Cyber Threats and Scams in FinTech Organizations: A brief overview of financial fraud cases, future challenges, and recommended solutions in Bangladesh

1st Md. Jafrin Hossain
Department of Computer Science and Engineering
BRAC University
Dhaka, Bangladesh
md.jafrin.hossain@g.bracu.ac.bd

2nd Rejuan Haque Rifat
Department of Computer Science and Engineering
BRAC University
Dhaka, Bangladesh
rejuan.haque.rifat@g.bracu.ac.bd

3rd Mahadi H Mugdho
Department of Computer Science and Engineering
BRAC University
Dhaka, Bangladesh
mahadi.hasan.mugdho@g.bracu.ac.bd

4th Mohona Jahan
Department of Computer Science and Engineering
BRAC University
Dhaka, Bangladesh
mohona.jahan@g.bracu.ac.bd

5th Annajiat Alim Rasel
Department of Computer Science and Engineering
BRAC University
Dhaka, Bangladesh
annajiat@gmail.com

6th Muhammad Abdur Rahman
Department of Computer Science and Engineering
BRAC University
Dhaka, Bangladesh
abdur.rahman@bracu.ac.bd

2022 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS) | 978-1-6654-7327-9/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICIMCIS56303.2022.10017467

***Abstract*—The idea of financial systems has changed with the touch of applications based on information technology and came up with a new terminology called 'FinTech' (Financial Technology). With the rising technology, Fintech has become a modern phenomenon. Financial organizations deal with highly confidential and sensitive information, including personal and financial data, all of which are the primary target of cybercriminals. Users and other stakeholders are massive in number, and many are not concerned about security, so they often find themselves as victims. The result of the study shows that from the perspective of Bangladesh, most of the attacks on the fintech industry are generated using ransomware and social engineering methods. It also shows that app-based Mobile Financial System (MFS) is the most affected sector in the financial system. The study provides a comprehensive framework, FinSec, which refers to the financial Security Framework to protect from cyber-attacks targeting any financial organization. It covers recommendations for regular end-users and anybody working in the financial sector. It also provides an architecture based on Consortium Blockchain, Hyper-ledger Fabric in a hybrid cloud to ensure a high level of security at the application level. Additionally, the framework proposes newer Three-Way Authentication (3WA) and Gamification to protect end-users. The research emphasizes ensuring a minimum level of training, as even after ensuring everything, massive damage can occur for the simplest mistake of the individuals related to the industry. To protect the financial system, from end-users to employees and user applications to the whole infrastructure, everything, and everyone should be secured. The framework hence recommends three subunits – Action, Knowledge, and Simulation Unit. These subunits protect the respective sector and, finally, end up protecting the fintech organizations.**

Keywords— Cybersecurity; FinTech; Cyber Threat; Financial Scam; MFS; Cyberattack; Social Engineering; Blockchain; Hyperledger Fabric; Framework; Prevention

I. Introduction

It is hard to envisage a nation or territory without sovereignty, protecting civilians from external and internal threats. If we consider the internet world a global region, there should have protectors to save its users from malicious threats and attacks. According to Marshall McLuhan, this region is a "Global Village" based on digitalized data communication [1]. The basic building block of today's worldwide data communication system is the Internet's invention,which made it feasible [2]. All services are reliant on computer systems because of their efficiency.

The success rate for stealing money from a user's account constantly rises. The more frightening con- cern is that cybercrime actors are not satisfied with targeting just one person. They are, however, targeting businesses, banks, and even reserve funds.

When it comes to Bangladesh, it has experienced one of the biggest heists globally, losing almost a billion-dollar from the country's reserve bank in 2016 [3]. After about a few years, the nation was hit by a cyber-attack that targeted 200 organizations in 2021 [4].

