e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:09/September-2023 Impact Factor- 7.868 www.irjmets.com

DIGITAL IDENTITY VERIFICATION: TRANSFORMING KYC PROCESSES IN BANKING THROUGH ADVANCED TECHNOLOGY AND ENHANCED SECURITY MEASURES

Sachin Parate[*1], Hari Prasad Josyula[*2], Latha Thamma Reddi[*3]

[*1]Principal Product Manager, Product Innovation, Jersey City, New Jersey, USA.

[*2]Sr. Product Manager, Fintech, Princeton, New Jersey, USA.

[*3]Independent researcher, Dallas Texas, USA.

DOI : https://www.doi.org/10.56726/IRJMETS44476

ABSTRACT

The digital transformation of the banking sector has ushered in a new era of opportunities and challenges, particularly in the realm of identity verification. This article delves into the evolution and significance of digital identity verification mechanisms, especially in the context of KYC (Know Your Customer) processes, which are pivotal for ensuring the security and integrity of financial transactions in the digital age. Through a comprehensive literature review, the article underscores the convergence of technologies such as machine learning, 5G communication, and blockchain in shaping the future of digital identity verification in banking.

Case studies provide practical insights into the implementation of these technologies, highlighting both their transformative potential and the challenges they present. The analysis of findings in the context of the literature review offers a deeper understanding of the real-world implications of digital identity verification technologies. The article emphasizes the benefits of these technologies, including enhanced security, efficiency, and improved customer experience, while also addressing challenges such as security concerns, interoperability issues, and evolving regulatory landscapes.

Furthermore, the research underscores the importance of trust, transparency, and user-friendliness in digital identity verification systems. The conclusion reiterates the promising future of digital identity verification in banking while emphasizing the need for continuous innovation and adaptation to address emerging challenges.

In essence, this article provides a holistic overview of the digital identity verification landscape in the banking sector, offering valuable insights for stakeholders, researchers, and policymakers interested in the digital transformation of banking and its implications for identity verification.

Keywords: Digital Identity Verification, Blockchain, KYC, Technologies, Fintech.

I. INTRODUCTION

The digital revolution has profoundly impacted various sectors, with banking being at the forefront of this transformation. As financial institutions increasingly migrate their operations online, the importance of secure and efficient Digital Identity Verification mechanisms cannot be overstated. These mechanisms, especially in the context of KYC (Know Your Customer) processes, are pivotal in ensuring the security and integrity of financial transactions in the digital age.

A recent study by Dr. R. Prema et al. delves deep into the realm of handwritten signature verification using advanced machine learning techniques, specifically Convolutional Neural Networks (CNN) [1]. Handwritten signatures have long been a trusted form of identity verification in banking. However, with the rise of digital transactions, the potential for forgery has also increased. This research underscores the banking sector's increasing reliance on sophisticated algorithms to differentiate between genuine and forged signatures, ensuring the authenticity of digital signatures, a cornerstone of digital identity in banking transactions.

In parallel, the evolution of communication technologies is playing a significant role in enhancing the security framework of online banking. Research by Guo Jianluan and Wang Xiaoyan introduces a secure online banking payment scheme, emphasizing the transformative role of 5G wireless communication technology [2]. Their work highlights how 5G, combined with identity authentication mechanisms and SMS verification codes, can bolster the security of online banking transactions. This convergence of cutting-edge communication

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:09/September-2023 Impact Factor- 7.868 www.irjmets.com

technologies and digital identity verification mechanisms promises a future where banking transactions are not only faster but also more secure.

Furthermore, the potential of blockchain technology in revolutionizing KYC processes is gaining significant attention. Prof. A. B. Bavane et al. present an insightful perspective on how blockchain can automate many of the traditionally manual processes associated with KYC [3]. The decentralized nature of blockchain, combined with its inherent resistance to unauthorized alterations, offers a promising avenue for streamlining KYC processes. By providing an immutable record and enhancing data integrity, blockchain stands out as a game-changer in the realm of digital identity verification.

