IOSR Journal of Business and Management (IOSR-JBM)
e-ISSN: 2278-487X, p-ISSN: 2319-7668 PP 15-20
www.iosrjournals.org

Digital Financial Security: Addressing Cyber Threats in The Era of Financial Inclusion

Bhawana Chand[1], Prof. (Dr.) Vandana [2], Dr. Arti Sharma[3]
[1]Research Scholar Soban Singh Jeena University Almora, Uttarakhand
bhawanachand96@gmail.com
[2]Dr. Shivanand Nautiyal Govt. Degree College, Pauri Garhwal Uttarakhand
[3]Assistant Professor, L. S. M. Campus, Pithoragarh

Abstract
In today's digital era, Financial services digitally have become more accessible, affordable and efficient. However, they are also increasingly vulnerable to cyber threats. The exposure of sensitive financial data and digital platforms creates opportunities for cyber criminals to commit fraud and phishing, often exploiting users' lack of awareness about emerging technologies. Cyber security system is crucial in current era, as it protect threats, safeguard critical infrastructure and ensuring national security. As India is the second largest digital market , vast amount of financial data available makes it a prime target for cyber-attacks. The Financial Stability Report, July 2020 published by Reserve Bank, states that the banking industry is a target of choice for cyber-attacks. It further observes that there has been an increased incidence of cyber threats in the post COVID-19 lockdown period. The study address advantages, disadvantages, challenges and future aspects of cyber security measures. The study investigate different types of cyber crimes like hackers(Black hat, White hat, Grey hat) , Malware programmes, cyber terrorism, phishing which pose significant threat to digital financial services. Artificial intelligence, humanoid robots and drones zero trust security cloud security are some advance technologies to safeguard customers interest. AI- powered threat detection enhances real- time fraud prevention, while blockchain ensures secure and temper- proof financial transactions. Quantum cryptography introduces unprecedented level of data security, and biometric authentication strengthens identity verification. The primary objective of this report is to analyse cyber security measures, identify potential loopholes, and explore ways to enhance their effectiveness in the future.

Keywords:- *Cyber Terrorism, Phishing, Artificial intelligence, Blockchain, Quantum Cryptography, Biometric authentication.*

I. Introduction

Financial Inclusion

The term " Financial Inclusion" Was first coined in 1993, although the work on this topic doesn't begin until 1998. Connecting every segment of society to the banking system is reffered to as financial inclusion. If all citizens use the financial system, a banking system can be built in a balanced fashion. In order for the economy to grow, a developed banking sector inside the financial system. (Prasenjit makur, 2023).

Financial inclusion refers to providing fair, transparent and equitable access to finance and financial services to everyone at reasonable price. Under this, the services should be available for disadvantaged people and low income groups. Thus, the main objective is to serve the basic banking services to the unreserved people in the country.

Financial inclusion is generally defined as a means of providing basic banking facilities to the population which is underserved. Financial Inclusion broadly encompasses three dimensions-access, usage and quality. The access aspect emphasize the supply of financial infrastructure and services to the people(individual, households, and enterprise) which when scaled up eases the process of mainstreaming the take up of services. (Srishti Chauhan, 2022) .

To make financial services available, accessible and affordable to all the citizens in a safe and transparent manner to support inclusive and resilient multi-stakeholder led growth. Financial Inclusion is increasingly being recognised as a key driver of economic growth and poverty alleviation the world over. Access to formal finance can boost job creation, reduce vulnerability to economic shocks and increase investments in human capital. Without adequate access to formal financial services, individuals and firms need to rely on their own limited resources or rely on costly informal sources of finance to meet their financial needs and pursue growth opportunities. At a macro level greater financial inclusion can support sustainable and inclusive socio-economic growth for all. (NSFI, 2019-2024).

During 2023-24, The Reserve Bank continued with Initiatives to deeper financial inclusion and improve credit delivery to agriculture, micro, small and medium enterprises (MSMEs), and other identified priority sectors. The composite financial inclusion Index (FI-Index) a comprehensive indicators of financial inclusion across the country, registered a year-on-year (y-o-y) growth of 6.6percent to 60.1in March 2023,with expansion across all the sub-indices.