In late 2011, a pioneer private bank, introduced the country's first mobile financial service, which attracted massive users within a time. However, scammers randomly targeted Mobile Financial Service (MFS) users and got the massive success that 10-12 incidents of extortion via leading app-based Service provider were recorded every day, according to the officer of a law enforcement agency in Bangladesh [5].

In 2021, so many Mobile Financial Services were introduced, and the cases rose high that they could find them accurately. The study emphasizes every aspect from the end user's perspective to top industrial infrastructure to find the best cyber-attack prevention. The research reflects that even a single mistake can open the door for attackers who may create substantial financial damage. It shows a framework for both individuals and organizations. The framework guides both pre-cautions and responses to the bad actors. So, in this era of the Internet and technology, cyber-attacks and bad actors can be dealt with by the given framework and keeping a security-centric mindset.

II. Literature Review

A. Fintech

Fintech can be described as integrating technology to automate and improve all the services offered by Financial Services Companies, including typical banks, cashless service

providers, mobile financial services, and e-money services, making it easier and faster to use daily end-users. Within the late 19th century, two distinct fields, finance, and technology, combined to deliver the introductory period of financial globalization.

After breaking the seed level of the fintech industry, the start-up which became the most successful one in this vast potential field of Fintech was known as PayPal [6]. According to Forbes, in terms of online payments, PayPal is one of the biggest service providers, with more than 377 million users, generating almost 15.4 billion in transaction costs of 1 trillion USD [7].

B. Cybersecurity

According to Burley (2017), cybersecurity refers to,

> *An interdisciplinary course of study, including law, policy, human factors, ethics, and risk management [8].*

In other words, Seemma Sundaresan, Nandhini M, Sowmiya. (2018) portrait cybersecurity as,

> *In a computing context, security comprises enterprises that use cybersecurity and physical security to save against unauthorized access to the data center and other computerized systems. Security, designed to maintain confidentiality, integrity, and data availability, is a subset of cybersecurity [9].*

C. Mobile Financial Service (MFS)

Mobile financial service refers to the App or Unstructured Supplementary Service Data (USSD) or Feature Code-based system where typical banking activities like cash-in, cash-out, payment, and transfer of funds can be made.

In the context of Bangladesh, people were intro- duced to MFS vastly by a growing venture of BRAC Bank, bKash Limited, back in 2011. International Finance Corporation (IFC) finds that bkash has more than 23 million active users and conducts around 110 million monthly transactions [10]. The success of bKash inspired other giant companies to come up with their offerings to compete with bKash. Hence, the people of Bangladesh have seen other ventures like Nagad, Rocket, Sure-Cash, and Upay.

D. Related Works

According to Prabhu, FinTech, or digital banking, has been the financial sector's most significant game-changer, and its expansion, on the other hand, represents more significant potential threat to the banking sector, considering the volume of efficient and high data stored inside it [11].

In 2018, Ioannis Agrafiotis, Jason R C Nurse, Michael Goldsmith, Sadie Creese, and David Upton showed a variety of data theft cyber-attacks on financial organizations, emphasizing the importance of understanding the propagation trends of harm so that we can predict the likely harm will be in future attacks and mitigate it [12].

Inaki Aldasoro, Jon Frost, Leonardo Gambacorta, and David Whyte proposed two solutions to cyber risk in the financial sector during Covid-19 as a growing work from home situation, the business institution has to adopt this situation as a long-term case scenario, and they have to concern about using public cloud and software is increasing [13].

In 2019, Jason Goldberg, a Barclays analyst, appeared on CNBC's "Power Lunch" and stated that the leading banking technology dangers include malware, unprotected data, and unsafe third-party service [14]. Cybersecurity risks are defined by Upguard, a ready-made platform for protecting your institution's confidential documents, as a series of fraudulent acts aimed at compromising data and disrupting the bank's electronic existence as a whole. According to Saiful, Akter, and Zahed (2017), financial fraud activities predicate offenses can be reduced primarily by observing the involvement of local criminals and their involvement with foreign networks and by implementing stringent anti-corruption measures such as digitalization and automated pro-cesses, adoption of a strict criminal identification policy, and assistance from foreign experts [15].

