Educational Administration: Theory and Practice
2024, 30(5), 15326 - 15332
ISSN: 2148-2403
https://kuey.net/ **Research Article**

Cyber Frauds In India's Digital Payment Ecosystem: Risk, Impacts, And Regulatory Responses

Ashish Sharma[1*], Dr. Yogender Singh[2]

[1*]Research scholar, Department of Law, MDU, Rohtak, ashish09bhardwaj@gmail.com
[2]Associate professor, Faculty of law, MDU, Rohtak, prof.ysingh@mdurohtak.ac.in

Citation: Ashish Sharma, et.al (2024), Cyber Frauds In India's Digital Payment Ecosystem: Risk, Impacts, And Regulatory Responses, *Educational Administration: Theory and Practice, 30(5)* 15326 - 15332
Doi: 10.53555/kuey.v30i5.8951

ARTICLE INFO

ABSTRACT

Digital transformation in financial transactions has changed the method of payment. We have witnessed amany-fold and rapid increase in the digital payment. As more individuals opt for digital payments, the potential of being exposed to cyber-attacks such as online fraud, the to identify, and spyware or virus attacks is rising. Transaction on digital mode has led to an increase in internet-based crimes known by the term 'cyberfrauds. Cyber fraud is an illegal act practiced by hackers on web applications, web browsers, and websites. Secured payment is critical for any company that deals with electronic payment s transactions. One of the most vital issues confronting players in the digital payment ecosystem is cybersecurity. The growth of such cyber-attacks can be attributed to various reasons, including a lackof knowledge and a poor digital payment infrastructure. To safeguard against threats of cybercrime, the are various cyber security techniques. This research paper deals in understanding the causes, threats, solutions and regulatory responses to cyber-attacks in digital payment methods.

INTRODUCTION

In the last few years, especially post demonetization in 2016 and the COVID-19 pandemic, there has been a major spike in the number of digital payments in India. Users can pay digitally using a variety of methods, including cards, wallets, mobile banking, QR codes, the Unified Payments Interface (UPI), and more. The expansion of digital transactions in India has been greatly aided by UPI. However, the growing use of these sophisticated payment methods has also given criminals hitherto unheard-of chances to commit fraud by taking advantage of human weaknesses and digital payment systems.
According to Cyber crime Magazine, by 2025 Cybercrime will cost the globe $ 10.5 trillion per year. Furthermore,during the next four years,world wide cyber crime losses may betoclimbbyabout15%annually. As per the annual report of the RBI, in 2022-23, 6,659 digital frauds (card/internet) were reported amounting to Rs 276 crore. This is up from 3,596 fraudulent transactions worth Rs 155 crore reported in the year before. Although many of the users are adopting online payment methods, some factors act as barriers to the development of online payment systems like lack of awareness, lack of strong ecosystem for cashless payment,securityconcerns,cashpaymentpreference,lackofproperdigitalregulations,andlackofeffectivegrievancesandredressalmechanisms.Thisleadstochancesofgettingtrappedbycyberassaultersandultimatelyfinancialloss es. Online fraud has increased as a result of the exponential growth in digital payments brought about by our daily integration of technology.
A huge number of people now prefer online modes of payment, which has inspired fraudsters to use innovative ways to dupe customers. Many customers have lost their hard-earned money to these scammers after disclosing personal information. Interconnected smart devices and online activity contributed to this trend of payment fraud by making customers more vulnerable to deception. E-commerce losses due to online payment fraud may be to increase by 131% from 2022 to 2027.Digitization has also make mushrooming of fraudsters, who are becoming smarter as they too adopt technology as it evolves. Striking a balance between security and seamless payments is now one of the major challenges for banks and financial institutions.

CYBERSECURITYANDDIGITALPAYMENTFRAUD

Several high-impact cyber security cases have been reported in past years across industries such as healthcare, e-business, telecom, monetary services, government services, manufacturing, and hospitality,resulting infar-reaching consequences and creating cyber security as one of the top business risks.

The threat of cyber fraud is not constrained by geographical boundaries.India's corporations have been exposed to this danger in a significant way. According to the KPMG report (2017), roughly 72%of businesses have observed cyber-attacks in some form. The attacks are result of the emphasis and astrong push for digital adoption leading to phishing attacks on payment channels. The most common attacks are (DDoS) andspam-acommon attack vector.As the usage of mobile phones for online transactions such as purchases, payments, and banking grew,also increased the cyber incidents.