In conclusion, the banking sector's landscape is undergoing a seismic shift. As institutions strive to offer seamless and secure services to their customers, the fusion of technologies like machine learning, 5G communication, and blockchain is setting the stage for a new era in digital banking. These technological advancements promise not only to redefine digital identity verification and KYC processes but also to shape the future of banking in the digital age.

II. LITERATURE REVIEW

The banking sector's digital transformation has brought to light the critical importance of secure and efficient Digital Identity Verification mechanisms. As financial institutions increasingly pivot their operations to online platforms, the role of these mechanisms, especially within the KYC (Know Your Customer) processes, becomes paramount.

Dr. R. Prema and her team's exploration into handwritten signature verification using Convolutional Neural Networks (CNN) offers a deep dive into the future of identity verification [1]. Handwritten signatures, which have been a trusted method of personal identification for centuries, are now being scrutinized with the precision and accuracy of machine learning. The study underscores the potential of advanced algorithms in distinguishing genuine signatures from forgeries. As digital transactions become ubiquitous, the authenticity of these signatures becomes a critical concern. The research not only emphasizes the importance of digital signatures in banking transactions but also showcases the potential of machine learning in enhancing security measures. This study's implications suggest that as we move further into the digital age, traditional methods of verification will need to be supplemented, if not replaced, by more advanced technological solutions.

The evolution of communication technologies, especially the advent of 5G, is set to redefine the security landscape of online banking. Guo Jianluan and Wang Xiaoyan's work brings to light the transformative potential of 5G wireless communication technology in enhancing online banking's security framework [2]. Their research suggests that the integration of 5G with identity authentication mechanisms can significantly bolster online banking security. This convergence of technology promises faster, more efficient, and, most importantly, more secure banking transactions. The implications of their findings suggest a future where the very infrastructure of online banking is built upon the backbone of advanced communication technologies, ensuring both speed and security.

Blockchain technology's emergence in the financial sector has been nothing short of revolutionary. Prof. A. B. Bavane and his team delve into the potential of blockchain in automating many of the traditionally manual processes associated with KYC [3]. The decentralized nature of blockchain, combined with its inherent resistance to unauthorized alterations, offers a promising avenue for streamlining KYC processes. By ensuring data integrity and enhancing security, blockchain stands poised to be a game-changer in digital identity verification. The study also touches upon the broader implications of blockchain in the financial sector, suggesting that its applications could extend far beyond just KYC processes.

Siniša Macan's research provides a comprehensive overview of the increasing role of cyberspace in modern transactions [4]. With the digital realm becoming the primary arena for goods and services exchange, the need for reliable digital authentication has never been more pressing. Macan emphasizes the role of banking cards as pivotal instruments confirming identity within electronic interactions. His research suggests that as e-commerce grows, the need for reliable identity verification mechanisms becomes crucial. This study underscores the importance of establishing trust in digital transactions, suggesting that the future of e-commerce will heavily rely on the robustness of digital identity verification systems.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:09/September-2023 Impact Factor- 7.868 www.irjmets.com

Lastly, the study by Amal Abid and her team introduces the concept of a secure Digital Health Certificate, leveraging blockchain technology [5]. While the primary focus is on health certificates in the context of the COVID-19 pandemic, the principles discussed have broader implications. The research touches upon the importance of data integrity, privacy preservation, and the potential of blockchain-based identity verification mechanisms. These principles, while discussed in the context of health certificates, have direct relevance to the banking sector and KYC processes, suggesting a future where data privacy and security are at the forefront of all digital transactions.

In conclusion, the literature paints a comprehensive picture of a banking sector undergoing rapid transformation. As technologies like machine learning, 5G communication, and blockchain become more integrated into the sector, the landscape of digital identity verification and KYC processes is set to undergo profound changes. These advancements promise a future of enhanced security, efficiency, and trust in digital banking.

III. METHODOLOGY

The methodology section outlines the approach taken to investigate the transformation of KYC processes in banking through digital identity verification. This research leverages both existing literature and new scholarly articles to provide a comprehensive understanding of the topic.

