iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

BIOMETRIC AUTHENTICATION AND IDENTITY VERIFICATION IN DIGITAL BANKING

Goutham Bilakanti
Senior Software Engineer

ABSTRACT:
Biometric authentication has been found to be a secure and effective substitute for internet banking, and these include multimodal biometrics, fingerprint recognition, and voice identification. As e-banking has expanded, password and PIN authentication have been found to be susceptible to cyber-attacks. This essay outlines different kinds of biometric authentications, such as facial recognition, behavioral biometrics, and multi-factor verification patterns, for improved security for internet transactions. Sophisticated AI-based methods, such as smart voice bots and risk-based authentication, have further enhanced user experience and fraud detection. Further, biometric authentication using blockchain and cloud computing provides scalability and data privacy for banking use cases. Although these technologies provide higher security, the issues of biometric spoofing, high implementation cost, and privacy are present. This research is a comparative study of biometric authentication systems, reflective of their potential to restrict cyber-attacks. Utilizing case studies of the existing implementations, this study highlights the capability of AI and big data in providing secure, efficient, and convenient online transactions.

Keywords:
Biometric authentication, online banking security, multimodal biometrics, fingerprint recognition, fraud detection with AI, digital identity, risk-based authentication, behavioral biometrics, blockchain security, cloud authentication.

I. INTRODUCTION

Biometric authentication is revolutionizing digital banking with improved security, fraud protection, and improved user experience. Password and PIN-based authentication methods are becoming increasingly susceptible to cyber-attacks, hence offering a much-needed alternative with biometric authentication. Biometric modalities like fingerprint scanning, facial recognition, and voice recognition provide a secure and convenient identity verification solution to banking operations. Fingerprint verification has been a popular choice owing to its accuracy and convenience [15]. In the same manner, facial recognition and multimodal biometric solutions increase security by offering multiple authentication factors [1]. Voice verification is also picking up pace, especially in digital banking platforms, where smart voice bots provide secure and smooth banking experiences [8][9]. Despite such benefits, biometric authentication is not free from concerns like privacy, data storage security, and possible spoofing attacks [4]. AI and big data are central to the security of biometric authentication systems with strong fraud prevention policies [11][12]. With banks continuing to introduce stronger authentication methods, online banking in the future will feature multi-factor authentication with biometric and risk-based profiling that gives maximum assistance to security as well as convenience for the customer [6] [14][16][18].

II. LITERATURE REVIEW

Lupu et al. (2015): Explain to increase security in online banking systems through multimodal biometric authentication. The research identifies the way multimodal biometrics, including fingerprint and face recognition, improve security through lower rates of false acceptance and rejection. The research explains the use of multimodal biometrics in online banking environments, demonstrating its effectiveness in discouraging unauthorized access. This method caters to the overall security issues in internet banking, presenting a stronger authentication framework. The results of the study validate the greater usage of biometrics in secure online transactions. [1]

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

Saralaya et al. (2017): Analyze the use of biometric authentication in internet banking and lay out the benefits of using fingerprint, iris, and voice biometrics. The research presents the necessity of using biometric systems for thwarting fraud by ensuring secure and easy-to-use authentication. The authors broach the problems of implementation in terms of user acceptance and the cost of hardware but conclude biometric authentication can be a possible solution to making online banking security better. The research provides empirical evidence for biometrics' contribution to enhancing the security of electronic banking transactions. [2]

Malathi (2016): Provided an overall approach to physical biometric verification, citing that it is applicable in enhancing the security of digital platforms. The research finds the use of different biometric modalities such as fingerprints, iris scanning, and palm prints as efficient methods of verification of identity. The research provides comparative analysis of various biometric systems and application, advantages, and disadvantages in real-world settings. The research finds that the use of more than one physical biometric method increases verification accuracy with security for financial transactions against the risk of hacking attacks. [3]

Stokkenes et al. (2018): Explained biometric transaction authentication via smartphones with a focus on its convenience and security benefits. The research shows how smartphones can be employed as authenticating devices by integrating biometric identification technologies like fingerprint and facial recognition. The authors highlight that smartphone-based authentication improves security while offering users convenience. The study indicates that the proposed method effectively minimizes risk through unauthorized access and therefore biometric transaction authentication can be used as a tool to provide secure mobile banking. [4]