Fraud in online payments

At any point, fraud can be committed. The following section describes some typical methods and strategies that fraudsters employ to carry out these scams throughout the payment ecosystem.

1. Typical types of fraud

1.1 Impersonation and identity theft

In order to gain access and start online payments or open a payment account to carry out transactions, fraudsters obtain users' personal information (such as PAN/Aadhaar details or social media credentials) or important information about their bank accounts. Customers' personal information is made public on the dark web, which makes it possible for scammers to commit this kind of fraud. In India, there have been numerous instances involving banks, payment banks, and identity theft victims who have stated that fraudsters have used their personal information to carry out fraudulent activities, including obtaining bank credit cards. Additionally, scammers may pose as a trusted acquaintance of the user or an authorised official (bank employee, police officer, government official, health professional, etc.

1.2 Phishing/vishing

Vishing scams are carried out by scammers that impersonate bank customer care representatives and persuade victims to update or complete their electronic Know-your-Customer (eKYC) online in order to maintain the account's activity. When a customer completes the procedure online, fraudsters are able to gain private information and use the shared OTP to carry out illicit activities. Phishing fraud occurs when scammers send emails or texts with a malicious link that directs the victim to a website that looks remarkably similar to the bank's real website. Customers ultimately mistake the bogus website for the real one and provide sensitive information, which the scammers exploit to carry out illicit operations.

1.3Skimming the web

Web skimming is a hacking method whereby scammers get sensitive financial information by installing malicious software on an application's payment or checkout pages. E-commerce websites, for example, use third-party programs, which makes it possible for scammers to insert their harmful code into a reliable third-party host website. In India, there have been several documented instances of web skimming, in which criminals utilise e-commerce websites to steal the card information of unwary consumers, including the card number, CVV, and expiration date. Due to their extensive visibility and popularity, e-commerce websites have been specifically targeted.

1.4 Through the use of QR codes

The naive consumer receives a phoney QR code from fraudsters, which they scan to get money into their bank account. Instead, the money is taken out of the customer's account after the code has been scanned. Additionally, in retail merchant locations, scammers may substitute their own QR code for the actual one, tricking customers into paying to the incorrect account.

1.5 Social engineering

Social engineering attacks often entail tricking unwary customers into disclosing private information by feigning a significant problem with their bank accounts.

1.6 Takeover of accounts

In this kind of fraud, scammers attempt to get unauthorised access to a user's account by obtaining their login information and completing payments. Most of the time, the fraudsters go undetected because they alter the information they initially got before making payments.

1.7 Help with remote access

In this kind of scam, the con artists persuade the victim to grant them remote access to their device in order to fix certain technical problems. They frequently accomplish this by pretending to be a member of the technical support staff of a laptop service provider or a bank representative assisting with account unblocking or KYC assistance. Once remote access has been obtained, the scammers collect all private data pertaining to the user's payment accounts and exploit it fraudulently to make purchases.

1.8 Botnet attack
Criminals introduce harmful software (commonly referred to as bots) into a network of computers and connect them to execute synchronized botnet assaults.
This enables criminals to infiltrate users' devices and bypass their current security measures to capture sensitive information.

2. Use of fraud typologies to perpetrate payment channels
2.1 UPI payments and wallets
UPI provides various payment methods, including QR code scanning, UPI ID-based transactions, or payments using phone numbers. A prevalent technique involves sending users a harmful link disguised as a request to collect payment for goods or services. Other frequently used fraudulent tactics in UPI transactions involve utilizing counterfeit QR codes and offering remote access support.

2.2 ATMs /point-of-sale (PoS) terminals
Fraudsters carry out transactions from a user's account by exploiting personal data acquired through remote access assistance or by using skimming devices placed on ATMs or PoS terminals.

2.3 Aadhaar-enabled payment system (AePS)
AePS is a payment method that allows customers to use their Aadhaar number for identification at a business correspondent (BC) who has a biometric PoS device to make cash withdrawals. Dishonest BCs may withdraw more than the requested amount without issuing a receipt, pocketing the extra funds. Additionally, criminals can replicate customers' fingerprints (biometrics) to steal money through AePS.

3. Future fraud risks
3.1 Frauds associated with near-field communication (NFC) technology:
NFC-enabled cards used for contactless payments are generally more secure since they utilize radio waves rather than internet connections. Nonetheless, a significant disadvantage of these cards is the absence of password protection. Criminals are likely to take advantage of this technology as the limits for payment acceptance on these transactions keep rising.

