International Journal of Aquatic Science
ISSN: 2008-8019
Vol 15, Issue 01, 2024

Emerging Cyber Security Threats in Digital Banking: A Comprehensive Analysis and Preventive Strategies

Dr. Raju BPG[1], Ms. Lakshmi SN[2], Ms.Teena Kumari B N[3]

[1]Prof. of Practice, Department of Management, Al Ameen Institute of Management Studies, Bangalore
[2]Research scholar-School of commerce-Presidency University, Bangalore & Assistant professor Department of Business Administration, Koshys institute of management studies
[3]Research Scholar, Kuvempu University, Shivamogga-577451 & Assistant Professor, MBA dept, Akash Institute of Engineering and Technology, Bangalore-562110, Karnataka

Abstract: The digital banking sector has revolutionized the financial industry, offering customers unprecedented convenience and access to banking services. However, the rise of digital banking has also attracted a myriad of cyber threats, from phishing attacks to sophisticated malware, posing significant risks to financial institutions and their customers. Traditional cyber security measures, while effective to some extent, often struggle to keep pace with the rapidly evolving landscape of cyber threats. In this context, Artificial Intelligence (AI) and Machine Learning (ML) have emerged as powerful tools in enhancing the security of digital banking systems. By leveraging advanced algorithms, AI and ML can detect, analyze, and prevent cyber threats with greater speed and accuracy than traditional methods. This research paper explores the role of AI and ML in detecting and preventing cyber threats in digital banking, highlighting their effectiveness, challenges, and future potential.

Keywords: Cyber-attacks, Cyber Security, digital banking.

1. INTRODUCTION

Cyber threats are attempts to destroy data in a computer network/system. These cyber threats are originated from various sources like websites or computer system. The main task of Cyber threats to target to an attempt to obtain sensitive information through online channels from may sectors. In many sectors the Digital Banking is affected by Cyber threats in more number. A cyber threat is any malicious act that attempts to gain access to a Digital Banking without authorization or permission from the Account holder. Where a security breach or customers of a major bank having money stolen from their accounts. In the year 2021, banks from all over the world have been hit by hackers. The main aim of cyber Security in Digital Banking is to provide safety measures to the user's account digital money like debit cards and credit cards for transactions.

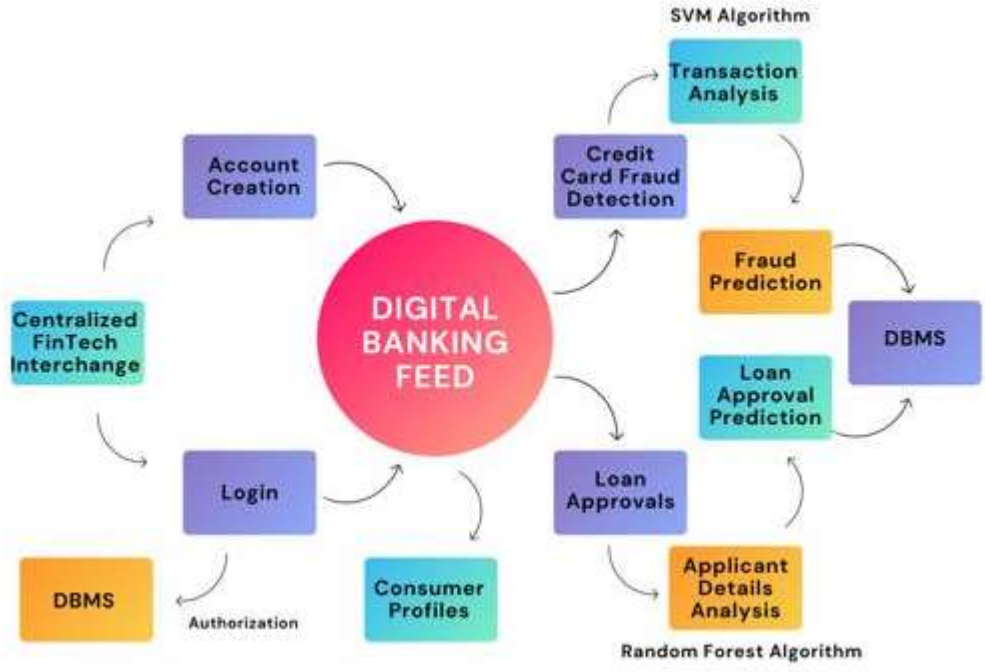
The banking sector in India, like many others worldwide, is undergoing a significant digital transformation driven by advancements in technology and evolving consumer expectations (Nawaz et al., 2024). This transformation promises increased efficiency, better customer experiences, and broader financial inclusion. However, it also brings forth substantial