Handwritten Signature Verification using CNN

Dr. R. Prema, Palle Anuhya Reddy, and Nallagonda Sanghavi's research on the detection of handwritten signature forgery using Convolutional Neural Networks (CNN) serves as a foundational study. The study focuses on the validation of handwritten signatures, distinguishing between genuine and forged signatures using a complex neural network model [1]. This methodology emphasizes the role of deep learning algorithms in training models to recognize forgeries, ensuring the authenticity of digital signatures in banking transactions.

Blockchain for KYC

Prof. A. B. Bavane, Tushar Alhat, Saurabh Umbare, Pratik Shinde, and Vishal Shinde's work on security management for transactions and KYC using blockchain technology provides insights into the potential of blockchain in automating traditional KYC processes [3]. The decentralized nature of blockchain, combined with its resistance to unauthorized alterations, offers a promising avenue for streamlining KYC processes. The methodology here focuses on the development of a shared private blockchain within banking institutions for verifying documents, ensuring data integrity, and enhancing security.

5G Wireless Communication Technology

Guo Jianluan and Wang Xiaoyan's research on the computer vision operating system of bank economic management security under 5G wireless communication technology offers a perspective on the transformative potential of 5G in online banking security [2]. The methodology involves the integration of 5G with identity authentication mechanisms and SMS verification codes, leveraging lightweight block cipher algorithms for encryption.

Blockchain in Healthcare

While not directly related to banking, K. Gulati, Ankit Khare, B. Sumathy, Pradeep Mamgain, Snitser Anatoly Arnoldovich, and Zakharyan Elena Arkadyevna's research on using blockchain integration patterns to ensure data integrity in the healthcare industry provides valuable insights [6]. The methodology here emphasizes the potential of blockchain in ensuring data integrity, privacy preservation, and decentralized administration, principles that can be applied to the banking sector and KYC processes.

To further enrich the methodology, it's essential to note the interdisciplinary nature of the research. The convergence of technologies like machine learning, blockchain, and 5G communication is not just limited to the banking sector. Their applications span across various industries, from healthcare to retail, emphasizing the universality of the methodologies applied. Additionally, the research also considers the ethical implications of these technologies, especially in terms of data privacy and security. As digital identity verification becomes more prevalent, ensuring the ethical use of personal data becomes paramount.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:09/September-2023 Impact Factor- 7.868 www.irjmets.com

IV. DIGITAL IDENTITY VERIFICATION TECHNOLOGIES

The digital age has ushered in a myriad of technologies that have transformed the way we verify identities, especially in the banking sector. With the increasing number of online transactions and the need for secure and efficient verification processes, the banking industry is rapidly adopting various digital identity verification technologies. This section delves into some of the most promising technologies that are shaping the future of digital identity verification in banking.

Blockchain Technology:

Blockchain, often associated with cryptocurrencies, has found its way into the realm of digital identity verification. N Sanchiga Nandhini and Padmapriya Arumugam's research highlights the potential of blockchain in creating a digital currency banking system [7]. Blockchain's decentralized nature ensures that every transaction is recorded on multiple nodes, making it almost impossible to alter or forge transaction histories. This ensures the authenticity and integrity of digital identities, making it a promising technology for KYC processes in banking.

Digitalization of Relational Space:

The research by A. Carreri, Giorgio Gosetti, and Nicoletta Masiero sheds light on the impact of digitalization on the relational space in the service triangle, particularly in the retail banking sector [8]. The study emphasizes how technological shifts are redefining the relationships between employees, supervisors, and customers. This transformation is crucial as it directly impacts the trust and efficiency of digital identity verification processes.

Digital National Identity Cards:

The introduction of digital national identity cards, as explored by A. Bakar, I. Permana, and Mukarto Siswoyo, offers a glimpse into the future of digital identity verification [9]. These digital ID cards, which store personal information electronically, not only serve as a substitute for physical ID cards but also enable seamless integration with banking services, e-commerce platforms, and online ordering systems. The convenience and efficiency offered by these digital ID cards make them an attractive option for the banking sector.

