Global Journey of FinTech Industry alongside Cyber Attacks

Prof. Krishn A. Goyal,
Department of Business Finance & Economics & Director,
Institute of Evening Studies,
Jai Narain Vyas University, Jodhpur
Email: kag.bfe@jnvu.edu.in.

Teena Mertiya,
(Corresponding Author)
Research Scholar,
Department of Business Finance & Economics,
Jai Narain Vyas University, Jodhpur
Email: teenamertiya97@gmail.com.

Sudha Bishnoi
Research Scholar,
Department of Management Studies,
Jai Narain Vyas University, Jodhpur
Email: sudh9156@gmail.com..

Abstract

FinTech is one of the most rapidly evolving industries, affecting almost every industry. Because of its widespread coverage, it has also been exposed to a variety of threats, which is dangerous for both the organization and the consumers. Countries are incurring significant financial losses as a result of cyber attacks. Besides India is a potential victim of true digital natives both as the world's largest client of technological gadgets and as a mass internet user. This study analyzes how far the world, including India, has migrated toward the FinTech safety menace. Additionally, a wide range of security risks are being classified, and security considerations for dealing with these concerns are provided. Lastly, bring forward cyber attack-wielding strategies to make the experience less dangerous and allow the FinTech industry, particularly in India, to thrive.

Keywords: FinTech, Cyber categories, Security standards

Introduction

The evolution of technology provides an opportunity for various techno services. One among them is FinTech, which is a portmanteau word combining financial and technology. Fintech, has unquestionably become a moniker for services that claim to be mobile-first, customer-centric, but disruptive to risk-averse firms. However, the industry's coverage is still far wider, including the back offices of financial institutions, insurers, real estate brokers, and government organizations, among others. As a result of digital content availability analysis and insight development becomes easier. However, this increases the data's vulnerability to security breaches.

While FinTech firms are being stressed on numerous fronts, thinking about the consumer zone, it too has its own set of challenges to overcome. If treated as a nation, cybercrime will account third-largest economy, worth $6 trillion worldwide in 2021, trailing only the USA and China. Further criminal overheads are expected to draw near $10.5 trillion by 2025, up from $3 trillion in 2015 if rise by 15% over the next five years. This would be ten times greater than the yearly devastation

due to natural catastrophes, blighting innovative investment impulses being the heaviest redistribution of economic output (Morgan, 2021). Furthermore, Information security and privacy were cited as impediments to FinTech's growth by nearly 56 percent of respondents in PwC's Global FinTech Survey 2016.

Nonetheless, governments and economies rejig to the new norm or focus on the costs of the dilemma. Moreover, technology developers are scrambling around the clock to deliver insights that will help businesses survive and prosper. Still, Fintech is causing havoc in every corner of the planet. As per the Cyber threat Defense Report 2022, Colombia, Turkey, and Spain appear to have actively targeted businesses throughout the world. Then the most manipulated cyber-attack is crypto weakness (39.7%), cross-site scripting (12%), and system patches (8%) (Lukehart, 2022). Similarly, India facing its own set of challenges as it moves toward a technology-enabled society, fuelled by legislative provisions and emerging technologies. Which encompass cyber threats, data privacy issues, difficulty in regulations in a extensive range like fund raising, teaching, nonprofits, and threat surrounding the different types of investment management (Realising India's fintech potential: Regulation and tech must evolve, 2020).

India being a developing nation is growing more towards FinTech technology. As the world's biggest client of smart solutions and a majority of internet users, India remains a delicate destination for cyber-attacks. The object of this paper is to analyze how the world including India is shifting towards FinTech cyber attacks. In addition, numerous security dangers will be categorized, and security criteria for coping with these threats will be presented. Finally, suggest future strategies for making the setting less dangerous, such that the FinTech industry, especially in India, may prosper while safeguarding consumers and employees from cyber attacks.

Literature Review

The evolution of e-payments, which ease customer mobility, has resulted from the shift to modern or electronic payment and related services from traditional services. Security-related issues, technology transformation, data privacy and confidentiality, and e-wallets are the main focus areas (Heng, 2004).

For FinTech to gain ground, collate verification procedures. "Perceived privacy," "perceived trust," and "perceived satisfaction. It was discovered that perceived utility would be the most important factor in evaluating verification methodologies. Then it implies that personal information leakage must be considered, which boosts public trust. Furthermore, given strong criterion results, biometrics verification techniques will be particularly suitable for examining or selecting the intended audience across Fintech start-ups (Wang, 2022).