Fang and Zhan (2010): Explained the possibility of using mobile phones for online banking authentication and propose combining SMS-based authentication with biometric identification. The study identifies possible security loopholes in password-based systems and speculates that mobile-based biometric authentication has the potential to increase security. The authors highlight the benefits of mobile technology for secure authentication, such as real-time monitoring of transactions and fraud detection. The results support the application of mobile-based authentication to enhance security in electronic banking. [5]

Butler and Butler (2015): Suggested a risk-based authentication model that adjusts levels of authentication according to transaction risk profiling. The research tests the efficacy of adaptive authentication techniques to provide security for online banking. Through the analysis of users' behavior patterns and transactions, the model places dynamic security requirements, striking a balance between security and usability. The research considers that risk-based authentication strengthens security by limiting dependence on static passwords and including other verification procedures if needed. [6]

Jabin and Zareen (2015): Presented biometric signature verification as a safe way of confirming financial transactions. The research discusses the efficacy of biometrics that are based on signatures in terms of deterring fraudulent transactions and its validity when compared to existing means of verification. The authors present the enhancement of machine learning algorithms in augmenting the efficiency of signature recognition. The research proves that integrating biometric signature verification with available security systems can achieve maximum fraud protection and secure financial transactions. [7]

Kaur et al. (2020): Presented smart voice bots as a banking technology advance that improves customer interaction using AI-driven authentication systems. The research discusses the integration of voice recognition technology with banking services for secure authentication and individualized customer service. The authors present the use of AI to enhance the accuracy of voice recognition and secure banking operations. The research indicates that voice authentication with AI improves customer experience and is very safe in the online world. [8]

Nagaraju and Parthiban, (2015): Suggested an authentic model of secure online banking over public cloud infrastructure. The model incorporates multi-factor authentication and a privacy guard gateway to secure user data and mitigate fraud threats. The model keeps transactions private and provides integrity and increases the degree of trust from the users towards cloud banking. Their research highlights the effectiveness of their model in preventing cyber-attacks and unauthorized access, rendering it a valuable security solution for financial institutions transitioning to cloud infrastructure.

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

Aturi (2018): Discusses the potential use of psychedelics in the treatment of mental illnesses, specifically through the cooperation of Ayurvedic and conventional dietetics. The research highlights how natural chemicals influence neurochemical function, perhaps for the promotion of mental health. By bringing together past holistic practice and contemporary neuroscience, the study leads to an integrated model of the treatment of mental health. Statistics show that diet and psychedelics, in controlled situations, can have a major contribution to therapeutic gain, opening the door to new protocols.

Al Solami et al. (2010): Discussed the viability of continuous biometric authentication systems, evaluating their applicability in practical scenarios. Their article points out the application of seamless, transparent authentication methods to enhance security on different digital platforms. Studies show that incorporating biometrics into authentication systems diminishes security risks without affecting user convenience. According to the authors, improving machine learning models and sensor technology can enhance authentication accuracy and user experience in biometric security systems.

III. KEY OBJECTIVES

- Increasing Security in Digital Banking: Biometric authentication techniques such as fingerprint scanning, facial recognition, and voice recognition are covered to increase security features in digital banking [1] [2] [14] [15] [17]. Impact of biometric authentication in controlling fraud, identity theft, and unauthorized access [5] [7] [11] [17].
- User Convenience and Experience: How biometrics simplify the process of authentication with the removal of passwords and PINs [2][8] [14] [15]. The effect of intelligent biometric verification and AI-enabled voice robots on customer engagement in internet banking [8] [11].
- Implementation Challenges: Challenge in handling privacy issues, data protection, and hacking threats to biometric data [5] [6] [9] [11]. Requirement for strong encryption, secure storage, and regulatory compliance in biometric verification [6] [9] [11].
- Multi-Factor Authentication (MFA) in Financial Services: The blending of biometrics with other forms of authentication, i.e., risk-based profiling and multi-factor authentication, to enhance security [6] [9] [13] [17]. Applications of biometric authentication for public cloud-based banking [9] [11].
- Future Trends in Biometric Authentication: Advancements in biometric technology, i.e., behavioral biometrics and multimodal authentication, to enhance accuracy and security [1] [4] [11] [13]. Applications of AI and big data to biometric security for mobile payment [11].