3.2SIM Swap Scam
Using social engineering techniques such as phishing, smishing and its other forms the fraudster acquires the victim’s banking information and registered mobile phone number. Through fake calls, they insistthe victim port their old SIM to a new one as the present SIM is blocked due to some reasons. So, theperson should beware of such calls and never swap a SIM, in such cases, they should directly contact the network’s authorized toll-free numbers.

3.3 Frauds with the onset of 5G technology:
With the advancement of future technologies, the integration of 5G technology into the payments system will enable quicker transactions. However, this advancement may also create a broader attack surface for fraudsters. In June 2022, the Indian Government Union Cabinet announced that the 5G network would deliver speeds and capacity that are ten times greater than that of 4G. Consequently, traditional methods for identifying fraud will not be adequate to tackle frauds initiated by 5G. The increased number of devices using a single credential, coupled with the speed and low latency of 5G technology, will necessitate more sophisticated fraud detection techniques to effectively mitigate and prevent attacks.

PRECAUTIONARYSTEPSTOAVOIDCYBERATTACKSANDONLINEFRAUD
Completing KYC
Many times, victims received a call from fraudsters that their KYC is incomplete, we will complete it right now on call otherwise your account will be suspended. The thumb rule to avoid such fraud ulent calls is not to respond to the mand never click on the link provided sms and emails.

Setting Passwords
The person should always choose unique passwords and must change them frequently. Make sure that the credentials for all kinds of transactions are distinct and difficult.Passwords should not include names, birthdays, or other personal information. It is crucial and fundamental not to share passwords with anyone and keeping the same passwords for multiple devices.

Avoid Usage of Public Wi-Fi
When making online purchases, avoid accessing public Wi-Fi networks since they are more vulnerable to cyber-attacks,theft,andotherfraudulentactivities.Verifiedsitesprovideahighlevelofsecurity,thusit’salsocrucial to utilize only reputablewebsites for online financial transactions.

Cross-Check QR Codes
Always double-check the beneficiary when scanning QR codes, as hackers may quickly swap a validQR code used during transactions with a malicious QR code.

Reading Financial Statements
Remember that you read all notifications received after each payment and that you study the financial summary in detail once a week or more. If you see any discrepancies, file a ticket or approach the bank/payment platform right away.

Regulations dealing with cybercrimes and frauds in India
(i) The ITAct of 2000.
(ii) Indian Penal Code, 1860.
(iii) The DPDP Act, 2023.

The IT Act have the framework for the punishment of cybercrimes, including hacking and unauthorized access to personal information. Under sections 43 and 66 of the IT Act, someone who willfully and illegally accesses, downloads, copies, or extracts any material or information from a computer and its related resources is subject to punishment in the form of damages and compensation. Additionally, section 72 of IT Act deals with the protection of personal data and data security. The IT Act does address identity theft specifically, but it also contains legal provisions for the unauthorized access to sensitive information and personal data. Section 66C: This section describes the consequences of identity theft and indicates that they may includessentence of up to three years in jail or fine upto one lakh rupees. Section 66D: This section outlines the consequences for utilizing a computer resource to impersonate another person in order to commit fraud. These include a maximum penalty of three years in jail, a maximum fine of one lakh rupees, or both. The two pieces of legislation discuss about identity theft and other online frauds connected to ATM are the IT Act and the IT (Amendment) Act of 2008.The IPC of 1860, Section 416 and 419, handles impersonation fraud and imposes fines or prison sentences of up to three years, or both.

The Digital Personal Data Protection Act of 2023 (DPDP)
On August 11, 2023, the Central Government of India enacted the long-anticipated Digital Personal Data Protection Act (DPDP). This legislation mandates that data fiduciaries:
•Engage only third-party data processors who are contractually bound to adhere to DPDP protocols.
•Verify that personal data is both complete and accurate prior to utilizing it for decisions that impact the data principal or before facilitating the transfer of such data.
•Establish appropriate security measures and conduct audits to safeguard personal data and mitigate the risk of data breaches.
•Properly delete and dispose of all personal data when a data principal revokes their consent, unless legal obligations necessitate the retention of that data. The DPDP also created the Data Protection Board of India to oversee compliance.