Joveda, Khan, and Pathak (2019), emphasized the importance of developing a conceptual framework for preventing cyber-crime in the financial industry of Bangladesh. It is essential to acknowledge how the security approaches in a financial framework potentially influence such illegal activities, consequently leading to a significant loss of economic development [16]. Hence, this study aims to develop a cybersecurity framework for identifying it.

III. Data Description

A. Problem Framing

This research expresses all the attacks on financial organizations, including mobile and regular banking. Hence, every case where end-users or organizations related to financial activities attacked attackers succeed or not is included in the dataset to create more considerable problem framing.

B. Data Collection

For this research, the research team performed multiple steps to gather information and prepare the datasets.

1) Collecting Raw Data: Raw data were collected for only the domestic context very sensitively to get an idea of the accurate picture of the problem. The research team collected raw data using Google Forms and a survey; however, the data was confidential, so the users and organizations wanted to provide them anonymously.

2) Global Data: The study uses different openly accessible datasets developed by proficient research teams. Then, the global dataset was analyzed, and it was found to specify the different cyberattack methods used in financial organizations worldwide.

3) Domestic Data: In the context of Bangladesh, there are not enough publicly accessible datasets on financial services, especially in the rising mobile financial service domain. The intrinsically confidential aspect of financial transactions leads to the lack of publicly available statistical data. So, a few financial scam information was collected about Bangladesh by creating a Google form and taking data from various authentic internet sources.

IV. Cyberattacks in Bangladesh

The financial sector of Bangladesh is vulnerable to cyber-attacks, and several doubts are being raised regarding financial institutions' precautionary action. After processing the secondary data collected from different publicly available

sources; in the following Fig. 1 it is clear that most of the attack types in Bangladesh are Ransomware.

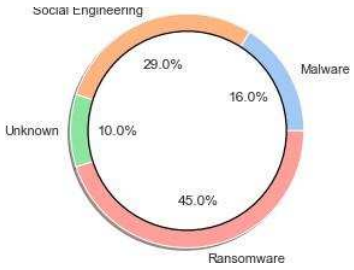

Fig. 1. Common Cyber-attacks in Bangladesh

Again, in Fig. 1, second most known types happened because of Social Engineering (29%). Then Malware is having a percentage of 16%, and 10% of total cases are still unknown.

A. Attacks on Financial Sectors in Bangladesh

The following Fig. 2 displays the cyber-attacks on various financial zones in Bangladesh.

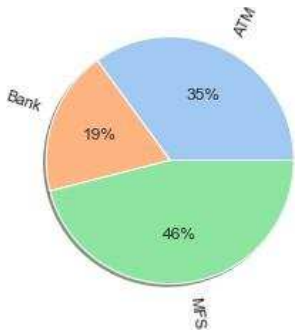

Fig. 2. Attacks on financial sectors in Bangladesh

The Fig. 2 shows that 46% of Mobile Financial Service (MFS) users have been affected by cybercriminals, and 19% of Banking organizations, and 35% of ATM users were affected due to these criminal activities in Bangladesh. Mobile Financial Service (MFS) suppliers, payment processors, and money transfer companies should be watchful for cyber threats and breaches used in electronic transfers.

B. Attacks on Mobile Banking in Bangladesh

The following Fig. 3 displays the illegal operations on mobile banking or digital payment. The survey was conducted on the mobile banking system of Bangladesh from 2019 to 2022. The Fig. 3 also shows that in the case of mobile banking, most of the criminal activities have taken place while cashing in. The second-largest money laundering occurred during cash out. Furthermore, the lowest amount of robbery took place while sending money.