A Financial Inclusion Dashboard- ANTARDRISHTI- was launched in June 2023 to strengthen policy insights for accessing and monitoring the progress of financial inclusion by capturing broad parameters under the three dimensions of financial inclusion, viz., Access, Usage and Quality. The Reserve Bank also conducted all India quiz on financial literacy for students of government and municipal schools across the country. (Annual Report 2023-24).

Digital Financial Inclusion

Digital Financial Inclusion involves offering digital financial services to the financially excluded and underserved populations, and using a mobile phone or other digital devices to increase access to digital financial services (Ozili, 2018). Digital Financial Services (DFS) are financial services that rely on digital technologies for their delivery and utilization by consumers. These services leverage digital platforms, such as mobile devices and the internet, to provide convenient, accessible, and secure financial solution.

Digital Financial Inclusion in India has seen a paradigm shift since 2014 with the introduction of JAM Trinity encompassing. Jan Dhan Yojana(PMJDY) for universal banking access for all, Aadhaar for unique biometric identifications, and mobile services for direct transfers. Further, the Digital India campaign launched in 2015 proved significant for roping the unbanked population into the mainstream economic system with a formal financial net that was earlier at the fringes. (Chauhan, 2022).

Digital finance has brought millions of people into the formal economy through payments, acceptance, invoice settlements, and fund transfers anytime and anywhere at their fingertips. The mobile phone and internet revolution over the last year's has penetrated the remotest of places. This has replaced cash heavy mapped to digital ID through technological innovations like net banking, mobile wallets, payment platforms, etc.

The discussion In this study contribute to the on going debate led by world Bank in support of financial inclusion as an effective solution for poverty reduction in developing countries. Insights from this article can provide national and global policymakers with an understanding of the issues associated with the rapid development of digital financial services, it's delivery to the poor and underprivileged.

Digital Financial Inclusion is described as affordable digital access to and use of formal banking services by the unserved and underserved people (Lauer and Lyman, 2025) . Digital financial inclusion refers to the internet access to use the formal financial services by excluded and underserved population (Saxena and Goyal, 2020).

In a broad sense, digital financial inclusion refers to the use of digital financial services to further the gaol of financial inclusion. It aims to leverage digital means to reach out to the financially unserved as well as underserved populations with a basket of formal financial services and products suited to their needs in an affordable, safe and transparent manner. At the same time, it promotes efficient and effective networking among participants. (BRICS Digital Financial Inclusion Report India, 2021).

More recently, the term financial inclusion has gained argument among professionals. " Financial Inclusion" focuses attention on the need to bring previously excluded people under the umbrella of financial institutions. There is no universally accepted definition of financial inclusion. Financial inclusion is generally defined in terms of exclusion from the financial system. The working or operational definitions of financial exclusion generally focuses on ownership or access to particular financial product and services. Furthermore, the definition have witnessed as shift in emphasis from the earlier ones, which defined financial inclusion and exclusion largely in terms of physical access, to a wider definition covering access to and use and understanding of products and services. (Priyanka Tandon, 2021).

Banking services are moving towards digitalization at an ever fast rate and, in developing countries economics, are increasingly being used by low income and low literacy users. As we outlined, many fintech companies are making significant progress in promoting financial inclusion thought new business models and novel products. The increasing use of technological tools such as digital identity, biometrics, internet of things Artificial intelligence and machine learning that we believe can further financial inclusion. Financial inclusion is about bridging the gap between bank and unbanked by providing affordable access to essential financial services like saving loan payments insurance and remittance to those traditionally excluded from the formal banking sector. Providing easy access to formal banking for unbanked population has become an important aspect of the development of all nations.

India has the second largest unbanked population globally, as over one 90,000,000 adults in the country lack access to financial services. The government launched the pradhanmantri jandhan yojana in 2014 with the purpose of universal accessibility of banking services at affordable rate through digital innovations and to assist in pulling a large population out of the ambit of poverty. To achieve dot targeted level of financial inclusion the Nachiket Moore committees which RBI constituted brought forward the suggestion of leveraging existing wallet and payment network to promote the unbanked.

the effect of digital finance on reliability and stability of the economy as well its side effect or guns are the main focus area of the study government international financial groups institutions (WTO IMF World Bank)are continuously promoting financial inclusion through digital platforms. despite of all these promoting innovations digital financial inclusion is not showing that much success as predicted on maybe it is due to the lack of awareness digital literacy poverty connectivity issue and diverse geographical area of India which are the major factors to the achievement of an ecommerce enable financial inclusion. this article shout to assess the various digital platforms and the risk belong to them which is one of the major reason to affect the trust of the consumers on digital platforms. das cyber fraud cyber threat are the barriers in the way of digital financial inclusion. The Government of India has always placed financial inclusion on its top list government take initiatives like pradhanmantri jandhan yojana Aadhaar mobile digital India have changed the game by ensuring that India’s under banked population has equal and economical access to financial services hence lowering income disparity.