challenges, particularly concerning data privacy and cybersecurity. As banks adopt new technologies such as cloud computing, artificial intelligence, and mobile banking, they become increasingly vulnerable to cyber threats and breaches, posing risks to sensitive customer information and financial stability (Farayola, 2024).

Conceptual Study

The conceptual study section delves into the theoretical underpinnings of AI and ML in cybersecurity, particularly in the context of digital banking.

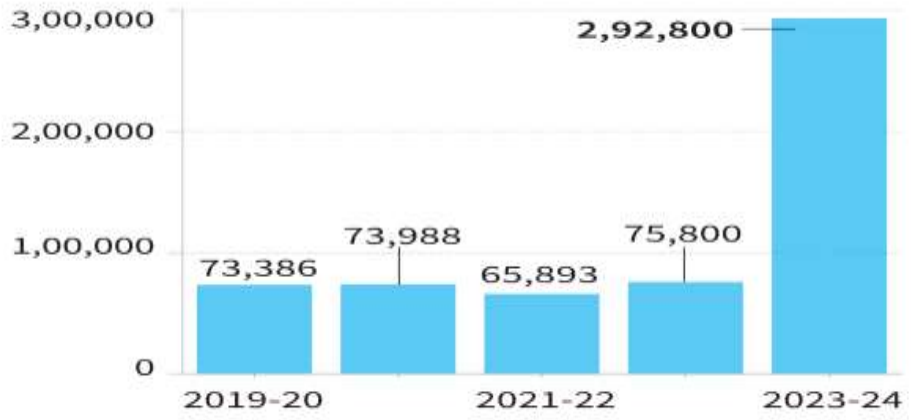
- **Artificial Intelligence**: AI in cybersecurity refers to the use of algorithms and models to simulate human intelligence, enabling systems to make decisions, learn from data, and adapt to new threats. In digital banking, AI can be used to automate threat detection, risk assessment, and response strategies.
- **Machine Learning**: A subset of AI, ML focuses on developing algorithms that allow systems to learn from data without being explicitly programmed. In cybersecurity, ML models can be trained to recognize patterns associated with cyber threats, predict potential attacks, and initiate preventive measures.
- **Applications in Digital Banking**: The study explores various applications of AI and ML in digital banking, such as fraud detection, anomaly detection, behavioral biometrics, and automated incident response. It also discusses the use of neural networks, deep learning, and natural language processing (NLP) in identifying and mitigating threats.



Source: Suri babu Nuthalapati / Kuey (2023)

Cyber fraud in banking transactions

India's impressive expansion in online transactions also coincides with an unprecedented spike in cyber frauds. According to data from the Reserve Bank of India, sent in response to the authors' Right to Information (RTI) application, ₹3,207 crore was lost because of 5,82,000 cases of cyber fraud between FY2020 and FY2024. With digital transactions set to significantly surge again this festival season, this statistic assumes significance.



Source: https://www.thehindu.com/data/cyber-fraud-in-banking-transactions-surges-in-fy24-data/article68813626.ece

Chart one shows that FY2024 has been an exceptional year for cyber fraud, outpacing the previous three years in terms of both the number of incidents and the amount of loss. The number of cyber fraud incidents has increased from 75,800 cases in FY 2023 to 2,92,800 cases in FY2024.