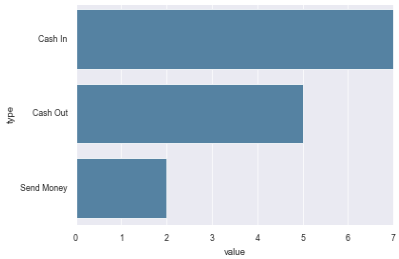

Fig. 3. Attacks on Mobile Banking in Bangladesh

V. Result and Discussion

The significant proportion of recognized incidents in Bangladesh is still unidentified, which is hugely concerning for our domestic security. Social engineering accounts for 29% of all breaches, while malware records for 16%. Ransomware accounts for 10% of all cases, while Crypto Molecular malware accounts for only 0.1%.

According to another study, many incidents focus on online services and their consumers, with most victims emerging from both industrialized and developing economies [17].

According to Babu, K. E. K, along with the modern world, the economy of Bangladesh is advancing at a fast pace, which has resulted in a strong rela- tionship with the digitalized economic system [18]. As a result, Bangladesh is also at a high risk of cyberattacks. Many incidents have already occurred on the financial instruction line in banks, corporate offices, and business institutions. Nevertheless, the primary data shows that the victim is the end-users in most cases. The study also shows that most of the attack occurs in the urban area, as the user rate is much higher than in the rural area. However, from a mobile banking perspective, most of the incident occurs in rural areas, which is about seventy percent of the total attack.

According to The Daily Star, the main reason is that the users do not know the proper use of this online system, and they do not have a fair idea of the use of Mobile Financial Service (MFS) and hacking procedures [19]. The research shows that attackers mainly use social engineering on the end-users to manipulate them in most cases. Besides, they also use Ransomware, a Malware type of attack on the business organization.

Another report in The Daily Star expresses that the matter of concern is that the organization does not know the kind of attack and how it is occurring in most cases [20]. As a result, they cannot guide their customers in systematic ways. The research team also found that, in mobile banking sectors, most of the attacks happen when the user goes for cash in their account rather than cash out and sends money, and it is an alarming scenario for Bangladesh.

VI. Solutions

A. Proposed Framework

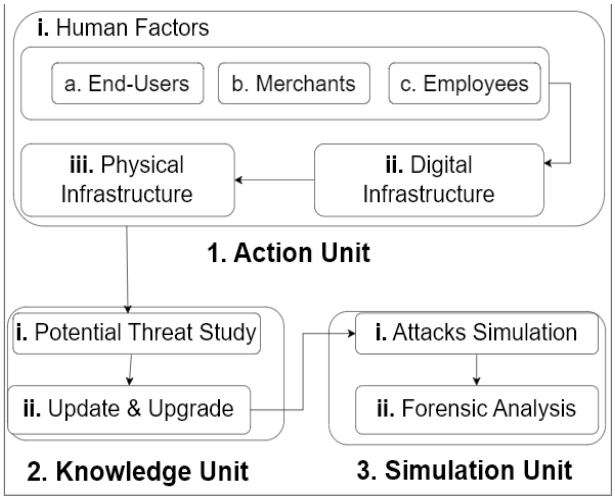

Fig. 4. Proposed "FinSec Framework"

The study provides a comprehensive framework to secure everyone related to the FinTech industry. The name of the proposed framework is "FinSec Framework," which stands for "FinTech Security Framework" shows in Fig. 4. The central diagram of the FinSec framework is added in the following section. The Fig. 4 also refers to the work process model of the Fintech Security (FinSec) Framework.

B. Short Description of FinSec Franework

There are mainly three different units in the frame- work which are sequential –

1) *Action Unit*
2) *Knowledge Unit and*
3) *Simulation unit*

Again, every unit also consists of different sub- units. The first unit, the action unit, contains three subunits – Human Factors, Digital Infrastructure, and Physical Infrastructure. Human factors also have three types of humans – End-Users, Merchants, and Employees of the financial organizations.

Additionally, the knowledge unit has two subunits named Potential Threats Study and Update and Up- grade subunits. Lastly, the simulation unit contains subunits named – Attacks Simulations and Forensic Analysis.

