biometric Security Indicators**
- **Voice recognition:** This option depends on vocal cord length and throat shape; voice recognition applies AI and machine learning to measure speech modulation, accent, tones, and frequencies with a reference template called voice print, created to identify individuals during subsequent interactions.
- **Facial Recognition:** Algorithms capture the appearance of facial features such as mouth, nose, or eyes by generating a face template through convolutional neural networks (CNN) technology. This method is widely used in biometric security for banking due to its affordability and convenience since it can be implanted using standard cameras or smartphones.
- **Fingerprint:** Recognition systems can digitize and scan the orientation of ridges in human fingerprints, thus creating biometric templates stored in datasets for quick search or comparison. Modern apps often utilize scanners for contactless reading, thus offering increased accuracy compared to traditional ink and paper methods.
- **Signature Recognition:** Available offline in static or dynamic (online) forms, signature recognition captures the graphic image of a handwritten signature for comparison with a saved copy. The online processing includes real-time evaluation of time, pressure, rhythm, and other aspects using a screen-sensitive device.
- **Elements of biometric security for banking**
- For effective implementation of comprehensive biometric security in digital banking, it is important to incorporate key aspects that enhance reliability in biometric identification. Incorporating these features, digital banking systems can strengthen their biometric security measures, align with regulatory needs, and offer a strong and trustworthy environment for users engaging in online financial transactions.
- **Multi-Factor Authentication:** The registration process should go beyond biometric scanning alone. In addition, more verification steps like date of birth confirmation and password verification or phone number verification should be included to strengthen security and reduce vulnerability.
- **Transaction Data Signing:** This feature plays a huge role in verifying transaction credentials by generating one-time confirmation codes, essential for high-risk transactions, large monetary transfers, or online personal detail changes.
- **Mobile Security Precautions:** Including essential measures such as advanced anti-debug, anti-hooking, and detection of root attempts is important given the widespread usage of neobanks on mobile devices; thus, defending against potential threats is important.
- **API for Quick Deployment:** Including an API is important for curating a custom biometric security system for banks to supply to third-party organizations [22]. This facilitates smooth implementation, thus allowing banks to deploy biometric scanning quickly.
- **Compliance with Regulatory Standards:** Ensuring

adherence to regulatory standards is important for fintech institutions. Verify the A.I. biometric system and ensure it complies with regulatory frameworks and standards relevant to the banking industry

- **User Experience and Interactions:** It is important to understand the preferences and behavior of the target users by analyzing the types of devices they use for online banking and ensure that the chosen A.I. biometric solution aligns with user habits, thus offering a user-friendly and seamless experience [23].
- **Data Privacy and Storage:** It is necessary to evaluate how the system manages and stores biometric data by considering whether on-premise or cloud-based storage is more suitable, considering privacy concerns and compliance with data protection regulations.
- **Reliability and Accuracy:** Assessing the accuracy and reliability of the biometric system in authenticating users is important by looking for systems that have high precision in recognizing unique biometric features while minimizing false negatives and positives.
- **Integration and Scalability:** It is important to consider the system's scalability to accommodate the growth of online banking users by ensuring that the solution integrates with existing banking infrastructure and can seamlessly adapt to future technological advancement [24].
- **Cost Effectiveness:** Evaluate the overall cost of implementing and maintaining the A.I. biometrics security system by considering the initial costs, ongoing upgrades, fees, and potential customization needs [25], thus ensuring alignment with budget constraints.

Challenges of MLOps and AI-Driven Customer Authentication in Banking

• Privacy Concerns Related to Mobile Banking Biometric Authentication

While biometric authentication in mobile banking offers increased security, it requires addressing privacy concerns about collecting and storing sensitive biometric data. Despite the advanced security provided by biometrics, it is important to recognize potential vulnerabilities [26]. For example, attackers can exploit biometric scanning tools by creating 3D models from publicly available photos or using deep fake technology. The storage of confidential user data generated by biometric systems further highlights the need for additional security measures like leveraging secure cloud computing for banking operations. For instance, the 2015 incident where fingerprints of 5.6 million U.S. government employees were compromised emphasizes the importance of integrating biometric technologies with complementary forms of authentication [27]. To curb risk related to data breaches, financial institutions need to implement strong privacy policies, employ encryption methods, and consider hybrid authentication methods.