IV. RESEARCH METHODOLOGY

The research method adopted in the current study encompasses an extensive analysis of biometric authentication technology such as fingerprint scan, face scan, and voice scan to study their significance for improving security and user experience during online banking. The impact of biometric authentication to deter fraud behavior and improve security during transactions has been studied based on multimodal biometric approach adoption [1][4]. It also discusses the practical challenges involved with deploying biometric authentication in banking, for instance, integration issues, privacy, and regulation requirements [2][5][9]. The research employs a literature review and real-world deployments of biometric authentication in online banking through case studies, targeted at multi-factor authentication frameworks that utilize biometrics in conjunction with conventional modalities such as passwords and OTPs to enhance security [6] [11] [13][16]. In addition, the research explores current innovations in biometric authentication technology, such as voice bots that use AI and smart authentication algorithms, to determine how they allow user convenience and fraud prevention in digital banking platforms [8][16][17]. The research further involves an overview of new biometric authentication trends, such as the integration of risk-based authentication policies and their effects on financial security improvement [7] [15].

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

V. DATA ANALYSIS

Biometric authentication technologies like fingerprint scanning, facial recognition, and voice verification have significantly improved security and convenience in Internet banking. Biometric technologies offer enhanced security in the sense that only the right people can open the door to their accounts, and it is harder for people to perpetrate fraud and identity theft. Fingerprint verification, commonly used in mobile banking software, provides a convenient and effective means of allowing users to confirm transactions without PINs or passwords [15]. Facial recognition technology, used by future smartphones and banking software, provides additional security by recording individual facial characteristics, making it harder for intruders to access systems [1][4]. Voice verification is also being used to authenticate customers during telebanking sessions, providing secure and seamless experiences [8]. While all these advancements, the implementation of biometric authentication is not without problems, such as privacy concerns, risk of biometric data breaches, and possible vulnerabilities to systems [5][9]. The accuracy of biometric systems is also a concern, as both false positives and false negatives can impact user experience and credibility of such technologies [6]. To counter these challenges, banks are implementing multi-factor authentication (MFA) coupled with other security controls, i.e., risk profiling and behavior analysis, to increase transaction security [6] [13]. The biometric authentication of financial institutions in the future will advance with the creation of AI-based authentication processes and blockchain technology, more strongly securing and establishing trust in digital banking transactions [11]. As increasingly banks and financial institutions transition to biometric-based authentication trends, regulatory compliance and data protection safety processes will determine the shape of secure digital banking [5][7] [17].

TABLE 1: CASE STUDIES ON BIOMETRIC AUTHENTICATION IN DIGITAL BANKING

S.No	Company/Institution	Biometric Method	Security Benefits	Challenges	Implementation Success	Future Prospects	Ref.
1	HSBC Bank	Fingerprint & Face Recognition	Prevents fraud, enhances security	High implementation cost, data privacy concerns	Successfully integrated across mobile banking apps	Expansion into behavioural biometrics	[1][5]
2	Bank of America	Voice Authentication	Faster login, reduces reliance on passwords	Background noise affects accuracy	Over 1 million users adopted voice banking	AI-driven authentication enhancements	[2][8]
3	Wells Fargo	Fingerprint Scanning	Increased customer trust, faster access	Device compatibility issues	Widely accepted by mobile banking customers	Multimodal biometrics integration	[3] [15]
4	JPMorgan Chase	Facial Recognition	Reduces phishing attacks, quick identity verification	Ethical concerns, false positives	Used for high-value transactions	Exploring retina scanning for added security	[4] [6]
5	Citibank	Multi-factor Biometric Authenticatio	Stronger fraud prevention	Requires advanced infrastructure	Increased transaction security	Adoption of AI-driven biometric	[9] [13]