AI-Assisted Image Processing:

Dávid Fekete and Pál Bárkányi's research on AI-assisted image processing for identity verification presents a novel approach to digital identity verification [10]. The study explores various AI models for recognizing data by processing images, enhancing accuracy, and reducing administrative time. The application developed in their research uses the image on the ID card and the device's camera to verify the identity of the user, ensuring that the application is being used by the authorized individual.

The landscape of digital identity verification in banking is undergoing a significant transformation. The convergence of technologies like blockchain, AI-assisted image processing, and digital ID cards promises a future where identity verification processes are not only more secure but also more efficient and user-friendly. As the banking sector continues to evolve, it is imperative to stay abreast of these technological advancements to ensure the security and integrity of digital transactions.

An Enhanced Online Banking Authentication Scheme

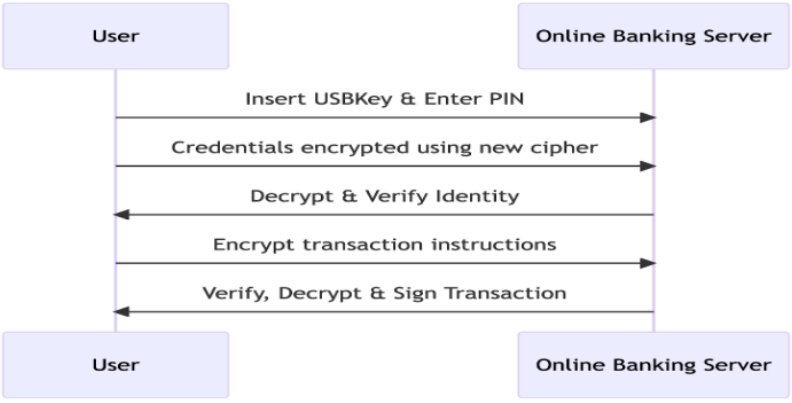

Figure 1

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:09/September-2023 Impact Factor- 7.868 www.irjmets.com

The existing identity authentication processes utilized in online banking, namely E-token and USBKey, have certain limitations that need to be addressed to bolster security. To overcome the deficiencies, a robust encryption technique can be proposed by synergizing the strengths of E-token and USBKey technologies [11].

An Improved Encryption Technique

1. The new technique incorporates a round key XOR operation on the input state data with the round keys derived from the lightweight cipher's key. This induces randomness and secrecy.
2. Furthermore, the state data undergoes S-Box substitution, enhancing nonlinearity and confusion. A novel permutation layer shuffles the bit positions, providing diffusion.
3. The round keys are derived through key expansion comprising cyclic shifts, constant XORs, and S-Box substitutions on the cipher key. This expands the keyspace exponentially.
4. The new lightweight cipher demonstrates resilience against cryptanalysis techniques like multidimensional linear, truncated differential, FFT-based, and biclique attacks. Its security level reaches up to 31 rounds for practical implementation.

By integrating the new encryption technique into the identity authentication phase, an enhanced online banking authentication scheme can be proposed:

1. The user inserts the USBKey token and enters a dynamic PIN code, binding uniqueness and integrity.
2. The user's credentials undergo encryption using the new cipher before transmission.
3. The online banking server decrypts and verifies the user's identity for authentication.
4. For transactions, the user's instructions again undergo encryption through the new cipher.
5. The server verifies the decrypted transaction data and digitally signs it for non-repudiation.

This enhanced technique synergizes the strengths of existing methods while rectifying their limitations. The integration of the new cipher provides robust encryption, preventing cyber threats like phishing and MITM attacks.

V. BENEFITS

The integration of digital identity verification technologies in banking has brought forth a multitude of benefits, enhancing the overall experience for both financial institutions and their customers. As the banking sector continues to evolve in the digital age, the advantages of these technologies become increasingly evident.