Cybersecurity Regulatory Authorities
To implement cybersecurity regulations, the following key regulatory authorities ensure that laws and standards are adhered to by all organizations in India.
1. Computer Emergency Response Team (CERT-In)
Established in 2004, the Computer Emergency Response Team (CERT-In) serves as the national focal point for the collection, analysis, forecasting, and dissemination of non-critical cybersecurity incidents. Beyond reporting and notification of cybersecurity incidents, CERT-In provides guidance on best practices for managing and preventing such incidents. CERT-In functions as the principal task force that:
• Evaluates cyber threats, vulnerabilities, and advisory information
• Addresses cybersecurity incidents and data breaches
• Coordinates appropriate responses to cyber attacks and conducts forensic investigations for incident management
• Identifies, defines, and implements effective measures to mitigate cyber risks
• Advises organizations on best practices, guidelines, and precautions for managing cyber incidents to enhance their response capabilities.
The latest regulations issued by CERT-In focus on cybersecurity reporting, requiring all Indian companies, service providers, intermediaries, data centers, and businesses to report any identified cybersecurity incidents and data breaches within a six-hour timeframe. However, numerous Indian organizations have expressed their discontent with this demanding requirement, arguing that the limited reporting period does not allow adequate time to respond to cybersecurity incidents with a comprehensive report.

2. National Critical Information Infrastructure Protection Center (NCIIPC)
The National Critical Information Infrastructure Protection Center (NCIIPC) was established on January 16,

2014, by the Indian government, in accordance with Section 70A of the IT Act, 2000 (as amended in 2008). The NCIIPC serves as the national nodal agency for the protection of Critical Information Infrastructure. Furthermore, it is recognized as a unit of the National Technical Research Organization (NTRO) and operates under the Prime Minister's Office (PMO). The Indian Parliament categorizes cybersecurity into two segments: "Non-Critical Infrastructure (NCI)," overseen by CERT-In, and "Critical Information Infrastructure (CII)," managed by NCIIPC. The NCIIPC is tasked with monitoring and reporting national-level threats to critical information infrastructure, which encompasses various essential sectors.

1. Energy and power
2. Financial services, banking, and insurance
3. Information and telecommunications
4. Transportation services
5. Governmental entities
6. Public and strategic enterprises

3. Cyber Regulations Appellate Tribunal (CRAT) Established under Section 62 of the IT Act, 2000, the Central Government of India instituted the Cyber Regulations Appellate Tribunal (CRAT) as a primary governing entity responsible for fact-finding, gathering cyber evidence, and evaluating witnesses. Although CRAT does not possess the same level of jurisdiction regarding cybersecurity notifications as CERT-In, it plays a crucial role in addressing and responding to cybersecurity incidents and breaches. The powers of CRAT include:

• Receiving evidence through affidavits • Ensuring the presentation of all electronic and cyber evidence and records in court

• Enforcing, summoning, and issuing regular commissions for the examination of witnesses, documents, and individuals under oath

• Reviewing final court decisions to resolve incidents and cases

• Approving, dismissing, or declaring applications from alleged defaulters as ex-parte.

1. The Securities and Exchange Board of India (SEBI), established in 1988, serves as the regulatory authority for the securities and commodity markets in India, operating under the Ministry of Finance. SEBI is tasked with addressing the requirements of market intermediaries, investors, and securities issuers, ensuring the protection of their data, customer information, and transaction integrity. As of April 2022, SEBI comprises six committee members responsible for providing guidance on cybersecurity initiatives pertinent to the Indian market and advising on the development and maintenance of cybersecurity standards in alignment with global industry practices. Furthermore, SEBI collaborates with various agencies, including CERT-In, the National Cyber Coordination Center (NCSC), the Department of Telecommunications (DoT), and the Ministry of Electronics and Information Technology (MeitY). SEBI has instituted guidelines applicable to entities within its jurisdiction, such as stock brokers, stock exchanges, asset management companies (AMCs), mutual funds, and depository participants. Non-compliance with SEBI regulations, such as breaches of disclosure requirements, incurs penalties of ₹20,000 per day until the offending companies achieve compliance.6. Telecom Regulatory Authority of India (TRAI) & Department of Telecommunications (DoT).

The Telecom Regulatory Authority of India, in collaboration with the Department of Telecommunications, has strengthened regulations concerning user data privacy and its utilization. In 2018, TRAI issued recommendations for telecom operators regarding "Privacy, Security, and Ownership of Data in the Telecom Sector." The latest guidelines from TRAI outline additional responsibilities related to consumer data management, reflecting the fact that a significant portion of digital transactions in India is conducted through mobile devices.

7. RBI measures to secure digital transactions

1)For adding new payees, specific OTPs are needed from a secondary channel, making the process more secure.