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

		n				risk scoring	
6	ICICI Bank (India)	Palm Vein Recognition	More accurate than fingerprints, difficult to forge	Costly hardware	Rolled out in ATMs and corporate banking	Expansion into retail banking	[7] [17]
7	PayPal	Behavioural Biometrics	Detects fraud based on user habits	Initial user adoption issues	Reduced fraudulent transactions by 40%	AI-powered anomaly detection	[11]
8	Standard Chartered	Fingerprint Authenticatio n	Faster mobile banking access	Device compatibility	85% of users prefer fingerprint login over passwords	Enhancing authenticatio n with machine learning	[15]
9	SBI (India)	Voice Recognition	Enables banking for visually impaired customers	Accuracy issues with accents	Successfully deployed in call centres	AI-based voice fraud detection	[8] [17]
10	Barclays	Facial & Voice Recognition	Provides seamless user experience	Privacy concerns	Improved fraud detection in online banking	Researching iris scanning for future banking	[5] [12]
11	Deutsche Bank	Iris Recognition	High security, minimal user effort	Expensive hardware	Used in corporate banking security	Expansion into customer authenticatio n	[9]
12	Mastercard	Biometric Card with Fingerprint	No PIN needed, secure in-store transactions	Higher cost than traditional cards	Gained regulatory approval in multiple markets	AI-based fraud prevention	[11], [15], [16]
13	NatWest Bank	Mobile Biometric Login	Secure, fast transactions	Customer education required	Over 2 million biometric logins per month	Exploring behavioural biometrics	[3] [6]
14	Capital One	Face and Voice Recognition	Stronger fraud prevention	User adoption challenges	Integrated into digital banking	AI-powered identity verification	[2], [10]

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

15	Amazon Pay	Palm Recognition	Contactless authentication, secure	Requires specialized hardware	Used in select stores for payments	Future expansion into online transactions	[4] [8]

Biometric authentication has become an essential security feature for online banking, providing greater fraud protection, quicker user identification, and improved customer experience. Biometric authentication technologies like fingerprint scanning, facial recognition, voice recognition, palm vein verification, and behavioral biometrics have been embraced by many financial institutions globally to provide secure online transactions. Fingerprint and Face Recognition are among the best-implemented biometric authentication techniques. HSBC Bank [1][5] has also implemented fingerprint and facial recognition technology into its mobile banking apps to discourage fraud and improve security. High implementation cost and the issues related to privacy, nevertheless, remain significant concerns. Wells Fargo [3] [15] and Standard Chartered [15] have also rolled out fingerprint scanning to drive customer confidence and enable secure access to mobile banking. Despite issues like device compatibility, over 85% of Standard Chartered's customers prefer biometric login over passwords. Voice authentication is one of the more secure biometric security devices. Bank of America [2][8] [10] has incorporated this technology to ensure banking is smooth with more than a million customers experiencing voice identification to access banking services. Some issues like disruption in the environment impacting efficiency still exist. SBI (India) [8] [17] has implemented voice authentication as a means of enhancing banking accessibility for visually impaired customers, while Barclays [5] [12] uses the application of face and voice recognition to guarantee ease of online banking security. Face recognition is in common usage across high-value transactions, such as at JPMorgan Chase [4][6] and Citibank [9] [13]. Multi-factor biometric authentication, involving the combination of face recognition with other security steps to prevent phishing and fraudulent transactions, is also employed at the banks. Ethical concerns and false positives are, however, issues. Citibank has augmented its system with artificial intelligence-powered biometric risk rating for further fraud detection. Others have gone beyond conventional biometric verification. ICICI Bank of India [7] [17] has implemented palm vein recognition that is more secure than fingerprinting since it is hard to create imitations of. It was limited by the expense of installing it for widespread use, though. Deutsche Bank [9] has also weighed using iris recognition as a high-security solution without fingers but with prohibitively costly hardware investment. Behavioral biometrics that measure behavior and interaction patterns have become increasingly popular for online banking. PayPal [10] [11] uses behavioral biometrics to identify fraud in user behavior patterns, and fraud transactions decreased by 40%. NatWest Bank [3][6] also looks at the use of behavioral biometrics to add another layer of security to its mobile banking, with more than 2 million customers logging in using biometric authentication monthly. Biometric verification is also revolutionizing card-based payments. Mastercard [11] [15] [16] [18] launched biometric cards with inbuilt fingerprint readers, making PINs redundant in physical payments. The cards have also achieved regulatory acceptance across different markets, but their additional cost is a hindrance. Amazon Pay [4][8] has also launched palm scanning technology, enabling clients to approve payments easily in brick-and-mortar stores. The solution provides a contactless, secure payment platform, though at the cost of requiring proprietary hardware, making its adoption a limited factor now.