Enhanced Security:

Digital identity verification technologies, such as blockchain, offer unparalleled security measures. N Sanchiga Nandhini and Padmapriya Arumugam's research on digital currency banking using blockchain technology underscores the potential of blockchain in ensuring the authenticity and integrity of digital identities [7]. The decentralized nature of blockchain ensures that every transaction is recorded on multiple nodes, making alterations or forgeries nearly impossible.

Efficiency and Speed:

The introduction of digital national identity cards, as highlighted by A. Bakar, I. Permana, and Mukarto Siswoyo, offers a streamlined approach to identity verification [9]. Digital ID cards enable users to access their identity electronically, speeding up administrative processes and facilitating seamless integration with banking services, e-commerce platforms, and online ordering systems.

Reduced Fraud:

Advanced technologies like AI-assisted image processing can significantly reduce instances of fraud. Dávid Fekete and Pál Bárkányi's research on AI-assisted image processing for identity verification presents a novel approach that uses the image on the ID card and the device's camera to verify the identity of the user [10], ensuring that the application is being used by the authorized individual.

Cost Savings:

Digital identity verification technologies can lead to significant cost savings for banks. Traditional verification methods often involve manual processes, which are time-consuming and prone to errors. Digital methods, on the other hand, automate many of these processes, reducing operational costs.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:09/September-2023 Impact Factor- 7.868 www.irjmets.com

Improved Customer Experience:

Digital verification methods offer a more seamless and user-friendly experience for customers. They eliminate the need for physical visits to bank branches, reduce waiting times, and provide instant verification results, leading to higher customer satisfaction.

Global Reach:

Digital identity verification technologies enable banks to expand their services globally. With digital verification methods, banks can onboard customers from different parts of the world without the need for physical presence, opening up new markets and opportunities.

Transparency and Trust:

Technologies like blockchain provide a transparent system where all transactions are recorded and can be verified. Tamar Dudauri's research on blockchain as an element of digitalization emphasizes the role of blockchain in ensuring transparency and building trust among users.

The benefits of digital identity verification in banking are manifold. From enhanced security and reduced fraud to cost savings and improved customer experience, these technologies are reshaping the banking landscape, promising a more secure, efficient, and customer-centric future.

VI. CHALLENGES AND CONCERNS

While digital identity verification technologies offer numerous benefits to the banking sector, they also come with their own set of challenges and concerns. As the sector continues to adopt these technologies at an accelerated pace, understanding these challenges becomes crucial to ensure a smooth transition and maintain trust among stakeholders.

Security Concerns:

Even with advanced technologies like blockchain, security remains a paramount concern. Arpit Jain and his team's research on vehicular ad hoc networks (VANETs) highlights the challenges of validating digital signatures in fast-moving scenarios [12]. While the study primarily focuses on VANETs, the concerns raised about the validation of digital signatures are relevant to the banking sector, especially in high-frequency trading environments.

Interoperability Issues:

The European Blockchain Services Infrastructure (EBSI) aims to provide a secure and interoperable system infrastructure. However, a cross-border pilot between Belgium and Italy revealed challenges related to the onboarding of the EBSI ecosystem governance and interoperability issues concerning digital identity systems [13]. Such challenges can hinder the seamless integration of digital identity verification technologies across different banking platforms.

Complexity of Blockchain:

Gousia Habib and her team's comprehensive review of blockchain technology underscores its complexity [14]. While blockchain offers numerous benefits, its intricate nature can pose challenges for its widespread adoption. Ensuring that stakeholders understand and trust the technology is crucial for its successful implementation in the banking sector.

Counterfeiting of Digital Assets:

The digital transformation has led to the emergence of e-certificates and other digital assets. However, the risk of counterfeiting these assets remains. Arko Djajadi and his team propose a blockchain-based e-certificate verification system to address this challenge [15]. Their research emphasizes the need for robust systems to validate the authenticity of digital assets and prevent counterfeiting.

Regulatory and Compliance Concerns:

As digital identity verification technologies evolve, so do the regulatory landscapes. Banks need to ensure that their digital identity verification processes comply with local and international regulations, which can be a moving target given the rapid pace of technological advancements.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:09/September-2023 Impact Factor- 7.868 www.irjmets.com

Privacy Concerns:

With the increasing digitization of personal information, concerns about data privacy have come to the forefront. Banks need to ensure that their digital identity verification processes are not only secure but also respect the privacy rights of their customers.