• Potential Biases in AI Algorithms for Biometric Authentication

Integrating AI algorithms in biometric authentication systems introduces the need to explore and address possible biases. Understanding the impact of biases within these algorithms is important for ensuring accuracy and fairness in authentication processes. Biases can come from the data used to train A.I. models, leading to disparate impacts on specific demographic groups [28]. Financial institutions should proactively deploy representative and diverse datasets while developing AI algorithms to handle bias issues. Regular assessments and audits of these algorithms are important for rectifying and identifying biases, thus promoting equitable authentication practices [29].

• Challenges of Seamless Integration into Mobile Banking Applications

Integrating biometric authentication into existing mobile banking applications seamlessly poses challenges requiring extra consideration. While biometrics enhance security, the integration process must prioritize user experience. It is important to ensure a stable balance between user convenience and security to avoid compromising the overall usability of mobile banking applications [30]. Banks should invest in user-friendly interfaces, conduct thorough testing, and obtain customer feedback to refine the integration of biometric authentication, thus ensuring that biometrics become an efficient and natural part of the mobile banking experience, strengthening both user satisfaction and security.

Conclusion

The rapid shift towards digital transformation in digital banking, especially amidst challenges brought about by the COVID-19 pandemic, has depicted the important need for strong security measures, mainly in mobile banking. The increased mobile banking usage has brought opportunities and challenges to the financial industry. The adoption of mobile banking brings the need for advanced authentication methods like biometrics in strengthening security frameworks. With the increased security threats, it is clear that traditional knowledge-based authentication methods are no longer enough. Biometric verification leverages unique behavioral or physical attributes, thus presenting a more user-friendly and secure alternative [31].

Nonetheless, integrating biometrics into the digital banking space has its challenges. The potential biases in A.I. algorithms, security concerns, and seamless inclusion of biometric authentication into existing applications are among the considerations that banks should navigate. Additionally, the advent of MLOps brings forth efficiency, scalability, and governance in managing the life cycle of machine learning models, mainly in mobile banking security. The role of MLOps in curbing security challenges, facilitating continuous training, enhancing code quality, and deploying models is important.

As the financial industry embraces technological advancements, biometric authentication and MLOps fusion become an important strategy to navigate the complexities of modern digital banking. With these considerations, financial institutions must carefully navigate the choices in AI-driven biometric security systems implementation; the selection should be influenced by understanding secure data storage practices, user interactions, and compliance with relevant regulations [32]. As the banking sector continues to grow, integrating MLOps and biometrics is a promising technique in strengthening the security foundations of mobile banking to ensure that the dynamic customer's needs are met and that security and resilience in the digital banking landscape.

References

1. Hammood WA, Abdullah R, Hammood OA, Asmara SM, Al-Sharafi MA, et al. (2020) A review of user authentication model for online banking system based on mobile IMEI number. In IOP Conference Series: Materials Science and Engineering 769: 012061.
2. Usman O, Monoarfa T, Marsofiyati M (2020) E-Banking and mobile banking effects on customer satisfaction. Accounting 6: 1117-1128.
3. Ali G, Ally Dida M, Elikana Sam A (2020) Two-factor authentication scheme for mobile money: A review of threat