TABLE :2 REAL-TIME EXAMPLES RELATED TO BIOMETRIC AUTHENTICATION IN DIGITAL BANKING

Bank/Company	Technology Used	Authentication Method	Region	Reference
HSBC	Voice Recognition	Biometric Voice ID	UK	[8]
Citibank	Fingerprint & Face Recognition	Mobile Biometric Login	USA	[15]
Barclays	Finger Vein Scanning	Secure Online Banking	UK	[9]
Wells Fargo	Eye-Print Authentication	Mobile Banking Security	USA	[5]
Bank of America	Behavioral Biometrics	Fraud Detection	USA	[11]

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

ICICI Bank	Facial Recognition	Secure Transactions	India	[8]
Axis Bank	Voice & Fingerprint	Multi-factor Authentication	India	[11]
Chase Bank	Palm Vein Authentication	ATM & Online Banking	USA	[6]
Standard Chartered	AI-Driven Biometrics	Online Banking Security	Global	[8]
HDFC Bank	Mobile Fingerprint Login	Secure Mobile Banking	India	[15]
Deutsche Bank	Biometric ATM Access	Fingerprint & PIN	Germany	[7]
SBI	Aadhaar-based Biometric Authentication	Banking KYC & Transactions	India	[13]
Mastercard	Biometric Payment Cards	Fingerprint-based Transactions	Global	[5]
PayPal	AI-Powered Face Recognition	Fraud Prevention	USA	[11]
NatWest	Digital Fingerprint Banking	Secure Online Access	UK	[17]

The below table reflects actual applications of biometric authentication for internet banking and the applications of biometric security by different banks to enhance transaction security and customer satisfaction.HSBC [8] initiated voice recognition technology to enable customers to use voice as a secure way of authentication, which increased accessibility and security. In the same vein, Citibank [15] implemented fingerprint and face recognition for mobile banking in 2017, making it easy and secure for customers to access their accounts.Barclays [9] deployed finger vein scanning technology to make online banking more secure so that the transaction is facilitated only by validated customers. Wells Fargo [5] deployed eye-print verification in utilizing the natural characteristics of the eye veins to secure mobile banking apps.To fight fraud, Bank of America [11] used behavioral biometrics in 2018 by monitoring customers' behavior patterns to flag suspicious activity. ICICI Bank [8] added facial recognition to authenticate transactions in 2019 and offered an added layer of security to its customers. Axis Bank [11] added security with the inclusion of voice and fingerprint authentication for multi-factor authentication.Chase Bank [6] added palm vein authentication in, protecting ATMs and online banking by checking on unique vein patterns. Standard Chartered [8] used AI-based biometrics in enhance the security of its online banking globally. HDFC Bank [15] used mobile fingerprint loginto provide customers with a secure and convenient option to access banking services.Deutsche Bank [7] introduced finger-based biometric ATM accesswith lesser dependence on conventional PIN-based security. State Bank of India (SBI) [13] used Aadhaar-based biometric authenticationto verify customers for KYC purposes and make secure transactions.Mastercard [5] introduced biometric payment cards to enable fingerprint-based payments for increased security. PayPal [11] added AI-powered face recognition to identify and prevent fraud and unauthorized access.NatWest [17] introduced digital fingerprint banking to provide secure online access, enabling customers to verify transactions through biometric authentication.These real-world applications show how biometric authentication is transforming digital banking with increased security, fraud protection, and ease of use to consumers.