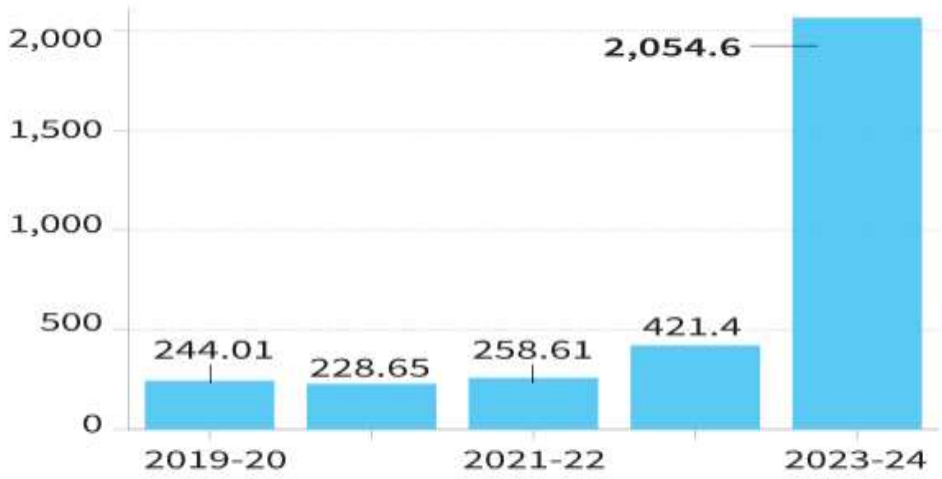


Chart 2: The chart shows the amount of loss incurred from cyber frauds in ₹ crore, The amount of money lost rose from ₹421.4 crore in FY2023 to ₹2,054.6 crore FY2024 **.** There were two major pushes for digital transactions. The first came in the wake of demonetisation in 2016. Nearly every national and regional daily then carried advertisements of a famous e-wallet company, thanking the Prime Minister for promoting digital transactions. The next impetus came during the COVID-19-induced lockdown when physical currency was considered a potential carrier of the deadly virus. Digital transactions are meant to curb tax evasion, corruption, and the use of hard cash in crime.

However, the decision to promote them was taken without putting in place adequate measures to prevent cyber fraud. Many people keep falling victim to new forms of online crimes. While financial institutions may implement sophisticated cybersecurity measures, many people find them too complex to navigate. Banks need to catch up and ensure cybersecurity before more money is lost.

Threats for Cyber security in Digital Banking

1. **Phishing and Social Engineering Attacks**

Phishing remains one of the most prevalent cybersecurity threats in digital banking. Cybercriminals use deceptive emails, text messages, or fake websites to trick users into divulging sensitive information such as login credentials or credit card details. Social engineering tactics exploit human psychology, such as urgency or fear, to manipulate individuals. Phishing attacks are increasingly sophisticated, with fraudsters often impersonating banks or financial institutions to gain trust. Spear-phishing, a targeted version of phishing, poses a significant threat to high-value customers and bank employees. These attacks can lead to unauthorized access to accounts and financial losses. Banks face reputational damage, and customers risk identity theft. Educating users about recognizing phishing attempts and implementing robust email security measures are essential defenses. Multi-factor authentication (MFA) also helps mitigate the risks. Ensuring regular updates and monitoring communication channels can further reduce vulnerabilities.

2. **Malware and Ransomware Attacks**

Malware and ransomware attacks target digital banking systems and user devices to steal data or disrupt services. Banking Trojans, a type of malware, are designed to capture login credentials, intercept transactions, or redirect users to malicious websites. Ransomware locks critical banking systems, demanding payment for restoring access. These attacks can halt operations, compromise customer data, and incur significant financial losses. With the rise of mobile banking, malware is also distributed through malicious apps or infected software. Cybercriminals exploit vulnerabilities in operating systems and third-party applications. Effective cybersecurity measures include deploying anti-malware solutions, patching software vulnerabilities, and monitoring network traffic. Banks should also regularly back up data to mitigate ransomware threats. Educating customers about safe browsing practices and avoiding suspicious downloads is equally critical.

3. **Data Breaches and Insider Threats**

Data breaches in digital banking expose sensitive customer information, such as account details, transaction history, and personal identification. Cybercriminals often exploit security gaps in databases or cloud storage to access this data. Insider threats, whether intentional or accidental, are another major concern. Employees with access to critical systems may misuse data for personal gain or fall victim to phishing attacks, inadvertently leaking sensitive information. These incidents erode customer trust, damage a bank's reputation, and lead to regulatory penalties. To address this, banks must implement role-based access controls, conduct regular security audits, and monitor employee activities. Encryption of sensitive data and strict compliance with data protection laws further enhance security. Building a culture of security awareness among employees is essential to minimize insider risks.