Attacks constitute prospective occurrences that undermine the authenticity of information resources, whether intentionally or unintentionally. Harnessing this knowledge necessitates a systematic process or paradigm that recognizes vulnerability. This is possible through Threat Modelling (TM) and Advanced Persistent Threats (APT) (Tatam et al., 2021).

Further FinTech has emerged as a new method of managing finances with the aid of technology. It is more advanced because it includes virtual currency, credential security etc. The Indian government has spent around $19 billion to support FinTech start-ups. From a post-demonetization scenario, the potential for FinTech in India requires a lot of awareness among the younger generation (Bhardwaj at el., 2019).

Like FinTech and banking sector services strengthening their collaboration, there are still many opportunities to grab, which necessitate properly framed rules and practices that shall be monitored to broaden its horizon. Various countries like the United States and Europe were studied, and risk-related measures for innovation sectors were proposed (Romanova, 2016).

Following the global financial crisis, there has been a tsunami surge in Fintech technological innovations, which has resulted in potential frauds and the growing need for cyber security for financial stability. The case of HKMA is examined, and future strategies for dealing with cyber security issues are suggested (Ng and Kwok, 2017).

FinTech is really not a fleeting fad. This holds the power to reinvent marketplaces, promoting innovation as well as competitive conditions. Therefore, as a serious pledge, it is becoming critical for the growth of existing mechanisms and the prospects of FinTech platforms increase consciousness of the necessity of regulative competencies in development (Choucri et al, 2014).

FinTech's expanding horizons invite a variety of security-related attacks. The existence of the fintech industry should never be left to destiny; rather, explicit strategies must shape its formation (Haddad & Hornuf, 2019). This will help with Fintech and technical financial activity to notice and thwart fraud adjacent to Fintech systems. The commandment and industry all benefit from knowing about new problems over the horizon, which aids in the development of new set of laws to look after banks and their customers (Nikkel, 2020).

Using the Petty and Cacioppo model as a moderating variable, a causal relationship between concern for information privacy and self-efficacy was established, implying FinTech services, their usefulness, ease of use, and convenience. Government deregulation of FinTech and securities issues are also important areas to focus on when establishing a FinTech platform (Kim al el., 2015).

Appropriate policy analysis and recommendations for legislative and technological improvements to detect fraud in financial transactions. Furthermore, policymakers will have a thorough understanding of the benefits and drawbacks of specific policy actions. Finally, establish a minimum standard for clients opening financial accounts, strengthen know-your-customer requirements, and regulate peer-to-peer devices. To ensure financial stability and integrity, legislators should amend the Bank Secrecy Act (BSA) to address these areas of concern (Treleaven, 2015).

Global status of cybercrime

Over the last two decades, cyberspace has expanded at a lightning pace, FinTech is providing a huge platform for the exchange of finances over Digi-tech which includes enormous services like foreign exchange, banking and payment, trade finance, and securities related to equity, bond, and derivatives. But new ways of doing business, led to the number of security incidents rising both for consumers and entrepreneurs. For instance, 71% of financial institutions view FinTech firms as a cyber security risk.

With breakthroughs in cyber venue disruption and distortion, comes the development of cyber hazards, whether by the original developers or others. Cyber threats have posed a serious threat to FinTech in recent years (Kaur and Lashkari, 2021) Figure 1 depicts the reported cyber-attacks and threats to financial institutions and banks that resulted in significant monetary losses between 2007 and 2019.

Figure 1: Shows a timeline of cyber attacks from 2007 to 2019 at the global level

Source: Reprinted from "Understanding cyber security management for FinTech: cyber security threats in FinTech" by Kaur, G., and Lashkari, A. H. (2021)

Table 1: The degree of cybercrime susceptibility in a nation

Country	Rank	Score
Finland	1	0.110
Denmark	2	0.117
Luxembourg	3	0.124
Australia	4	0.131
Estonia	5	0.134
Norway	5	0.134
Japan	6	0.138
United States	7	0.145
Austria	8	0.162
Switzerland	9	0.172
New Zealand	10	0.179
Belgium	11	0.190
Mauritius	12	0.200
Canada	13	0.207
United Kingdom	13	0.207
Spain	14	0.210
Sweden	14	0.210
France	15	0.228

Source: Global Cybersecurity Exposure Index 2020

This even suggests that cybercrime is irresistible. Every year, innumerable cyber attacks occur, ranging in value from a few bucks to hundreds of dollars. Based on the Cyber security Exposure Index (CEI), Finland is the least exposed to cybercrime out of 108 economies, while Afghanistan is the most sensitive one. Since the COVID-19 virus spread, attacks on pharmaceuticals and medical testing facilities are more prevalent. So businesses must weigh not just immediate losses, but the corporate disruption, downtime, and missed opportunities (Smith et al., 2020).