.Since 2014 the rise of digital financial services in India has been divided into 3 distinct periods. The first phase which lasted from 2014 to roughly August 20 16 was marked by a continuous increase in volume growth on the leading digital platforms of approximately 2% per month. The second phase was mainly fuelled by demonetisation whereas the 3rd stage was fuelled by the unified payment interface rather than prepaid instruments.(source-journey map report, RBI data) .

The advancement in information technology has on negative effect on the banking sector as well as it has given rise to criminal activities such as hacking ,fraud ,and phishing. Some of the common thread involve data theft,, online fraud ,spying, use of malicious software,DDoS attacks, hacking, spamming etc. .Syber security is one of the major issues faced by digital financial service providers.. this is study focused on cyber security as a critical issue or major barriers in front of financial inclusion initiative. The concept of cyber crime and its role in hindering financial inclusion in India,, especially in rural area,, remains widely unexplored despite the rising challenges of cyber crimes, particularly among the rural population. hence the present study will determine the digital financial security and its impact of cyber crime on financial inclusion in Indian rural area.

In a landmark initiative 2 strengthen cyber security resilience in the banking financial services and insurance(BFSI) sector, Certified (MeitY), CSIRT-Fin and SISA, a global cyber security company, collaborated to launch the digital threat report 2024 for the BFSI sector. Cyber security is no longer an optional safeguard but the foundation of financial instability in the digital age. S India’s BBFSI sector rapidly expands securing digital transactions is not just a regulatory necessity but an economic imperative. It’s serves as a strategic blueprint, equipping financial institutions with the intelligence needed to anticipate vulnerability and build cyber resilience in an era of increasingly sophisticated threats.

DBFSI sector is at the heart of global digital transformation, with digital payments projected to generate 3.1 trillion dollar by 2028, accounting for 35% of total banking revenues., however, the rapid shift to digital transactions has also expanded the attack surface. For cyber criminals. The 2024 digital thread report stands apart by not only examining current threats and emerging vulnerability but also offering a deep drive into adversarial technics that impact system level operation.

With increasing digitization, cyber security has become a critical concern. Threats such as phishing, malware, data breaches, and ransomware attack jeopardize user trust and Financial stability.

Digital Financial system, while efficient, are vulnerable to risks that affect both consumers and institutions. The use of Artificial intelligence, biometric authentication, and digital identities demands a secure infrastructure. Government and international organization like the IMF and world Bank promote digital. Platforms, yet challenges persist due to poverty, poor digital literacy, and connectivity gaps.

Cyber security threats such as deep fakes prompt injection attacks, and data manipulation are growing rapidly. These emerging threats can manipulate decision making system and compromise sensitive data.

Categories of cyber attack

Malware: Malware is a common thread in the digital world and includes a variety of malicious software, design 2 cause serious damage to computer, network and server .in ransomware attack the attacker encrypts the victims data and offers are decryption Key in exchange for payment. files malware does not require attackers to install any code on the target, making it difficult to detect.

Adware: Adware ,Is software than displays or downloads unwanted advertisements, typically in the form of banners or pop ups. It collects web browser history and cookies to target user with specific advertisements users Might also download applications already corrupted with adware. Alternately, adware can be included in a software bundle when downloading a legitimate application or come pre installed on a device also known as bloatware. Like- fireball, Gator, Dollar revenue etc.

Wiper Malware : Also known as wiperware or data wiper. It is often categorized as a type of ransomeware.It aims to block access to the victim data. In destroys the data rather than hold it for or ransom. It is not for financial risk but to erase data.

Crypto jacking :Crypto jacking the process of verifying transactions within the blockchain is highly profitable but requires immense processing power.