2)New OTPs are required for high-value transactions, enhancing security for important financial dealings.

3)The time limit for OTPs is closely managed to reduce the chance of misuse.

4)Using digital signatures and Key-based Message Authentication Codes (KMAC) to identify and stop unauthorized transactions.

5)Educating customers about their rights as per the Consumer Protection Act and the responsibilities and risks linked with internet banking.

6)Informing customers via an alternate method for transactions exceeding a value specified by the customer.

8)Introducing systems to assess transaction patterns and highlight unusual activities, ensuring that transactions align with the customer's typical behaviour.

CONCLUSION

The present research discusses cybercrime and fraud in digital payment systems. Due to digitalization,all the payments are taking place on the web. This scenario has given exposure to cybercrime. The research presents various cyber frauds and the cyber security techniques to monitor the morto escape from the

secrimes.Ithighlightstheshiftofpaymentgatewayfromconventionaltodigital.This research paper presents the various regulatory bodies that regulates the cyber transaction and monitor the cybercrime across the country and the world. Many institutions like NCIIP and CERT-In have worked to monitor and control these cyber frauds. Themajorreasonsandmeasurestoavoidorgetsafefromtheseattacksareobservedintheresearch.

SUGGESTIONS

In 2023 alone, over 11 lakh complaints on digital payment fraud were reported through the National Cybercrime Reporting Portal (NCRP), helpline number 1930, and through complaints lodged with the police, and the victims have rarely seen any recovery of lost funds.

1. Curbing the presence of fraudulent apps on Android and iOS: The easy availability of predatory loan apps, fake KYC apps, and other types of fraudulent apps on Android and iOS is one of the primary factor of financial fraud. The Indian Cybercrime Coordination Centre (I4C) maintains a repository of such fraudulent apps and periodically sends hash values of these to Google for appropriate action. Separately, illegal and fraudulent lending apps are found on both Google Play Store and Apple App Store and these are being regularly sent to these entities for urgent action against such apps.

2. Promoting local fintech apps over foreign-owned apps: The Committee noted that Google Pay and Phonepay, both owned by foreign entities, dominate the Indian fintech sector as they command over 80 percent of the UPI market share. It urged the government to promote local alternatives as regulation of Indian apps would be more feasible for regulatory bodies.

3. Formulating region-specific strategies to address crimes in hotspots like the Mewat and Jamtara regions: The two major pockets from where cyber frauds originate are the Mewat Region (Delhi, Haryana, Uttar Pradesh and Rajasthan) and Jamtara Region (Jharkhand, Bihar, West Bengal, Chattisgarh and Odisha). The types of fraud committed in these areas include KYC fraud, remote accessing of phones, sextortion, AePS fraud, fake franchise fraud, QR-based fraud and spreading of Android malware.

4. Addressing AePS frauds carried out by biometric cloning: The Aadhaar Enabled Payment System (AePS) is a payment system that allows users to make financial transactions using their Aadhaar number and biometrics.

5. Addressing the usage of virtual accounts to mask the trail of money: A common tool used in committing financial fraud, especially in investment and predatory loan app scams, is virtual accounts. Banks provide virtual account facilities to some customers such as payment aggregators allowing them to open and map multiple virtual accounts to a single current or escrow account. These payment aggregators in turn assign these virtual accounts to their customers. Law enforcement agencies have little insight into what goes on in these virtual accounts as all the transactions are attributed to the main account. Furthermore, virtual accounts are provided with minimal KYC. Along with virtual accounts, virtual cards that work on Visa and Mastercard networks are used to egress money out of India. Hence, these virtual accounts and cards are being used to mask the trail of funds and might be evading anti-money laundering measures.

6. Working with foreign jurisdictions to curb crimes carried out from outside the country: Many cyber frauds include activity carried out outside the country, especially by Chinese actors operating from Dubai, Cambodia, Vietnam, and Hong Kong. Investment scams which run largely through the Telegram app, task-based scams, illegal loan apps, illegal gaming apps, ransomware, and matrimony scams (largely from Nigeria) are carried out from other jurisdictions. In these frauds, it is difficult for Indian agencies to locate the perpetrators. Sothe government focus on proper connection with legal agencies of the countries from which these scammers operate.