As a result of cybercrime, businesses and people may become risk-averse. But it is proving exceedingly difficult to give up digital services, specifically after the COVID curfews. While public trepidation about engaging in online activities has diminished, worries over confidentiality have intensified across countries. Here are a few examples: an IT security breach at Avon left the company's systems inaccessible for over a month, affecting operations in the United Kingdom, Argentina, Brazil, Poland, and Romania (Cimpanu, 2020). Norsk Hydro was targeted with ransomware, locking files on multiple servers and PCs across 40 countries, resulting in a loss of around $71 million (Briggs, 2019). Furthermore, the Danish transport and logistics firm Maersk, which operates container ships as well as supply vessels in over 130 nations, got hacked with the NonPetya ransomware (Osborne, 2018).

Therefore to keep up stability and development, every government needs safeguards. For example: In the wake of challenges, the United States spends massively, mostly on intelligence. By deploying advanced technologies against rising cyber threats, the US safeguards the health of the state's key pillars (Kolivand et al., 2018). End-user spending on security and risk management in the Middle East and North Africa (MENA) is expected to reach $2.6 billion in 2022, an increase of 11.2 percent over the previous year (Qadir, 2022).

The ASEAN-India Fund has taken up multiple action plans for joint work inside this domain. Reportedly, the Department of Telecom and the ASEAN Secretariat are drafting policies for a number of training programmes, notably "Cyber Forensics" or "5G and its Prospective Application" (Ray, 2022).

Further, Ng and Kwok (2017) found that the HKMA's major initiatives have been: guarding e-banking operations; systemic governance or management in partnership with the Cyber security Fortification Initiative (CFI); and setting up a FinTech innovation cluster. In that order, human capital development can be defined as gaining a better understanding of cyber risk, developing experts in this field, and taking preventative action through proactive intervention by industry and university minds.

Table 2: Cyber Risks management by HKMA

Scope	Initiatives taken	Risk management and Compliance measures	Human Capital development
Enhancing existing banking operations	Safeguarding e-banking and internet banking operations	Directives for operational enhancement of regulated financial institutions	Upgrading knowledge about embracing cyber risk
Safeguarding integrity of GFC	Systematic governance and management with CFI	Comprehensive cyber security approach	Development of future risk-management professionals for the industry
Market innovation	Establishing a FinTech innovation hub	Establishing FinTech supervisory sandbox	Preventive measures through early engagement of talents in the industry, universities, and the science park

Source: Reprinted from "Emergence of Fintech and cyber security in a global financial centre: Strategic approach by a regulator" by Ng, A., and Kwok, B. K. B. (2017)

The issue of cyber security, therefore, can be addressed at the national-international level, by maintaining a well-framed system envisaging all standard parameters both at the national and international levels. While developing a well-organized environment for FinTech development in any country one-time-password system, proper monitoring, mandatory password change from time to time, shortening long sessions i.e. reduction in access timing so that hackers get less time to attack and multi-factor or multi-phase adaptive authentication should be properly deployed.

Besides that, enterprises operate in many countries because each country's cyber security ethos and regulations differ, organizations must conduct a thorough examination of them. Numerous businesses adapted their business models in the aftermath of the existential crisis by shifting to virtual markets, and, of course, implementing security precautions is critical in such a volatile climate. The outward-looking and integrated nature of the global business hampers

sovereignty and also raises transnational concerns, necessitating the deployment of universal strategies. It is therefore recommended to choose multilevel collaboration to foster safety ethics, then should try to pull players involved on each tier along, ensuring effective communication channels between echelons (Tziarras, 2014).