4. **Identity Theft and Account Takeover**

Identity theft is a growing concern in digital banking, where cybercriminals use stolen personal information to impersonate customers and access accounts. Techniques like credential stuffing and brute-force attacks exploit weak or reused passwords to gain unauthorized access. Account takeover attacks involve cybercriminals locking out legitimate users from their accounts by changing login credentials. These attacks can result in unauthorized transactions, financial loss, and compromised credit scores. Implementing strong password policies, biometric authentication, and transaction monitoring helps reduce these risks. Banks also need to adopt anomaly detection systems to flag suspicious activities. Customers should be educated about safeguarding their personal information and avoiding

the reuse of passwords across platforms. Swift response mechanisms can mitigate the damage caused by such attacks.

5. **Distributed Denial of Service (DDoS) Attacks**

Distributed Denial of Service (DDoS) attacks aim to overwhelm digital banking servers with a massive volume of traffic, rendering services unavailable. These attacks disrupt online banking, mobile apps, and payment gateways, causing inconvenience to customers and financial losses for banks. Cybercriminals often use botnets—networks of infected devices—to launch large-scale DDoS attacks. In some cases, attackers use DDoS as a distraction to execute other malicious activities, such as data breaches. Banks must invest in DDoS mitigation tools, including traffic filtering and load balancing systems, to counter such threats. Regular stress testing of IT infrastructure helps ensure resilience. Collaborating with internet service providers (ISPs) and adopting scalable cloud-based solutions also strengthen defenses. Quick incident response and clear communication with customers are crucial during an attack.

6. **Weak Authentication and Unauthorized Access**

Weak authentication mechanisms are a significant vulnerability in digital banking. Cybercriminals exploit weak or default passwords and systems that lack two-factor authentication (2FA) to gain unauthorized access to accounts. Biometric authentication, though increasingly common, is not immune to spoofing attacks. Session hijacking and man-in-the-middle attacks further exacerbate the risk of unauthorized access. Implementing multi-factor authentication and end-to-end encryption are essential for securing digital banking platforms. Banks should enforce strong password policies and regularly prompt users to update their credentials. Using behavioral analytics to detect unusual login patterns can help prevent unauthorized access. Customers should be educated about recognizing phishing attempts that aim to steal authentication credentials. Regularly updating authentication systems and staying ahead of emerging threats is critical for long-term security.

7. **Mobile Banking Vulnerabilities**

The increasing reliance on mobile banking has introduced unique cybersecurity challenges. Mobile apps are often targeted by cybercriminals through malicious software, fake apps, and vulnerabilities in application programming interfaces (APIs). Public Wi-Fi networks and unsecured mobile devices further expose users to attacks like session hijacking and data interception. Rooted or jailbroken devices are particularly vulnerable to malware. Banks must ensure that mobile banking apps undergo rigorous security testing and comply with secure coding practices. Features like app sandboxing and secure APIs enhance security. Customers should be encouraged to use only official app stores for downloads and to avoid accessing banking services on unsecured networks. Implementing device authentication and transaction alerts can help mitigate risks. Regular updates to mobile apps are essential to address newly discovered vulnerabilities.

Lack of Cyber Security in E-Banking:

1. Weak Security Protocols in E-Banking Systems

The lack of robust security protocols in e-banking systems exposes customers and financial institutions to cyber threats. Many banks rely on outdated encryption methods, making it easier for hackers to intercept sensitive information. Weak firewall protections and unpatched software vulnerabilities further exacerbate the risks. Hackers exploit these gaps to access account details, execute fraudulent transactions, or launch ransomware attacks. Implementing advanced security frameworks, such as multi-factor authentication and end-to-end encryption, is essential for securing e-banking platforms. Without stringent security protocols, customer trust in digital banking diminishes. Regular penetration testing and real-

time monitoring can help banks detect and mitigate security breaches. Compliance with cybersecurity standards like PCI-DSS is also critical. Additionally, banks must invest in upgrading legacy systems to stay ahead of cybercriminals.