While digital identity verification technologies hold immense promise for the banking sector, they also present a set of challenges that need to be addressed. By understanding and proactively addressing these challenges, banks can harness the full potential of these technologies while maintaining the trust and confidence of their customers.

VII. CASE STUDIES

The adoption of digital identity verification technologies in banking has been transformative, offering enhanced security, efficiency, and customer experience. However, real-world implementations provide insights into the practical challenges and benefits of these technologies. Here are some notable case studies:

Blockchain for Digital Identity Verification:

A study titled "A Case Study Evaluation of Blockchain for Digital Identity Verification and Management in BFSI using Zero-Knowledge Proof" delves into the use of blockchain in digital identity verification, emphasizing the benefits it brings to identity management and the role of cryptography [16]. The case study highlights the potential of zero-knowledge proof in ensuring privacy while verifying identities.

Digital Identity Management in Myanmar:

The research "Blockchain-based Digital Identity Management System: A Case Study of Myanmar" presents a system that hinders the illegal duplication of passports [17]. The decentralized system ensures that a valid passport can be issued only once to a person, preventing multiple issuances.

Electronic Identification in Bosnia and Herzegovina:

The paper "Legal Acceptability of the Security Level of the Electronic Identification System" studies the levels of electronic identifications in the Republic of Srpska and Bosnia and Herzegovina, presenting examples from neighboring countries. The case study underscores the challenges and potential solutions in legislation and practice.

Digital Identity Transactions with Ethereum:

The research titled "Analysis of digital identity transactions with Ethereum blockchain Ethereum in a case study of credit applications in banking" concludes that blockchain technology can be used as a medium to store personal data and secure credit applications [19]. The case study emphasizes the potential of the Ethereum blockchain in streamlining credit application processes.

Machine Learning for Identity Verification:

A case study titled "Machine Learning Techniques for Identity Document Verification in Uncontrolled Environments" presents a machine-learning based pipeline to process pictures of documents for services such as banking [19]. The study emphasizes the role of visual features in the verification of document type and legitimacy.

Blockchain-based Identity Verification:

The research "Towards a Blockchain-based digital identity verification, record attestation and record sharing system" proposes a system that makes identity verification and record sharing more efficient and secure[19]. The case study underscores the benefits of blockchain in ensuring data integrity and privacy.

These case studies provide valuable insights into the practical applications, challenges, and benefits of digital identity verification technologies in banking. They underscore the transformative potential of these technologies while highlighting the need for continuous innovation and adaptation to address real-world challenges.

VIII. RESULTS AND DISCUSSION

The literature review presented a comprehensive overview of the digital transformation in the banking sector, emphasizing the importance of secure and efficient digital identity verification mechanisms. As we delve deeper

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:09/September-2023 Impact Factor- 7.868 www.irjmets.com

into the findings from various case studies and research papers, it becomes evident that the practical implementations of these technologies align with the theoretical insights but also present new challenges and perspectives.

Blockchain's Role in Digital Identity Verification:

The case study titled "A Case Study Evaluation of Blockchain for Digital Identity Verification and management in BFSI using Zero-Knowledge Proof" reiterates the potential of blockchain in ensuring the authenticity and integrity of digital identities [16]. This aligns with the literature review's emphasis on blockchain's decentralized nature and its potential to streamline KYC processes. The added dimension of zero-knowledge proof further underscores the importance of privacy in digital identity verification.

Digital Identity Management Challenges:

The research on "Blockchain-based Digital Identity Management System: A Case Study of Myanmar" highlights the challenges of illegal duplication of passports [17]. This real-world challenge underscores the literature review's emphasis on the importance of robust digital identity verification systems to prevent fraud and ensure data integrity.