models and countermeasures. Future Internet 12: 160.
4. Karamitsos I, Albarhami S, Apostolopoulos C (2020) Applying DevOps practices of continuous automation for machine learning. Information 11: 363.
5. Wang C, Wang Y, Chen Y, Liu H, Liu J (2020) User authentication on mobile devices: Approaches, threats and trends. Computer Networks 170: 107118.
6. Kumar A N (2023) Devops For Machine Learning: Accelerating Model Development And Deployment. https://techbullion.com/devops-for-machine-learning-accelerating-model-development-and-deployment/.
7. Tamburri D A (2020) Sustainable MLOps: Trends and challenges. In 2020 22nd international symposium on symbolic and numeric algorithms for scientific computing (SYNASC) 17-23. IEEE.
8. Treveil M, Omont N, Stenac C, Lefevre K, Phan D, et al. (2020) Introducing MLOps. O'Reilly Media 186. https://www.ebooks.com/en-in/book/210177483/introducing-mlops/mark-treveil/.
9. Wu H, Sun Y, Wolter K (2018) Energy-efficient decision making for mobile cloud offloading. IEEE Transactions on Cloud Computing 8: 570-584.
10. Zhou Y, Yu Y, Ding B (2020) Towards mlops: A case study of ml pipeline platform. In 2020 International conference on artificial intelligence and computer engineering (ICAICE) 494-500. IEEE.
11. Raj E (2020) Edge MLOps framework for AIoT applications. https://www.theseus.fi/bitstream/handle/10024/342167/Raj_Emmanuel.pdf?sequence=2&isAllowed=y.
12. van den Heuvel WJ, Tamburri DA (2020) Model-driven ML-Ops for intelligent enterprise applications: vision, approaches and challenges. Proceedings Springer International Publishing 10: 169-181.
13. Vadavalasa RM (2020) End to end CI/CD pipeline for Machine Learning. International Journal of Advance Research, Ideas and Innovation in Technology 6: 906-913.
14. Chen A, Chow A, Davidson A, DCunha A, Ghodsi A, et al. (2020) Developments in mlflow: A system to accelerate the machine learning lifecycle. In Proceedings of the fourth international workshop on data management for end-to-end machine learning 1-4.
15. Suhel SF, Shukla VK, Vyas S, Mishra VP (2020) Conversation to automation in banking through chatbot using artificial machine intelligence language. In 2020 8th international conference on reliability, infocom technologies and optimization (trends and future directions)(ICRITO) 611-618.
16. Vijai C, Suriyalakshmi SM, Elayaraja M (2020) The future of robotic process automation (RPA) in the banking sector for better customer experience. Shanlax International Journal of Commerce 8: 61-65.
17. Ng M, Coopamootoo KP, Toreini E, Aitken M, Elliot K, et al. (2020) Simulating the effects of social presence on trust, privacy concerns & usage intentions in automated bots for finance. In 2020 IEEE European symposium on security and privacy workshops (EuroS&PW) IEEE 190-199.
18. Kathuria R, Wadehra A, Kathuria V (2020) Human-centered artificial intelligence: antecedents of trust for the usage of voice biometrics for driving contactless interactions. Proceedings, Part I 22 Springer International Publishing 325-334.
19. Wewege L, Lee J, Thomsett M C (2020) Disruptions and digital banking trends. Journal of Applied Finance and Banking 10: 15-56.
20. Bakunova T V, Trofimova E A, Lapteva E V (2019) Biometrics as a method of information security in the banking sector digitalization. In International Scientific and Practical Conference on Digital Economy (ISCDE 2019) Atlantis Press 929-934.
21. Guennouni S, Mansouri A, Ahaitouf A (2019) Biometric systems and their applications. In Visual impairment and blindness-what we know and what we have to know. IntechOpen. https://www.intechopen.com/chapters/65920.
22. Chigada JM (2020) A qualitative analysis of the feasibility of deploying biometric authentication systems to augment security protocols of bank card transactions. South African Journal of Information Management 22: 1-9.
23. Gayathri M, Malathy C, Prabhakaran M (2020) A review on various biometric techniques, its features, methods, security issues and application areas. Computational Vision and Bio-Inspired Computing: ICCVBIC 2019 931-941.
24. Obaidat MS, Traore I, Woungang I (2019) Biometric-based physical and cybersecurity systems Cham: Springer International Publishing 1-10.
25. Merhi M, Hone K, Tarhini A (2019) A cross-cultural study of the intention to use mobile banking between Lebanese and British consumers: Extending UTAUT2 with security, privacy and trust. Technology in Society 59: 101151.
26. Maček N, Adamović S, Milosavljević M, Jovanović M, Gnjatović M, et al. (2019). Mobile banking authentication based on cryptographically secured iris biometrics. Acta Polytechnica Hungarica 16: 45-62.
27. Kochhar K, Purohit H, Chutani R (2019) The rise of artificial intelligence in banking sector. In The 5th International Conference on Educational Research and Practice (ICERP) 127.
28. Mehrotra A (2019) Artificial intelligence in financial services–need to blend automation with human touch. In 2019 International Conference on Automation, Computational and Technology Management (ICACTM) IEEE 342-347.
29. Ris K, Stankovic Z, Avramovic Z (2020) Implications of implementation of Artificial Intelligence in the banking business with correlation to the human factor. Journal of Computer and Communications 8: 130-144.
30. Boobier T (2020) AI and the Future of Banking. John Wiley & Sons. DOI: 10.1002/9781119596165
31. Soni VD (2019) Role of artificial intelligence in combating cyber threats in banking. International Engineering Journal for Research & Development 4: 7-7.
32. Isaac RA, Chaturvedi P, Gareja P, Grover R (2018) Secured E-Banking System using Artificial Intelligence. International Journal of Emerging Technologies in Engineering Research (IJETER) 6. https://www.ijeter.everscience.org/Manuscripts/Volume-6/Issue-10/Vol-6-issue-10-M-05.pdf.