In terms of the work process of the framework, the action unit is the core part of the overall framework. First, the framework secures the action unit using different methodologies to secure the physical and digital infrastructure and train the Human factors.

After securing the action unit, the knowledge unit keeps researching potential threats for future cyber-attacks and update or upgrade the system according to the result.

Lastly, the simulation unit is dedicated to attacking simulation and penetration testing. Nevertheless, even after ensuring every level of security, if damage happens due to cyberattacks, a dedicated subunit forensic analysis is here to report and research the incident.

C. Action Unit

The action unit is the core part of the proposed FinTech Security Framework. If it is closely observed, it would be clear that there are mainly three major factors related to the industry. The research team says these as –

- Human Factors
- Digital Infrastructure factors and
- Physical Infrastructure factors

D. Securing Human Factors

The research team encourages organizations to adopt the existing security guidelines. However, the research team believes that the existing and proposed solutions are not enough as these have been followed for a long. Nowadays, anyone who has a trade license can register as a merchant of any app-based Mobile Financial Service (MFS) in Bangladesh. The team proposes to make sure someone has minimum ground-level knowledge to tackle common scams and frauds before registering as a merchant.

E. Securing Digital Factors

1) Three Way Authentication (3WA): To secure the end-users from the scammers and a thousand of their phishing attacks, the research team proposes a "Three-Way Authentication," 3WA, to make any successful transactions. To implement Three Way Authentication (3WA), a digital signature is required, which can be the answer to a question or a voice note, or any single word or phrase. Whenever someone opens an account, he should be asked to choose a category of digital sig- nature; then, he would input it as instructed, and the given signature will be stored in the authentication database. It is suggested to store the signature as the hash value.

The following Fig. 5 shows how Three Way Authentication (3WA) can be implemented in any application –

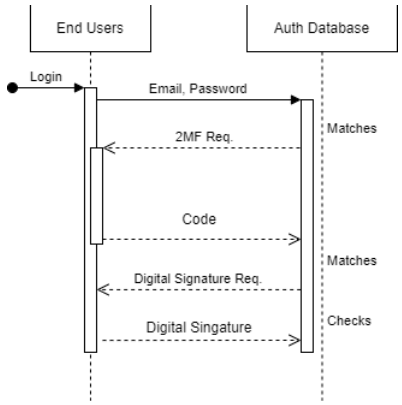

Fig. 5. Three Way Authentication (3WA)

2) Three Way Authentication (3WA) API: The research team also suggests using the previously mentioned Three Way Authentication method while requesting an API. For instance, when someone is trying to pay via a third-party payment gateway, it asks for OTP and pin-based password. The following Fig. 6 shows the final architecture of Three Way Authentication (3WA). Moreover, it would be almost impossible for an attacker to breach OTP, pin code, and the digital signature.

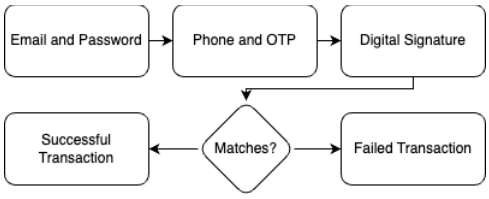

Fig. 6. Three Way Authentication (3WA) Workflow

3) Gamification: The research team proposes a gamified approach to security training for the end-users, specially Mobile Financial Service (MFS) users in Bangladesh. The following Fig. 7 shows a basic idea of gamification to secure the community. The Fig. 7 also proposed that if an end-user successfully passes the security training, Three Way Authentication (3WA) will be optional for the user.