7. Setting up a nodal centre with representatives from various agencies to tackle cyber crimes more holistically: The issues related to cyber security are diverse ranging from hacking of critical digital infrastructure to social engineering techniques to lure people for quick financial gains, a single agency can't focus on all aspects, the Committee noted, stressing the need for coordination among various agencies like the IT Ministry, the Indian Cybercrime Coordination Centre (I4C), CERT-In, RBI, and NPCI.

8. Training staff in monitoring and law enforcement agencies to tackle cyber crime: Cyber security has diverse domains and to cater to these domains adequate staff specialised and trained in tackling cybercrimes is required. To this effect, the government train staff in monitoring and law enforcement agencies such as CERT-In, and state law enforcement agencies, equipping them with skills needed to understand and tackle cybercrime.

9. Punitive measures to curb cyber crimes have not been effective and need to be overhauled: Despite the exponential rise in cyber crimes and frauds over the last few years, the conviction rate in these cases is very low. The punitive measures have not been very effective in tackling cyber crimes and called for a statutory and legislative overhaul in the domain of cybercrimes so that punitive measures in legal system act as a deterrent for criminals. Additionally, the committee noted that only having punitive measures to combat cyber fraud is long-drawn, time-consuming, and less effective, and instead, the government must try to have a multipronged approach with effective coordination of all stakeholders.

10. Streamlining the process of returning money to victims of fraud: While fraud is rising at an alarming rate, in comparison to that recovery made the amount returned to the victim is very low. For example, in 2022, Rs 2294 crore was lost in cyber frauds but only Rs. 57 crore was returned to the victims. Additionally, there is a high turnaround time to close complaints lodged by victims of fraud and fraud money is only refunded through a court order.

11. Strengthening cybersecurity of government infrastructure: The government to strengthen the cyber security of government websites and other critical digital infrastructure and to ensure adherence to cybersecurity guidelines issued by the IT Ministry.

REFERENCES

1. Al-Zahrani, A. (2022). Assessing and Proposing Countermeasures for Cyber-Security Attacks. *InternationalJournalofAdvancedComputerScienceandApplications*,*13*(1).Advanceonlinepublication.doi:10.14569/IJACSA.2022.01301102
2. Avizienis, A., Laprie, J. C., Randell, B., & Landwehr, C. (2004). Basic concepts and taxonomy of dependable and secure computing.*IEEE Transactions on Dependable and Secure Computing*,*1*(1),11–33.doi:10.1109/TDSC.2004.2
3. Ciampa,M.(2012).*Security+guidetonetworksecurityfundamentals*.CengageLearning.
4. Gupta, M., Verma, S., &Pachare, S. (2021). An analysis of Conventional and Alternative financing—Customers'perspective.*InternationalJournalofFinance&Economics*,1–11.doi:10.1002/ijfe.2541
5. Halder,D.,&Jaishankar,K.(2021).CybergovernanceanddataprotectioninIndia:Acriticalle-gal analysis. In *Routledge Companion to Global Cyber-Security Strategy* (pp. 337–348). Routledge.doi:10.4324/9780429399718-28
6. Hong,Y.,&Furnell,S.(2021).Understandingcybersecuritybehavioralhabits:Insightsfromsituationalsupport. *JournalofInformationSecurityandApplications*,*57*,102710.doi:10.1016/j.jisa.2020.102710
7. Jha, S. K., & Kumar, S. S. (2022). Cybersecurity in the Age of the Internet of Things: An Assessmentof the Users' Privacy and Data Security. In *Expert Clouds and Applications* (pp. 49–56). Springer.doi:10.1007/978-981-16-2126-0_5
8. Le Nguyen, C., & Golman, W. (2021). Diffusion of the Budapest Convention on cybercrime and thedevelopmentofcybercrimelegislationinPacificIslandcountries:'Lawonthebooks'vs'lawinaction'.*Computer Law &Security Review*, *40*,105521. doi:10.1016/j.clsr.2020.105521
9. Penev, P. S., Atick, J. J., &Joseph, J. (1996). Local Feature Analysis: A General Statistical Theory for ject Representation.*Network: Computation in Neural Systems*, *7*(3), 477–500.
10. Feurer, M., Klein, A., Eggensperger, K., Springenberg, J., Blum, M., &Hutter, F. (2015).Efficient and robustautomatedmachinelearning.*Advances in Neural Information Processing Systems*,*28*, 2944–2952.
11. Jebaline, G.R. (2015).*S.GomathiCSE department, Francis Xavier engineering college, Tirunelveli, Tamil Nadu,"A novel method to enhance the security of ATM by using biometrics"/International conference on circuit, power and computing technologies*.