2. Ineffective Customer Authentication Mechanisms

Weak authentication mechanisms in e-banking systems lead to unauthorized access and financial fraud. Many banks still rely on single-factor authentication, such as simple passwords, which are vulnerable to phishing and brute-force attacks. This lack of strong authentication increases the likelihood of account takeovers and identity theft. Advanced authentication methods like biometric verification, OTPs, and behavioral analytics are necessary to secure user access. However, their implementation remains inconsistent across banks, creating gaps in security. Customers often reuse passwords, further compounding the issue. Banks must enforce strong password policies and promote awareness of authentication best practices. Two-factor authentication (2FA) and adaptive authentication systems can significantly enhance security. Consistent and user-friendly authentication measures reduce risks while maintaining customer convenience.

3. Limited Awareness among Customers

The lack of cybersecurity awareness among e-banking users is a significant vulnerability. Many customers fail to recognize phishing attempts or understand the importance of strong passwords. They often click on malicious links, share sensitive information with fraudsters, or use unsecured devices for banking transactions. This lack of vigilance makes it easier for cybercriminals to exploit their accounts. Banks must prioritize customer education through campaigns, workshops, and regular alerts about potential threats. Interactive tools like phishing simulations can help users identify scams. Providing clear guidance on secure banking practices, such as using official banking apps and avoiding public Wi-Fi, is essential. Empowering customers with knowledge creates an additional layer of security against cyberattacks.

4. Vulnerabilities in Mobile and Online Banking Platforms

Mobile and online banking platforms often have security weaknesses that cybercriminals exploit. Vulnerabilities in mobile apps, such as improper API configurations and unencrypted data, allow hackers to intercept transactions or steal credentials. Additionally, some e-banking platforms fail to implement secure session management, leading to risks like session hijacking. Public Wi-Fi networks further expose users to man-in-the-middle attacks. Banks must ensure their platforms comply with secure coding practices and undergo regular security audits. Encryption of data in transit and at rest is critical to protecting sensitive information. Multi-factor authentication (MFA) and device recognition can minimize risks. By addressing platform vulnerabilities, banks can strengthen trust and ensure secure digital banking experiences.

5. Insufficient Incident Response and Monitoring

A lack of real-time monitoring and ineffective incident response mechanisms leave e-banking systems exposed to prolonged cyberattacks. Many banks do not have robust systems to detect anomalies or respond quickly to breaches. Cybercriminals exploit this delay to carry out large-scale data theft or financial fraud. Implementing real-time threat detection systems powered by AI and machine learning can help banks identify and mitigate attacks proactively. An effective incident response plan ensures quick recovery and minimizes damage. Banks should also establish a dedicated cybersecurity team to handle incidents and continuously improve their defenses. Regularly updating incident response protocols and conducting drills prepares banks for evolving threats. Transparency in communicating incidents to customers builds trust and accountability.

6. Overreliance on Legacy Systems

The dependence on outdated legacy systems in e-banking creates significant cybersecurity challenges. Legacy systems often lack modern security features, making them vulnerable to sophisticated cyberattacks. They are also difficult to update, leading to unpatched vulnerabilities that hackers can exploit. Overreliance on such systems hampers the implementation of advanced security measures like blockchain-based transactions or real-time fraud detection. Migrating to modern, secure, and scalable platforms is essential for reducing risks. Cloud-based solutions with integrated security protocols offer a viable alternative. Banks must allocate resources to upgrade infrastructure and ensure compatibility with new technologies. Investing in cybersecurity innovation protects customer data and maintains the integrity of e-banking systems.

Cyber security in E-Banking:

The increasing adoption of digital banking has transformed the way financial transactions are conducted, offering convenience and efficiency to customers. However, this digital shift has also made the banking sector a prime target for cybercriminals. Cybersecurity in digital banking involves implementing robust measures to protect sensitive financial data, customer information, and banking infrastructure from malicious activities. Below are key aspects of cybersecurity in digital banking:

1. Importance of Cybersecurity in Digital Banking

Cybersecurity is essential for safeguarding customer trust, preventing financial fraud, and complying with regulatory requirements. Banks handle vast amounts of sensitive data, including personal and financial details, which, if compromised, can lead to severe consequences for both customers and institutions. Strong cybersecurity measures ensure the confidentiality, integrity, and availability of digital banking systems.