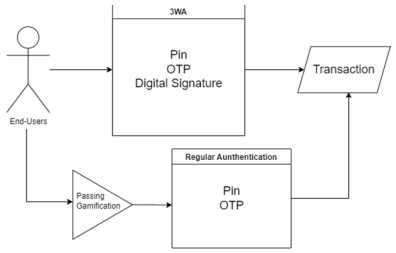

Fig. 7. Gamification to pass 3WA (Three Way Authentication)

4) Operation-Based OTP: The research team highly suggests sending "Operation-Based OTP" from the backend to the end user's mobile phone. The OTP message never says about the operation that will be done after inputting the OTP. Nevertheless, if the backend system can inform about the operation after inputting the OTP, it can also send the information on the financial activity when the OTP is required; then, the user would get a precise idea of what is going to happen after submitting the OTP.

5) Memorable Information for Third-Party Authenticator: The study finds that even though peo- ple use highly secure third-party authenticators, the application cannot assure security if the device is somehow hacked. So, the research team suggests inputting some digits from the auto-generated third-party authenticator's array of numbers. The digit's position will be dynamically asked, so any bot cannot breach the system so quickly even though it gets the code.

F. Hyperledger fabric

The key reason to choose the platform for financial organizations, as it is created on the top of blockchain and has some essential features required by any fintech organization. Again, the significant advantages of Hyperledger Fabric are discussed here, *Modular Architecture*: The most significant benefit of using Hyperledger fabric is "Modular Architec- ture". Hence, different departments of any financial organization can use the architecture to work together with data integrity and confidentiality.

Permissioned Membership: Hyperledger provides permission-based membership, which can be utilized in traditional banking systems whether someone newly creates an account.

1) According to some sources, some big giants like PayPal and Visa are using this technology. Nevertheless, the way they are using that is not available publicly because of security concerns. So, the real-world implementation of Hyperledger Fabric is already tested and ready to perform in any financial organization. In terms of Bangladesh, Standard Char- tered Bank [21], HSBC Bank [22], and Prime Bank [23] are using blockchain for LC or Letter of Credit. Upay, comparatively new MFS in Bangladesh, announced they are using blockchain in their app [24].

G. Hybrid Cloud

The risk of using only the public cloud for any financial system is alarming, as discussed previously. Again, using only a private cloud excludes getting the higher benefits of using a cloud.

Hence, the study proposes to use a hybrid cloud to build robust, secure, and comprehensive Digital Infrastructure for financial organizations. Moreover, the research team suggests keeping persistent volume and other confidential data like digital signatures and user details in the private cloud for better security purposes.

H. Physical Infrastructure

Though in the proposed hybrid cloud architecture, the security of cloud devices relies on the cloud provider; however, security of physical devices in private, on-premises cloud and all the devices of any employees are mandatory to protect from any cyber-attacks. The research acknowledges the existing security methods for protecting physical infrastructures. Moreover, the study emphasizes the following ones –

I. Securing Physical Factors

1) Authorized Vendor: It is recommended is to buy devices only from the authorized vendors, even if it is a single modem or printer for any sub-branch of the Bank. Every device's authenticity should be verified.

2) NGFW: NGFW or Next-Generation Firewalls protects devices and networks by implementing application monitoring, awareness and controls, integrated prevention, and special threat intelligence dedicated to a cloud platform. These features are not available in regular firewall.

3) NGIPS: NGIPS refers to "Next-Generation Intrusion Prevention System" which protects devices and networks from various known-unknown, zero-day threats.

4) Insider Threats: A financial company cannot make it fully secure without getting rid of insider threats, who have access to the system or critical information. Hence, the company should always keep severe concerns regarding this issue.

J. Knowledge Unit

The research team believes that it is almost im- possible to keep the security framework up to date without having a dedicated knowledge unit. Knowledge Unit consists of –

- Potential Threats Study
- Upgrade and Update

1) Potential Threats Study: Cyberattackers or scammers have colossal time to learn about different cyber-attacks outside the country. This is why the research team highly recommends establishing a dedicated team that will mainly study the trending cyber-attacks and case studies to take precautions before getting attacked.