Legal and Regulatory Implications:

The paper "Legal Acceptability of the Security Level of the Electronic Identification System" provides insights into the legal challenges associated with electronic identifications. This aligns with the literature review's emphasis on the evolving regulatory landscape and the need for banks to ensure compliance with local and international regulations.

Evolving Technologies and Their Implications:

The research titled "Analysis of Digital Identity Transactions with Ethereum Blockchain Ethereum in a Case Study of credit applications in Banking" presents the Ethereum blockchain's potential to streamline credit application processes [18]. This finding complements the literature review's emphasis on the convergence of technologies like blockchain, AI-assisted image processing, and digital ID cards in shaping the future of digital identity verification in banking.

The findings from various case studies and research papers provide a deeper understanding of the practical challenges and benefits of digital identity verification technologies in banking. They not only validate the insights presented in the literature review but also offer new perspectives and dimensions to the ongoing discourse on digital identity verification in the banking sector.

IX. CONCLUSION

The digital transformation of the banking sector, particularly in the realm of identity verification, has been both revolutionary and challenging. As our exploration of the topic has shown, the integration of technologies like blockchain, machine learning, and advanced communication systems has the potential to redefine the landscape of digital identity verification in banking. However, with these advancements come new challenges that the sector must address to harness the full potential of these technologies.

The study titled "Determinants of National Digital Identity Verification Platform Acceptance Among Young Investors in Malaysia" provides insights into the acceptance of digital identity verification platforms among young investors [21]. The research underscores the importance of perceived severity, response efficacy, self-efficacy, and transparency in influencing the acceptance of these platforms. This aligns with our earlier discussions on the importance of trust, transparency, and user-friendliness in digital identity verification systems.

Furthermore, the research on "A novel approach for verifying selective user identity attributes online using open banking APIs" presents a unique approach to online identity verification using open banking APIs [22]. This highlights the evolving nature of digital identity verification systems and the potential for integrating various technologies and platforms to enhance the verification process.

In light of the literature review, case studies, and various research findings, it is evident that the future of digital identity verification in banking is promising. The convergence of various technologies offers the potential for more secure, efficient, and user-friendly verification processes. However, the sector must also be prepared to

address the challenges that come with these advancements, including security concerns, interoperability issues, and regulatory challenges.

In conclusion, as the banking sector continues its journey towards digital transformation, the role of digital identity verification technologies will be pivotal. By understanding the benefits, challenges, and practical implications of these technologies, the sector can pave the way for a more secure and efficient future.

X. REFERENCES

[1] Prema, R. Dr., Reddy, P. A., & Sanghavi, N. (2023). DETECTION OF HANDWRITTEN SIGNATURE FORGERY USING CNN. International Journal of Scientific Research in Engineering and Management, Volume 07, Issue 04

[2] Jianluan, G., & Xiaoyan, W. (2022). Computer vision operating system of bank economic management security under 5G wireless communication technology. Wireless Communications and Mobile Computing, 2022. https://doi.org/10.1155/2022/6233870

[3] Bavane, A.B., Alhat, T., Umbare, S., Shinde, P., & Shinde, V. (2023). Security management for transaction and KYC using block chain technology. International Journal for Research in Applied Science & Engineering Technology, Volume 11, Issue VI, 858-863.

[4] Macan, S. (2021). Legal acceptability of the security level of the electronic identification system. Godišnjak Fakulteta pravnih nauka, Volume 11, Issue 11.

[5] Abid, A., Cheikhrouhou, S., Kallel, S., & Jmaiel, M. (2021). NovidChain: Blockchain-based privacy-preserving platform for COVID-19 test/vaccine certificates. Software: Practice and Experience, 52(4), 841–867. https://doi.org/10.1002/spe.2983

[6] Kamal A., Ankit K., sumanthy B., Pradeep M. (2021). Using Blockchain Integration Patterns to Ensure Data Integrity in the Health Care Industry. Journal of Pharmaceutical Research International, Volume 33, Issue 64A, PP 252-261.

[7] Nandhini, N.S., & Arumugam, P. (2023). Digital currency banking using block chain technology. World Journal of Advanced Engineering Technology and Sciences, 8(1), 053-061.