2. Common Cyber Threats in Digital Banking

Digital banking faces several threats, such as phishing, ransomware attacks, data breaches, malware infections, and Distributed Denial of Service (DDoS) attacks. These threats exploit vulnerabilities in banking systems, mobile apps, and customer devices. Additionally, insider threats and social engineering tactics contribute to cybersecurity risks.

3. Role of Technology in Enhancing Cybersecurity

Advanced technologies like Artificial Intelligence (AI), Machine Learning (ML), and blockchain play a pivotal role in cybersecurity. AI and ML help in real-time threat detection and predictive analysis, while blockchain enhances the security of transactions through decentralized systems. Encryption, firewalls, and secure APIs are critical components of a bank's cybersecurity infrastructure.

4. Multi-Factor Authentication (MFA) and Biometric Security

MFA and biometric authentication are essential for strengthening user authentication. MFA requires customers to verify their identity through multiple layers, such as passwords, OTPs, and fingerprint or facial recognition. These methods reduce the likelihood of unauthorized access and account takeovers.

5. Regulatory Compliance and Standards

Banks must comply with cybersecurity regulations, such as GDPR, PCI-DSS, and data protection laws. These standards ensure that financial institutions implement adequate security measures to protect customer data. Regulatory compliance fosters a consistent approach to addressing cybersecurity challenges.

6. Educating Customers on Cybersecurity

Customer awareness is a critical component of digital banking security. Banks must educate their customers about phishing scams, the importance of strong passwords, and safe online banking practices. Regular communication, such as alerts and tips, helps customers avoid falling victim to cyberattacks.

2. CONCLUSION

IT is become the backbone of the Digital banking system. It provides a best support for the digital banking. Presently the digital banking sector where attacks by cyber crimes like, phishing, hacking, forgery, cheating etc. are committed. By ensuring authentication, identification and verification techniques the cyber crimes can be prevented. The weapons for cyber crime is Cyber Security which is used in digital banking as one of the best and important tool. With the growth of digitalization in the banking the threats or attacks from cyber criminals as became more to avoid that the cyber security awareness and different cyber security techniques are used.

3. REFERENCES

[1] Dr. M. Lokanadha Reddy , Mrs. V. Bhargavi "Cyber security attacks in banking sector: Emerging security challenges and Threats" in http://www.iasir.net
[2] Nandkumar Saravade, Director, "Cyber Security and Compliance NASSCOM : Cyber Security Initiatives in India"
[3] Claessens, J., Dem, V., De Cock, D., Preneel, B., &Vandewalle, J. (2002). On the security of today s online electronic banking systems. Computers & Security, 213: 253-265.
[4] Basha, S. M., & Ramaratnam, M. S. (2017). Construction of an Optimal Portfolio Using Sharpe's Single Index Model: A Study on Nifty Midcap 150 Scrips. Indian Journal of Research in Capital Markets, 4(4), 25-41.
[5] Krishnamoorthy, D. N., & Mahabub Basha, S. (2022). An empirical study on construction portfolio with reference to BSE. Int J Finance Manage Econ, 5(1), 110-114.
[6] Mohammed, B. Z., Kumar, P. M., Thilaga, S., & Basha, M. (2022). An Empirical Study On Customer Experience And Customer Engagement Towards Electric Bikes With Reference To Bangalore City. Journal of Positive School Psychology, 4591-4597.
[7] Ahmad, A. Y. A. B., Kumari, S. S., MahabubBasha, S., Guha, S. K., Gehlot, A., & Pant, B. (2023, January). Blockchain Implementation in Financial Sector and Cyber Security System. In 2023 International Conference on Artificial Intelligence and Smart Communication (AISC) (pp. 586-590). IEEE.
[8] Janani, S., Sivarathinabala, M., Anand, R., Ahamad, S., Usmani, M. A., & Basha, S. M. (2023, February). Machine Learning Analysis on Predicting Credit Card Forgery. In International Conference On Innovative Computing And Communication (pp. 137-148). Singapore: Springer Nature Singapore.
[9] Kalyan, N. B., Ahmad, K., Rahi, F., Shelke, C., & Basha, S. M. (2023, September). Application of Internet of Things and Machine learning in improving supply chain financial risk management System. In 2023 IEEE 2nd International Conference on Industrial Electronics: Developments & Applications (ICIDeA) (pp. 211-216). IEEE.
[10] Sheshadri, T., Shelly, R., Sharma, K., Sharma, T., & Basha, M. (2024). An Empirical Study on Integration of Artificial Intelligence and Marketing Management to Transform

Consumer Engagement in Selected PSU Banks (PNB and Canara Banks). NATURALISTA CAMPANO, 28(1), 463-471.