How Indian Fintech responding to cyber threat

The Indian financial market has financial organisations, start-ups, cybernetic businesses, and regulatory actors. All shape the financial industry in a certain palpable fashion. India is rather well equipped for future extension and worldwide prominence in FinTech. Its first-generation businesses are achieving extraordinary results that can outperform all BigTech entities. Indeed, many start-ups are also registering for initial public offerings (IPOs), which can lend a helping hand to dawning FinTech firms to thrive. India is possibly the only country in which firms of divergent scales can cohabit as well as flourish smoothly.

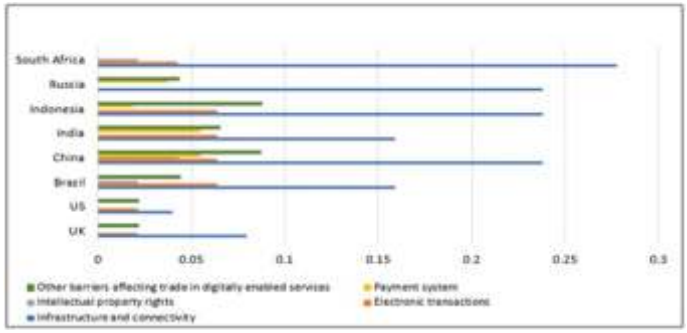
Fintech businesses have a long way to go in a rapidly changing market like India. According to the State of Indian Fintech Report, the size of India's marketplace is anticipated to jump by 31% CAGR to $1.3 trillion by 2025. Lending technology is estimated to produce 47% ($616 billion) of the total, while insurtech accounts for 26% ($339 billion) and digital payments account for 16% ($208 billion) (INC42 PLUS, 2022).

To remain competitive, FinTech firms must focus on building customer loyalty rather than just resolving technical issues (Sharma, 2020). Financial institutions and technology corporations are therefore willing to ally with FinTech firms to unleash their unique digital products. Notably, the administration, as well as agencies, continues working upon statutes or digital infrastructure to fabricate potential conduits for the FinTech value chain.

The finTech market is the future of India, keeping that in mind big players are competing for regulatory permits. While there are multiple innovative categories, such as cryptocurrency and blockchain, that are gently progressing despite having to dawdle for regulatory clarity.

WealthTech, InsurTech, never had enough momentum, now resurfaces. Other aspects, such as transactions, financing, and revenue, continue to benefit. At the same time, cyber attacks start with data leakage, service disruption, and change in payment instructions. A cyber threat can originate at the workplace, at home, or on the move while operating on a laptop, or even mobile. The main agenda of a cyber attacker is gaining money, some attackers are for fun, and some are hired by competitors to spoil others' image. This will happen through a broken process, phishing email, or a targeted technology attack which requires a lot of preparation and understanding. Previously, financial institutions used to provide services underneath a sole shade, the whole lot from banking to trading. Presently, Fintech separates these services into individual offerings.

Figure 2: Trade Restriction Index for Digital Services (2019)



Source: The Organisation for Economic Cooperation and Development, Digital Services Trade Restrictiveness Index

Therefore, India has to grow through a lot of development which makes it stronger and more compatible with handling issues related to cyber security and privacy. Currently, only 32% of the FinTech companies prioritize investment in their cyber security solution. Out of 2035 Fintech start-ups in India, only 58 focuses on Cyber security (Source PricewaterhouseCoopers, Simmons & Simmons, IOActive).

National privacy grounds are at the forefront of all global actions. That outlines a feasible strategy for tackling India's public safety concerns whilst keeping an unfettered economic atmosphere. In the context of an evolving spectrum of intrusions, the Ministry of Information Technology has opted to ban 59 applications because they

are allegedly involved in practices that are deleterious to sovereignty, integrity, and public order (Government Bans 59 mobile apps, 2020). As per the OECD's Digital Trade Service Restrictiveness Index, India's index rose from 0.21 to 0.34 from 2014 to 2019 (Mittal, 2020). Besides five key elements of the Global Cyber security Index, 2020 puts India at 10th, up from 47th rank in 2018. As it received a score of 97.5; its relative strength precincts: legal, capacity building, and global collaboration, as well as potential growth precincts: technical measures and organizational measures. Even so, the Indian government needs to offer assistance towards improving the cyber security stance.