2) Upgrade and Update: According to the outcome of the threat analysis, the research team suggests implementing an upgrade to the system. It is also suggested to update only those patches which passed all the test cases.

K. Simulation Unit

The simulation unit keeps the framework up to date by simulating attacks and researching forensic analysis. The simulation Unit consists of –

1) Attacks Simulation: One of the most significant issues with Bangladeshi Financial organizations is that few organizations have a dedicated security team. The research team highly suggests creating a secret pen-testing team to evaluate the system.

2) Forensic Analysis: While managing the vast digital and physical infrastructures and massive human factors, it is not impossible to experience damage or attacks in any portion. So, a forensic team must analyze the failures or problems and the footprint of the attacks.

The research team suggests the following Fig. 8 as a security team for every organization.

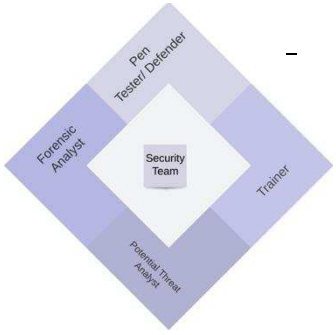

Fig. 8. Proposed Security Team

VII. Conclusion

With the revolution of Fintech, thoughts on framework for banking and other financial services has changed. Technology has reached a state where any- one can send money or make payments anywhere with a few clicks. Nevertheless, the fact is that most end-users are not always concerned about the security of their personal and financial data. Even from a professional's perspective, ensuring all the best practices to secure the system is not always possible. The study reflects all these boundaries and suggests a comprehensive and robust framework, FinSec, to keep the digital financial sector safe and prepared for cyberattacks. In the context of Bangladesh, the study especially emphasizes training people, whether he is a regular end-user or an industry personnel, as the slightest mistake can lead to substantial financial damage not only on the personal level but also directly on the national economy.

References

[1] E. Georgiadou, "Marshall mcluhan's "global village" and the internet," *Canterbury, Yayımlanmamıs¸ Yu¨ksek Lisans Tezi.*, vol. 10, 1995.

[2] L. Kleinrock, "An early history of the internet [history of communications]," *IEEE Communications Magazine*, vol. 48, no. 8, pp. 26–36, 2010.

[3] T. Desk, "When north korean hackers almost pulled off a billion-dollar heist from bangladesh bank,"The Daily Star, 06 2021. [Online]. Available: https://www.thedailystar.net/toggle/news/when-north-korean-hackers-almost-pulled-billion-dollar-heist- bangladesh-bank-2115317

[4] "Cyber attacks hit over 200 organizations including bangladesh bank, btrc," Dhaka Tribune, 04 2021. [Online]. Available: https://archive.dhakatribune.com/bangladesh/ 2021/04/02/cyber-attacks-hit-over-200-organizations- including-bangladesh-bank-btrc

[5] T. Report, "Dmp arrests 9 members of a bkash fraud ring," The Business Standard, 10 2020. [Online]. Available: https://www.tbsnews.net/bangladesh/crime/dmp- arrests-9-members-bkash-fraud-ring-146305

[6] R. Shevlin, "PayPal's Domination Of Mobile Payments Is Coming To An End," *Forbes*, 07 2021. [Online]. Available: https://www.forbes.com/sites/ronshevlin/2021/07/ 13/paypals-domination-of-mobile-payments-is-coming-to- an-end/?sh=6793da402e6d

[7] L. Hoory, "Paypal vs. venmo 2022: Which one is best for you?" Forbes Advisor, 09 2021. [Online]. Available: https://www.forbes.com/advisor/business/paypal-vs-venmo/

[8] M. Bishop, D. Burley, S. Buck, J. J. Ekstrom, L. Futcher, D. Gibson, E. K. Hawthorne, S. Kaza, Y. Levy, H. Mattord *et al.*, "Cybersecurity curricular guidelines," in *IFIP World Conference on Information Security Education*. Springer, 2017, pp. 15–16.