Rootkit : A root cat is malicious software that enables threat attacker to remotely access and control a device. Root kits facilitate the spread of other types of malware including ransomware viruses and key loggers.

The first root kit, appeared in 1999 hacker defender one of the most widely Deloitte root kids of the 2000s was released in 2003.

Keyloggers: keyloggers can be hardware and software. Hardware keyloggers are mannually installed into keyboards. After a victim uses the keyboard, the attacker must physically retrieve the device. Software keyloggers on the other hand, do not require physical access. The agent tesla keyloggers first emerged in 2014.

Trojan horses : Trojan is malicious software that appears legitimate to users. Trojan rely on social engineering technique to invade device. Remote access trojan enable attackers to take control of an infected device. Once inside, attackers can use the infected device to infect other devices with RAT and create a botnet.

Bots : A not is a self replicating malware that spreads itself to other devices, Creating on network of bots or a botnet. Once infected device performs automated task commanded by the attacker. Botnets are of often used in DDoS attacks.

Anticipated cyber threats and 2025

Rise of deep fake and A I generated content

The advancement of deep fake technology enables the creation of highly realistic And manipulated audio and video content that can convincingly impersonate individuals. Deep fake voice and video allows cyber perpetrators to mimic The voices and experience of executive, employee or trusted partners.

The challenges in detection and verification of such AI generated content are significant. As the technology become more sophisticated and accessible it become increasingly difficult for users to distinguish between genuine and manipulative media.

Growing threats of supply chain attacks and Malicious libraries :

Another concerning trend is the distribution of malicious libraries distinguish as genuine. attackers publish counterfeit libraries that mimic legitimate ones, often with names that are deceptively similar to popular libraries.

Emerging threats of LLM prompt hacking in application :

Attackers may use prompt injection attacks 2 override system prompts or extract confidential data that the model has been exposed to during training. In applications like chalkboards virtual assistant or interactive voice response system, attackers with knowledge of the underlying LLM can manipulate prompts to

- Inject malicious content : Choosing the LLM 2 generate harmful or inappropriate responses that could damage the organisations reputation or lead to legal issue.
- Exfiltration : Extracting sensitive information from the model such as proprietary data or personally identifiable information that the model has been trained on.
- Manipulate decision making processes : Influencing the outputs of the LLM in way that could affect business decisions customer interaction or automated system.

Challenges post by cyber attacks on India

critical infrastructure vulnerability: India’s critical infrastructure such as power greed’s , transportation systems ,And communication network, is venerable to cyber attacks that end disrupt essential services and endanger public safety and national security.

Financial sector threats: The financial sector in India faces a high risk of cyber attacks from cyber criminals who seek to profit from stealing or extorting money. Attacks on banks, financial institutions,, and online payments system can cause financial losses, identity theft, anda loss of trust in the financial system. For instance, in March 20 20, on malware attack on the city Union Bank SWIFT system led to unauthorised transactions worth USD 2million.

Data Breaches and Privacy Concern: As India moves towards our digital economy, the amount of personal and government data stood online increases. This also increases the risk of data breach, where hackers assess and leak sensitive information. Data breaches can have serious consequences for the privacy and security of individuals and organisations., for example, in May 20 21, the personally identifiable information and test results of 1,90,000 candidates 4 the 2020 common admission test, used to select applicants 2 the I I Ms, were leaked and put up for sale on a cyber crime forum.

Cyber Espionage: cyber espionage Is the use of cyber attack to spy the interest of other countries are entities., India, like other countries, is the target for cyber espionage Activities that aim to steal confidential information and gain a strategic edge. Cyber espionage which can affect India's national security, foreign policy, and economic development.

Advanced persistent threats: advanced persistent threats r complex and prolonged cyber attacks, usually carried out by well resourced and skilled groups. These attacks are designed too infiltrate and remain hidden in the targets network for a long time, allowing them to steal or manipulate data and cause damage.

supply chain vulnerability: Supply chain vulnerability report to the weaknesses in the software or hardware components that are used by government and businesses. for their operation. cyber attackers can exploit these venerability to compromise the systems and services that depend on these components and cause widespread damage.