The investment and the focus point of FinTech in cyber security are low when keeping in mind the co-relation and co-existence of cyber security and "The Right to Privacy" For each financial market, the threat & susceptibility factors shall be taken into consideration to assess the overall cyber threat. Impact of security breaches leads to financial loss, loss of customer confidence, reputational loss, intellectual property loss, and legislative breaches to legal actions about cyber law. As far as " Right to Privacy" is concerned, the past has witnessed its evolution and development through a series of rulings, culminating in the Puttuswamy v. Union of India [(2017) 10 SCC 1], where the Apex Court in a historic judgment declared “Right to Privacy” a constitutionally protected fundamental right. Further, from IT Act (2000) to the personal data bill, security and privacy laws and regulations in India have evolved over years and are being continuously strengthened.

However, the authorities lack the resources to govern cyber threats. To overcome this imbalance country can work under the PPP framework. They might form a state-wide Computer Emergency Response Team (CERT) to reinforce state-level cyber measures. At the same time establishing a securities center at the state and national levels can help along with regular cyber inspections. Even a para-cyber force, as well as an e-force, must be established alongside the regular force and coordinate with intelligence communities. In addition, to win the battle of cyberwar, higher education institutions must invest more resources in cyber specialists, maybe with the help of big corporations (Maidergi, 2020).

Suggestions regarding safeguards:

Knowledge about different threats and handling procedures- Threat literacy or threat safety knowledge should make liberal for the common man in different ways so that one can know them and tackle them according to their convenience level. Some common threats and an easy recommendation for the common public to handle them are discussed below:

a) **Phishing attack-** Phishing involves deceptive computer-based practices which swindle people into disclosing personal information sensitive. Phishing links look like forged link, that requests personal information, and traps like a logo design. One can be saved from such attacks by non-responding to such emails and links and by not providing sensitive information.

b) **Malware-** It is malicious software that aims to damage, disrupt, or gain unauthorized access to a computer system to steal its sensitive data. Virus, Trojan Horse, Spyware, Adware, Riskware, Ransomware, Scareware, and Zero-day are all types of different Malware. Ransomware encrypts files and directories on a computer to prevent users from accessing them. Another type is Riskware which is a legitimate program that can expose the device's security flaws and is used to collect data from the device and route users to malicious websites. Adware, Trojan, and Zero-day i.e. the period when the vulnerability is unknown to the users and a malicious application is created to exploit the data. One should install antivirus on their devices to get rid of them.

c) **Vishing-** Vishing is a type of voice-over-internet protocol in which a caller uses social engineering to persuade a victim to provide sensitive information over the phone. Voice calls either is real-time or recorded which attackers used for doing fraudulent transactions. One has to be alert for such types of calls and try not to respond.

d) **Smishing-** It is a criminal activity in which cell phone text messages are used to lure people to reveal personal information. A website URL could be used to capture

people's information in a text message. Message mode can be instant or forwarded. SMS of price winning is a kind of smishing attack. So whenever we receive such type of message we should block their address and can report at the same time.

Manage assets: You can't protect what you don't know, as the saying goes. Thus, first step in implementing processes recognizes your assets and effectively manages changes that allow a seamless change ensures that the organization's most valuable assets are never exposed.

Data Protection Law: Established FinTech sandboxes by RBI to evaluate the implications of technology in the sector are a step in the right direction. However, there is a requirement for a strong data protection framework in India. In this context, the personal data protection bill, of 2019, must be passed after thorough debate and deliberation.

Understanding security life cycle by the firm: Every FinTech company should develop a cyber security strategy that considers the security lifecycle, which includes identifying, protecting, detecting, responding, and recovering. This implies that the organization understands cyber security risk management, which aids in the delivery of critical infrastructure services through the implementation of appropriate safeguard mechanisms against cyber attacks.

Practice cyber security hygiene: Maintain a secure environment. The importance of basic security precautions has not waned. It is therefore recommended to choose an alpha-numeric passcode or two authentication checkpoints, for instance, a pair of fingerprints, or a face lock or pin. This includes performing security updates and changing passwords regularly, depending on the sensitivity of the repository.

Security standard: Relevant Security Standards should be considered to build a security framework by every FinTech organization are- ISO 27001:2013 Information Security, ISO 31000:2009 Risk Management, ISO 22301:2012 Business Continuity, NIST CSF NIST SP 800-53, PCI-DSS, HIPPA, IT act 2000, national cyber security policy, national information security policy (MHA), national cyber coordination center, national critical information infrastructure protection center, state CERT sectoral.