[9] P. Seemma, S. Nandhini, and M. Sowmiya, "Overview of cy- ber security," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 7, no. 11, pp. 125–128, 2018.

[10] I. BUSINESS CASE STUDY, "bkash ifc investment - international finance corporation," The Daily Star, 03 2021. [Online]. Available: https://www.ifc.org/wps/wcm/connect/62b9cc8b-419c-433d-bf10-e880a2559d09/bKash Builtforchangereport.pdf?MOD=AJPERES&CVID=lv1KPMb

[11] V. Prabhu, "Security Challenges Within the FinTech Sector," 05 2021. [Online]. Available: https://www.itproportal.com/ features/security-challenges-within-the-fintech-sector/

[12] I. Agrafiotis, J. R. Nurse, M. Goldsmith, S. Creese, and D. Upton, "A taxonomy of cyber-harms: Defining the im- pacts of cyber-attacks and understanding how they propa- gate," *Journal of Cybersecurity*, vol. 4, no. 1, p. tyy006, 2018.

[13] I. Aldasoro, J. Frost, L. Gambacorta, D. Whyte *et al.*, "Covid-19 and cyber risk in the financial sector," Bank for International Settlements, Tech. Rep., 2021.

[14] J. Goldberg, "Biggest Threats To Cyber Security In Banking: Safe Fintech Solutions," 05 2021. [Online]. Available: https://innovecs.com/blog/biggest- threats-to-cyber-security-in-banking-safe-fintech-solutions/

[15] M. S. Islam, S. A. Eva, and M. Z. Hossain, "Predicate offences of money laundering and anti money laundering practices in bangladesh among south asian countries." *Stud- ies in Business & Economics*, vol. 12, no. 3, 2017.

[16] N. Joveda, M. T. Khan, and A. Pathak, "Cyber laundering: a threat to banking industries in bangladesh: in quest of effective legal framework and cyber security of financial information," *International Journal of Economics and Fi- nance*, vol. 11, no. 10, pp. 54–65, 2019.

[17] Y. Namestnikov, "Cybercriminals vs financial in- stitutions in 2018: What to expect," 10 2019. [Online]. Available: https://securelist.com/cybercriminals- vs-financial-institutions/83370/

[18] K.-E.-K. (Babu), "Cyber Security in the Global Village and Challenges for Bangladesh: An Overview on Legal Context," *Cybersecurity, Privacy and Freedom Protection in the Connected World*, pp. 253–267, 2021.

[19] S. B. Report, "Bangladesh vulnerable to cyber attacks," The Daily Star, 03 2015. [Online]. Available: https://www.thedailystar.net/business/bangladesh- vulnerable-cyber-attacks-73048

[20] M. G. S. M. M. Islam, "Mobile financial services: Strengthen compliance with anti-money laundering, anti-terror financing measures," The Daily Star, 01 2021. [Online]. Available: https://www.thedailystar.net/mobile- financial-services-strengthen-compliance-anti-money- laundering-anti-terror-financing-measures-2029925

[21] M. Hasan, "Stanchart executes bangladesh's first- ever blockchain lc transaction," The Daily Star, 08 2020. [Online]. Available: https://www.thedailystar.net/business/news/stanchart-executes-bangladeshs-first-ever-blockchain-lc-transaction-1945733

[22] "Blockchain for Trade Finance," 2022. [Online]. Available:https://www.business.hsbc.com.bd/en-gb/ campaigns/innovation-digital-transformation/blockchain- for-trade-finance

[23] "Prime Bank becomes the first Bangladeshi Bank to execute interbank blockchain LC transaction." [Online]. Avail- able: https://www.primebank.com.bd/interbank-blockchain- lc-transaction/

[24] T. F. Express, "Ucb launches digital banking platform," The Financial Express, 10 2017. [Online]. Avail- able: https://thefinancialexpress.com.bd/trade/ucb-launches- digital-banking-platform-1508267168