[11] Joe, M. P. (2024). Enhancing Employability by Design: Optimizing Retention and Achievement in Indian Higher Education Institution. NATURALISTA CAMPANO, 28(1), 472-481.

[12] Dawra, A., Ramachandran, K. K., Mohanty, D., Gowrabhathini, J., Goswami, B., Ross, D. S., & Mahabub Basha, S. (2024). 12Enhancing Business Development, Ethics, and Governance with the Adoption of Distributed Systems. Meta Heuristic Algorithms for Advanced Distributed Systems, 193-209.

[13] Singh, A., Krishna, S. H., Tadamarla, A., Gupta, S., Mane, A., & Basha, M. (2023, December). Design and Implementation of Blockchain Based Technology for Supply Chain Quality Management: Challenges and Opportunities. In 2023 4th International Conference on Computation, Automation and Knowledge Management (ICCAKM) (pp. 01-06). IEEE.

[14] Almashaqbeh, H. A., Ramachandran, K. K., Guha, S. K., Basha, M., & Nomani, M. Z. M. (2024). The Advancement of Using Internet of Things in Blockchain Applications for Creating Sustainable Environment in the Real Word Scenario. Computer Science Engineering and Emerging Technologies: Proceedings of ICCS 2022, 278.

[15] Kotti, J., Ganesh, C. N., Naveenan, R. V., Gorde, S. G., Basha, M., Pramanik, S., & Gupta, A. (2024). Utilizing Big Data Technology for Online Financial Risk Management. In Artificial Intelligence Approaches to Sustainable Accounting (pp. 135-148). IGI Global.

[16] Shaik, M. (2023). Impact of artificial intelligence on marketing. East Asian Journal of Multidisciplinary Research, 2(3), 993-1004.

[17] Reddy, K., SN, M. L., Thilaga, S., & Basha, M. M. (2023). Construction Of An Optimal Portfolio Using The Single Index Model: An Empirical Study Of Pre And Post Covid 19. Journal of Pharmaceutical Negative Results, 406-417.

[18] Basha, M., Reddy, K., Mubeen, S., Raju, K. H. H., & Jalaja, V. (2023). Does the Performance of Banking Sector Promote Economic Growth? A Time Series Analysis. International Journal of Professional Business Review: Int. J. Prof. Bus. Rev., 8(6), 7.

[19] Rana, S., Sheshadri, T., Malhotra, N., & Basha, S. M. (2024). Creating Digital Learning Environments: Tools and Technologies for Success. In Transdisciplinary Teaching and Technological Integration for Improved Learning: Case Studies and Practical Approaches (pp. 1-21). IGI Global.

[20] Mahabub, B. S., Haralayya, B., Sisodia, D. R., Tiwari, M., Raghuwanshi, S., Venkatesan, K. G. S., & Bhanot, A. An Empirical Analysis of Machine Learning and Strategic Management of Economic and Financial Security and its Impact on Business Enterprises. In Recent Advances in Management and Engineering (pp. 26-32). CRC Press.

[21] Mahabub Basha Shaik, "Investor Perception on Mutual Fund with Special Reference to Ananthapuramu, Andhra Pradesh", International Journal of Science and Research (IJSR), Volume 4 Issue 1, January 2015, pp. 1768-1772, https://www.ijsr.net/getabstract.php?paperid=SUB15756

[22] EMERGING BUSINESS PARADIGMS TRANSITION FROM INDUSTRY 4.0 TO INDUSTRY 5.0 IN INDIA. (2024). CAHIERS MAGELLANES-NS, 6(2), 629-639. https://magellanes.com/index.php/CMN/article/view/347