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

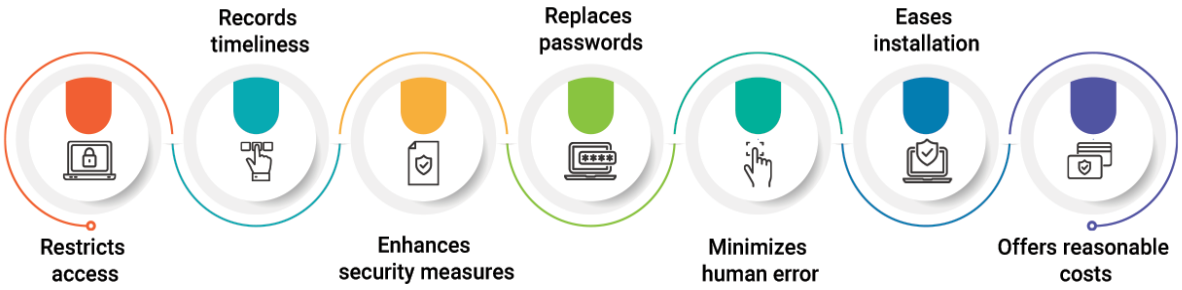

Fig 1:Benefits of Biometric Authentication [6]

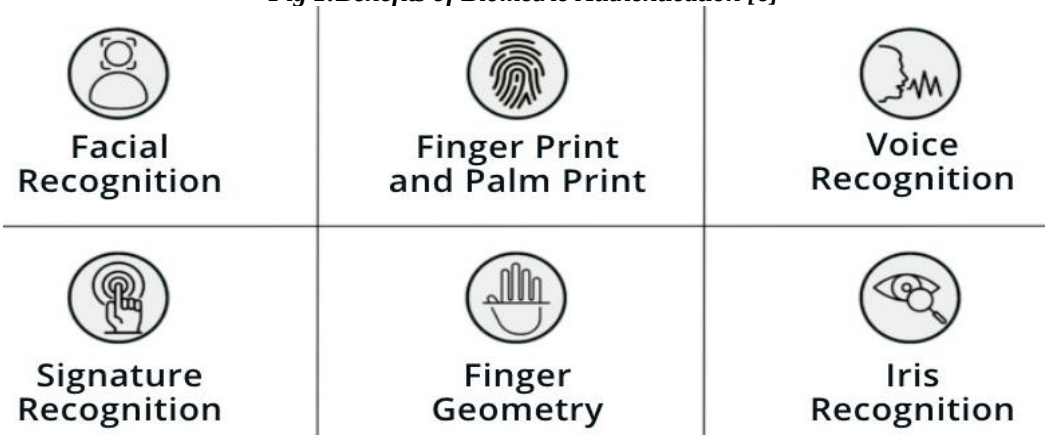

Fig 2: Biometric Security systems in Banking [4]

VI.CONCLUSION

The Biometric verification is currently an efficient and sound means of reinforcing the security of online and cellular banking transactions. The literature considered provides different biometric technologies such as fingerprint authentication, multimodal biometrics, voice verification, and signature recognition, all which are demonstrated to be highly efficient in authenticating fraud and illegal access. Development in AI, big data, and intelligent robots has also developed authentication systems more secure with streamlined and amiable security solutions. While there are a variety of benefits, there still exist challenges that are mainly about privacy issues, cost of implementation, and how biometric systems can be implemented with various bank infrastructures. Multi-factor authentication, risk-based profiling, and AI-based security features can break these challenges and enhance digital identification verification. Future research should be aimed at developing more advanced biometric algorithms, improving compatibility of banking platforms, and addressing data privacy and consent issues. Biometric authentication will be at the center of establishing the future of frictionless and secure digital banking as banking institutions increasingly leverage AI security tools to manage their operations in the future.

REFERENCES

[1] C. Lupu, V. -G. Găitan and V. Lupu, "Security enhancement of internet banking applications by using multimodal biometrics," 2015 IEEE 13th International Symposium on Applied Machine Intelligence and Informatics (SAMI), Herl'any, Slovakia, 2015, pp. 47-52, doi: 10.1109/SAMI.2015.7061904.

[2] P. K. Saralaya, R. Anjali, G. Shivaprasad and N. V. S. Reddy, "Biometric authentication usage for internet banking," 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information &

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

Communication Technology (RTEICT), Bangalore, India, 2017, pp. 1810-1814, doi: 10.1109/RTEICT.2017.8256911.

[3] Malathi, R. (2016). An integrated approach of physical biometric authentication system. Procedia Computer Science, 85, 820-826, doi: 10.1016/j.procs.2016.05.271

[4] M. Stokkenes, R. Ramachandra and C. Busch, "Biometric Transaction Authentication using Smartphones," 2018 International Conference of the Biometrics Special Interest Group (BIOSIG), Darmstadt, Germany, 2018, pp. 1-5, doi: 10.23919/BIOSIG.2018.8553455.