Use a defense-in-depth strategy. If one protocol or protection fails, the layered security structure ensures that other defenses continue to function. Use cloud-based solutions, identity and access management, and multifactor authentication (Choucri et al., 2014).

Infrastructure: The most important aspect of cybercrime is the protection of the support infrastructure. This is particularly true for both the electrical grid and data transmission lines. Cyber terrorism is quite often attempted on outmoded machinery. A model supporting security compliance would guarantee the revamping of infrastructure.

E-governance: Under e-governance, the authorities can serve products online. Additionally, it kind of improves coordination among governments and enterprises. The goal is to push the state of the art enough so people get more autonomy. Unfortunately, e-governance is still not actively applied in most nations.

Generate awareness among employees: Increase employee awareness and communication by giving them more power. Shift the culture toward cyber security accountability by providing training and investing in employees. By promoting cross-cultural dialogue.

Effective cyber security practices do not limit innovation. India can develop a balanced approach to technology-driven growth by keeping these and other standard cyber security principles in mind. Integrating safety from the start will result in a stronger, more efficient FinTech environment, which is better protected against threats and well-positioned for the future.

Conclusion

The speed of the digital revolution has dramatic implications for service exchange, allowing simpler cross-border service transactions that increase the value of digital information. A well-coordinated innovation strategy is expected to accelerate the growth of FinTech services. However security is an important component of FinTech solutions from the consumer's perspective, and the provider

is responsible for it. Major worldwide fears are data breaches, third-party security risks, cloud-based malicious attacks, malware risks, etc.

Security and data privacy will be critical in gaining consumer trust and catalyzing FinTech adoption in any country in the future. Looking at the global environment, it is clear that very few nations have comprehensive cyber security regulations. Nevertheless, cyber security experts are revisiting traditional security models as the industry evolves and capitalizes on the increasing computing power via Smart phones and laptops. This implies that organisational security architectures must be redesigned to account for these trends, which affect not only FinTech but also other industries and device manufacturers. Finally, the personnel that is inventive and open to ideas must be enticed, retained, and developed for cyber security tasks.

Given India's digital vision shining brightly beneath Industry 4.0, there is a large market that can be used to supplement any innovation. But a solid structure is required to address various cyberspace vulnerabilities. A significant move has been triggered by developing the National Cyber Security Strategy 2020. It will be fascinating to observe how well it remedies earlier shortcomings and builds the groundwork for a vibrant and safe digital India.

Reference

- Arner, D., Barberis, J., & Buckley, R. P. (2015), "The Evolution of Fintech: A New Post-Crisis Paradigm?" University of Hong Kong Faculty of Law Research Paper No. 2015/047; UNSW Law Research Paper No. 2016-62. Available at SSRN: http://ssrn.com/abstract=2676553
- Bhardwaj, G. N., Sinha, G., & Pal, S. (2019). FinTech and the Younger Generation. *IUP Journal of Information Technology* , Vol 15, Issue 1, PP 16-33.
- Briggs, B. (2019, December 16). Hackers hit Norsk Hydro with ransomware. The company responded with transparency. *Transform*. https://news.microsoft.com/transform/hackers-hit-norsk-hydro-ransomware-company-responded-transparency/
- Cimpanu, C. (2020, June 16). *Avon recovering after mysterious cyber-security incident*. ZDNet. https://www.zdnet.com/article/avon-recovering-after-mysterious-cyber-security-incident/
- Choucri, N., Madnick, S., & Ferwarda,J. (2017). Institutions for Cyber Security: International Responses and Global Imperatives. *Information Technology for Development* , pp 96-121. doi:10.1080/02681102.2013.836699
- Government Bans 59 mobile apps which are prejudicial to sovereignty and integrity of India, defence of India, security of state and public order, (June 29, 2020). https://pib.gov.in/pib.gov.in/Pressreleaseshare.aspx?PRID=1635206
- Heng, S. (2004). E-Payments: Modern Complement to Traditional Payment Systems. *SSRN* , Economics Working Paper No. 44. http://dx.doi.org/10.2139/ssrn.542523
- Haddad, C., & Hornuf, L. (2019). The emergence of the global fintech market: Economic and technological determinants. *Small Business Economics*, *53*(1), 81–105. https://doi.org/10.1007/s11187-018-9991-x
- INC42 PLUS. (2022). *State Of Indian Fintech Report*. https://inc42.com/reports/state-of-indian-fintech-infocus-bnpl-q1-2022-report/
- Kim, Y et al., (2015). An Empirical Study on the Adoption of "Fintech" Service: Focused on Mobile Payment Services. *Advanced Science and Technology Letters* , Vol 114, pp 136-140.
- Kolivand, H et al., (2018). Photorealistic rendering: A survey on evaluation. Multimedia Tools and Applications, 77(19), 25983-26008.
- Lukehart, A. (2022). *Cyber Attack Statistics, Data, and Trends | Parachute*. https://parachute.cloud/2022-cyber-attack-statistics-data-and-trends/
- Morgan, S. (2021). *Cyber Warfare In The C-Suite* (p. 19). Cyber Security Ventures.
- Maidergi, V. (2020, October 3). Addressing the Cyber Security Challenges faced by India. *Science Policy Forum*. https://thesciencepolicyforum.org/