[23] Dr.V. Jalaja, Dr. Thejasvi Sheshadri, Dr.V.K. Arthi, Dr.S. Thilaga, Dr.J. Bamini, S. Mahabub Basha, & Manyam Kethan. (2024). Maximizing Marketing Value: An Empirical Study on the Framework for Assessing AI and ML Integration in Marketing Management. Indian Journal of Information Sources and Services, 14(3), 64–70. https://doi.org/10.51983/ijiss-2024.14.3.09
[24] Raji N, George, V., Iyer, R. S., Sharma, S., Pathan, F. I., & Basha S, M. (2024). REVOLUTIONIZING RECRUITMENT: THE ROLE OF ARTIFICIAL INTELLIGENCE IN TALENT ACQUISITION. ShodhKosh: Journal of Visual and Performing Arts, 5(1), 750–759. https://doi.org/10.29121/shodhkosh.v5.i1.2024.2141
[25] Policepatil, S., Sharma, J., Kumar, B., Singh, D., Pramanik, S., Gupta, A., & Mahabub, B. S. (2025). Financial Sector Hyper-Automation: Transforming Banking and Investing Procedures. In Examining Global Regulations During the Rise of Fintech (pp. 299-318). IGI Global.
[26] Venkatarathnam, N., Goranta, L. R., Kiran, P. C., Raju, B. P. G., Dilli, S., Basha, S. M., & Kethan, M. (2024). An Empirical Study on Implementation of AI & ML in Stock Market Prediction. *Indian Journal of Information Sources and Services*, *14*(4), 165–174. https://doi.org/10.51983/ijiss-2024.14.4.26
[27] Kavishwar, Rahul Krishnaji. "Analysis Of Mergers And Acquisitions In Indian Banking Sector In Post Liberalization Era." (2014).
[28] Kavishwar, R. K., Patil, S. R., & Rajendraprasad, K. H. (2012). Mergers and acquisitions in indian banking sector. *Journal of Commerce and Management Thought*, *3*(1), 98-111.
[29] Sri Hari, V., Raju, B. P. G., & Karthik Reddy, L. K. (2024). Big Data Analytics in Support of the Decision Making Process in IT Sector. *Journal of Informatics Education and Research*, *4*(2).
[30] Kavishwar, R. K., Patil, S. R., & Rajendraprasad, K. H. (2012). Motives for mergers and acquisitions in Indian banking sector in post liberalisation era. *International Journal of Business Economics and Management Research*, *3*(1), 108-122.
[31] Kavishwar, R. K. Cross Border Mergers and Acquisitions in Indian Banking Sector.
[32] Chatterjee, S. (2017). Skill Development for Youths: Recent Initiatives in Karnataka. Social Sciences, 7(02).
[33] Rathnam, N. V., & Narasaiah, P. V. (2012). Sericulture Industry-A Boon for Rural Poor: Special Focus on Chittoor District of AP. SEDME (Small Enterprises Development, Management & Extension Journal), 39(3), 17-33.
[34] Venkatarathnam, N., & Suresh, K. (2018). Job Satisfaction of Employees in Amararaja Batteries Limited, Tirupati-A Pragmatic Study. International Journal of Management, IT and Engineering, 8(6), 8-18.
[35] Dilli, S., Venkatarathnam, N., & Naidu, R. (2022). A Study On Stress Management Practices And Its Influence On Organizational Behavior Among Information Technology Employees. Journal of Positive School Psychology, 6(10), 2174-2182.
[36] Raman, M. S., Venkatarathnam, N., Kumar, B., Anjani, P. K., Srinivasan, M., & Kannappan, S. (2022). A Study on 'Role of Financial Literacy in Women Empowerment and Financial Inclusion in Developing Economies during COVID-19 Pandemic Outbreak'. NeuroQuantology, 20(5), 3009.
[37] Rathnam, N. V., Narasaiah, P. V., & Murthy, D. S. (2013). Current Status of Silk Industry in India-An Evaluation. SEDME (Small Enterprises Development, Management & Extension Journal), 40(4), 55-68.

[38] Murthy, D. S., Subramanyachary, P., Naidu, N. G., Singh, S., & Rathnam, N. V. (2022). Digital Entrepreneurship: An Aisle For Success Of Business Enterprises. NeuroQuantology, 20(8), 3224.