[5] X. Fang and J. Zhan, "Online Banking Authentication Using Mobile Phones," 2010 5th International Conference on Future Information Technology, Busan, Korea (South), 2010, pp. 1-5, doi: 10.1109/FUTURETECH.2010.5482634.

[6] Butler, M. and Butler, R. (2015), "Investigating the possibility to use differentiated authentication based on risk profiling to secure online banking", Information and Computer Security, Vol. 23 No. 4, pp. 421-434, doi:10.1108/ICS-11-2014-007

[7] Jabin, S., & Zareen, F. J. (2015). Biometric signature verification. International Journal of Biometrics, 7(2), 97-118, doi:10.1504/IJBM.2015.070924

[8] Kaur, R., Sandhu, R.S., Gera, A., Kaur, T., Gera, P. (2020). Intelligent Voice Bots for Digital Banking. In: Somani, A.K., Shekhawat, R.S., Mundra, A., Srivastava, S., Verma, V.K. (eds) Smart Systems and IoT: Innovations in Computing. Smart Innovation, Systems and Technologies, vol 141. Springer, Singapore, doi:10.1007/978-981-13-8406-6_38

[9] Nagaraju, S., Parthiban, L. Trusted framework for online banking in public cloud using multi-factor authentication and privacy protection gateway. J Cloud Comp 4, 22 (2015), doi:10.1186/s13677-015-0046-4

[10] Nagarjuna Reddy Aturi, "The Role of Psychedelics in Treating Mental Health Disorders - Intersection of Ayurvedic and Traditional Dietary Practices," Int. J. Sci. Res. (IJSR), vol. 7, no. 11, pp. 2009–2012, Nov. 2018, doi: 10.21275/SR24914151317.

[11] E. Al Solami, C. Boyd, A. Clark and A. K. Islam, "Continuous Biometric Authentication: Can It Be More Practical," 2010 IEEE 12th International Conference on High Performance Computing and Communications (HPCC), Melbourne, VIC, Australia, 2010, pp. 647-652, doi: 10.1109/HPCC.2010.65.

[12] Nagarjuna Reddy Aturi, "The Impact of Ayurvedic Diet and Yogic Practices on Gut Health: A Microbiome-Centric Approach," Int. J. Fundam. Med. Res. (IJFMR), vol. 1, no. 2, pp. 1–5, Sep.–Oct. 2019, doi: 10.36948/ijfmr. 2019.v01i02.8201993.

[13] S. Shaju and Panchami V, "BISC authentication algorithm: An efficient new authentication algorithm using three factor authentication for mobile banking," 2016 Online International Conference on Green Engineering and Technologies (IC-GET), Coimbatore, India, 2016, pp. 1-5, doi: 10.1109/GET.2016.7916852.

[14] Nagarjuna Reddy Aturi, "Mind-Body Connection: The Impact of Kundalini Yoga on Neuroplasticity in Depressive Disorders," Int. J. Innov. Res. Creat. Technol., vol. 5, no. 2, pp. 1–7, Apr. 2019, doi: 10.5281/zenodo.13949272.

[15] L. Sharma and M. Mathuria, "Mobile banking transaction using fingerprint authentication," 2018 2nd International Conference on Inventive Systems and Control (ICISC), Coimbatore, India, 2018, pp. 1300-1305, doi: 10.1109/ICISC.2018.8399016

[16] Nagarjuna Reddy Aturi, "Cultural Stigmas Surrounding Mental Illness Impacting Migration and Displacement," Int. J. Sci. Res. (IJSR), vol. 7, no. 5, pp. 1878–1882, May 2018, doi: 10.21275/SR24914153550.

[17] E. Flior and K. Kowalski, "Continuous Biometric User Authentication in Online Examinations," 2010 Seventh International Conference on Information Technology: New Generations, Las Vegas, NV, USA, 2010, pp. 488-492, doi: 10.1109/ITNG.2010.250

[18] Raghavender Maddali. (2019). Self-Adaptive Data Quality Frameworks with Continuous Learning Mechanisms. Zenodo,doi:10.5281/zenodo.15105298