articles/perspectives/addressing-cyberspace-challenges/

- Mittal, U. (2020, November 10). *A New Framework for a Secure Digital India*. ORF. https://www.orfonline.org/research/a-new-framework-for-a-secure-digital-india/
- Nikkel, B. (2020). Fintech forensics: Criminal investigation and digital evidence in financial technologies. *Forensic Science International: Digital Investigation* , Vol 33. *200908–*. doi:10.1016/j.fsidi.2020.200908
- Ng, A., and Kwok, B. (2017). Emergence of Fintech and cybersecurity in a global financial centre: Strategic approach by a regulator. *Journal of Financial Regulation and Compliance* , 25(1).https://doi.org/10.1108/JFRC-01-2017-0013
- Osborne, C. (2018, January 26). *NonPetya ransomware forced Maersk to reinstall 4000 servers, 45000 PCs*. ZDNet. https://www.zdnet.com/article/maersk-forced-to-reinstall-4000-servers-45000-pcs-due-to-notpetya-attack/
- Qadir, J. (2022, April 20). Middle Eastern CISOs work internationally to tackle security issues. *CIO*. https://www.cio.com/article/308833/middle-eastern-cisos-work-internationally-to-tackle-security-issues.html
- Qureshi,M., & Rizwi,K. (2021, November 23). The Evolution of Right to Privacy in India: A Look at the Past, Present & Future. *The Quint* .
- Realising India's fintech potential: Regulation and tech must evolve. (2020, December 7). *ET Edit in ET Editorials, India, ET* .
- Romanova, I., & Kudinska,M. (2016). Banking and Fintech: A Challenge or Opportunity? *EconPapers* , Vol. 98, pp 21-35.
- Ray, T. (2022). *An ASEAN-India Cybersecurity Partnership for Peace, Progress, and Prosperity: Report of the Third ASEAN-India Track 1.5 Dialogue on Cyber Issues*. ORF. https://www.orfonline.org/research/asean-india-cybersecurity-partnership-for-peace-progress-and-prosperity/
- Smith, Z. M., Lostri, E., & Lewis, J. A. (2020). *The Hidden Costs of Cybercrime*. McAfee Enterprise.
- Sharma, N. (2020, October 29). *FinTech in India-Challenges and way ahead*. https://www.linkedin.com/pulse/fintech-india-challenges-way-ahead-nitya-sharma
- Tziarras, Z. (2014). The Security Culture of a Global and Multileveled Cyber Security. In *Cyber-Development, Cyber-Democracy and Cyber-Defense: Challenges, Opportunities and Implications for Theory* (pp. 319–335). Springer Science+Business Media. https://doi.org/10.1007/978-1-4939-1028-1_13
- Treleaven, P. (2015). Financial regulation of FinTech. *Journal of Financial Perspectives* , vol. 3, issue 3, 114-121.
- Tatam, M., Shanmugam, B., Azam, S., & Kannoorpatti, K. (2021). A review of threat modelling approaches for APT-style attacks. *Heliyon*, *7*(1), e05969. https://doi.org/10.1016/j.heliyon.2021.e05969
- Vishwanath,S., & Bhat.A. (2020). *Security challenges in the evolving fintech landscape.* PwC Analysis.
- Wang, J. S. (2022). Verification Techniques in FinTech Compared from User Perspectives. *Social Science Computer Review*, 08944393211058310. https://doi.org/10.1177/08944393211058310