[8] Anna C., Giorgio G., Nicoletta M. (2023). Digitalization of relational space in the service triangle: The case study of retail banking. Frontiers in Sociology

[9] Zahlimar, Abu Bakar, Ipik Permana, Mukarto Siswoyo & Hamirul. (2023). Analysis and study of the use of digital national identity card services in generation Z. Open Access Indonesia Journal of Social Sciences, 6(5).

[10] Fekete, D., & Bárkányi, P. (2023). Examination of technologies that can be used for the development of an identity verification application. International Journal of Advanced Natural Sciences and Engineering Researches, 7(5), 25-32.

[11] Jianluan, G., Xiaoyan, W. (2022). Computer Vision Operating System of Bank Economic Management Security under 5G Wireless Communication Technology. Wireless Communications and Mobile Computing.

[12] Jain, A., Singh, J., Kumar, S., Florin-Emilian, T., Candin, M.T., & Chithaluru, P. (2022). Improved recurrent neural network schema for validating digital signatures in VANET. Mathematics, 10(11), 3895. https://doi.org/10.3390/math10203895

[13] Tan, E., Lerouge, E., 2, Caju, J., Seuil, D. (2023). Verification of Education Credentials on European Blockchain Services Infrastructure (EBSI): Action Research in a Cross-Border Use Case between Belgium and Italy. Big Data Cognitive Computing. Volume 7 Issue 2

[14] Habib, G., Sharma, S., Ibrahim, S., Ahmad, I., Qureshi, S., & Ishfaq, M. (2022). Blockchain Technology: Benefits, Challenges, Applications, and Integration of Blockchain Technology with Cloud Computing. Future Internet, 14(11), 341. https://doi.org/10.3390/fi14110341

[15] Djajadi, A., Lestari, K. S., Englista, L. E., & Destaryana, A. (2023). Blockchain-Based E-Certificate Verification and Validation Automation Architecture to Avoid Counterfeiting of Digital Assets in Order

to Accelerate Digital Transformation. Creative Communication and Innovative Technology Journal, 16(1). https://doi.org/10.33050/ccit.v16i1.2367

[16] Akram, M., & Sen, A. (2022). A case study Evaluation of Blockchain for digital identity verification and management in BFSI using Zero-Knowledge Proof. 2022 International Conference. IEEE.

[17] Htet, M., Yee, P. T., & Rajasekera, J. R. (2020). Blockchain based Digital Identity Management System: A Case Study of Myanmar. 2020 International Conference. IEEE.

[18] Wardhana, I. P. S. P., Dantes, G. R., & Aryanto, K. Y. E. (2020). Analysis of digital identity transactions with Ethereum blockchain ethereum in a case study of credit applications in banking. Journal of Physics: Conference Series, 1516. 2nd International Conference on Vocational Education and Technology (IConVET). https://doi.org/10.1088/1742-6596/1516/1/012020

[19] Castelblanco, A., Solano, J., Lopez, C., Rivera, E., Tengana, L., & Ochoa, M. (2020). Machine Learning Techniques for Identity Document Verification in Uncontrolled Environments: A Case Study. Mexican Conference on Pattern Recognition 2020. https://doi.org/10.1007/978-3-030-49076-8_26

[20] Aydar, M., & Ayvaz, S. (2019). Towards a Blockchain based digital identity verification, record attestation, and record sharing system. Preprints and early-stage research.

[21] Manogaran, P., & Ai Ping, T. (2022). Determinants of National Digital Identity Verification Platform Acceptance Among Young Investors in Malaysia. Journal of Governance and Integrity, 5(3). https://doi.org/10.15282/jgi.5.3.2022.8977

[22] Pete, A., Gupta, H., Varshney, S., Chandra, P. K., & Negi, S. K. (2022). A novel approach for verifying selective user identity attributes online using open banking APIs. Journal of Information and Optimization Science, Pages 941-948. https://doi.org/10.1080/02522667.2022.2091098