Government initiative regarding cyber security

- National Cyber Security Policy—This policy aims to build or secure and resilient cyberspace for citizens businesses and government. It outlined various objectives and Strategies to protect cyber space information and infrastructure build capabilities to prevent and respond to cyber attacks, And minimise damages through coordinated efforts of institutional structures, people, processes and technology.
- Cyber Surakhshit Bharat Initiative : This initiative was launched to raise awareness about cyber crimes and created safety measures for chief information security officers (CISOs) and frontline IT staff across all government departments.
- Indian Cyber Crime Coordination Centre : This and there was established to provide a framework and ecosystem for law enforcement agencies to deal with cyber crimes in a comprehensive and coordinated manners it has 7 components namely –
- National cyber crime threat analytics unit
- National cyber crime reporting portal
- National cyber crime training centre
- Cyber crime ecosystem management unit

-Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre) : this centre was launched in 2017 to create a secure cyberspace by detecting botnet infections in India and notifying, enabled cleaning and securing system of end users to prevent further infections.

- Computer Emergency Response Team – India (CERT- In) : it is an organization of the MeitY which collects, analysis and disseminate information on cyber incidents, and also issues alerts or cyber security incidents.
- Critical Information Infrastructure : it is defined as a computer resources, the destruction of which, shall have debilitating impact on national security, economy, public health or safety.

The government has established the National Critical Information Infrastructure Protection Centre to protect the CII of various sectors, such as power, banking, telecom, transport, government, and strategic enterprises.

- Defence Cyber Agency : The DCyA is a tri- service command of the Indian armed forces that is responsible for handling cyber security threats. It as the capability to conduct cyber operation, Such as Hacking ,Surveillance ,data recovery, encryption, and counter measures against various cyber threat.

Recommendation for Cyber Security Measures:

• Strengthening Existing Legal Framework – India's primary legislation in governing cyber crimes is the information technology act of 2000, which has been amended several times to address new challenges and threats., however, The IT act still has some gaps and limitations, such as the lack of clear definitions, Procedures and penalties for various cyber offences, the low conviction rate of cyber criminals. India needs to ,comprehensive and updated laws that cover all aspects of cyber security, such as ,Cyber terrorism, cyber warfare, cyber espionage, and cyber fraud .

• Enhancing Cyber Security Capabilities: India has several initiatives and policies to improve its cyber security, such as the national cyber security policy, the cyber cells and cyber crimes investigation units.

• Establish a Cyber Security Board : India must establish a cyber security board with government and private sector participants that has the authority to convince, following a significant cyber incident, to analyse what happen and make concrete recommendations for improving cyber security.

II. Conclusion

Digital financial inclusion in India has emerged as a transformative force aimed at bridging the socio-economic divide and empowering the underbanked population. The government's initiatives, such as Pradhan Mantri Jan Dhan Yojana, Aadhaar, and Digital India, have laid a robust foundation for accessible, affordable, and inclusive financial services. However, the journey toward full digital financial inclusion is not without its challenges.

One of the most significant barriers is the escalating threat of cybercrime, which undermines user trust and hinders the adoption of digital financial platforms—especially in rural areas. Cybersecurity threats such as malware, phishing, data breaches, ransomware, and advanced persistent threats pose a severe risk to individuals, institutions, and the economy at large. The growing sophistication of threats, including deep fakes and AI-driven attacks, calls for a dynamic and responsive cybersecurity framework.

India has taken commendable steps by launching initiatives like the National Cyber Security Policy, CERT-In, and the Indian Cyber Crime Coordination Centre. Yet, to ensure long-term success in digital financial inclusion, it is imperative to address legal, technological, and institutional gaps. Strengthening the existing legal framework, enhancing cyber defence capabilities, and fostering a culture of digital literacy and trust among users are critical.

In conclusion, while digital finance holds immense potential to redefine the financial landscape in India, its sustainability hinges on building a secure, resilient, and inclusive digital ecosystem. Cybersecurity must evolve from being a technical safeguard to a foundational pillar of financial empowerment in the digital era.

Reference:

[1]. Www.cert-in.org.in
[2]. BRICS Digital Financial Inclusion Report
[3]. Digital Threat Report, 2024.
[4]. National Strategy for Financial Inclusion, 2019-2024.
[5]. Data Security Council of India
[6]. India Cyber Threat Report, 2025