International Journal of Engineering and Management Research e-ISSN: 2250-0758 | p-ISSN: 2394-6962
Volume-11, Issue-5 (October 2021)
www.ijemr.net https://doi.org/10.31033/ijemr.11.5.28

Cyber-Security Threats and Challenges with Third Party Banking Partners

Dr. Umar Khalid Farooqui[1] and Dr. Mohammad Husain[2]
[1]AIIT, Amity University, Lucknow Campus, INDIA
[2]Faculty of Computer and Information Systems, Islamic University of Madinah, Al Madinah Al Munawarah, SAUDI ARABIA

[1]Corresponding Author: ukfarooqui@amity.edu

ABSTRACT

Cyber-security is a key topic of research studies and discussion in recent days. Due to our ignorance and lack of information, people are susceptible to risks and vulnerabilities in their daily banking operations. Attacks like malware, spoofing, phishing, DDOS, DOS, and many others are included in cyber-attacks, which primarily destroy the customer's information. Because of the ongoing rise in digitization and the continued use of outdated cyber-security measures, attacks intensified during the COVID-19 pandemic period. This paper discusses the dangers brought on by small-scale banking partners (often referred to as third-party vendors), whether those risks were intended or not. the manner in which the issue is made known to them beforehand so that they might avoid the dangerous circumstances.

Keywords-- Cyber-Security, Third-Party, Vendors, Banking System

I. INTRODUCTION

The banking and finance industry is notorious for its reliance on third-party vendors that help provide customers with quality financial products and services. It is one of the highly interconnected sectors, which makes it one of the most vulnerable to cyberthreats and cyberattacks. Since third parties work through the banks with which they contract, any loss is the loss of the banks.

It is utmost important to remember that signing a contract with a third-party vendor doesn't mean at all that responsibility and accountability has been outsourced to the third party as well. It becomes the responsibility of the bank that how much of information is the third party prone to regarding the bank's customers, their databases their backend servers and many more.

Although there have been several data breaches over the years where third- party vendors were clearly at fault, recent events show this is happening and will continue to happen –

- April 2017 scottrade Bank admits personal data breach than 20,000 of its customers because a third-party vendor uploaded files to servers without adequate cybersecurity protections.

  (This shows how much our information is prone to cyberattacks)
- In July 2017, Italian bank UniCredit's accounts were hacked by one of its third-party vendors, exposing 400,000 customer loan accounts.
- Target Data Breach (2013) - This cyber-attack is considered to be one of the largest retail data breaches in history. Hackers gained access to Target's point-of-sale systems by using stolen credentials from a third-party HVAC vendor [1].
- JPMorgan Chase Data Breach (2014) - In this cyber-attack, hackers gained access to JPMorgan Chase's systems through a third-party vendor, resulting in the theft of personal information from over 76 million households and 7 million small businesses [2].

  (These are only the cases that are listed here and many more are still pending to be noted and listed)

So, now further in this paper "Cyber-security vulnerabilities with small scale banking partners" is going to be discussed and further discussions and conclusions will be made along with a literature survey.

Central Banking System with Third Party Vendors

II. CYBER-SECURITY APPROXIMATIONS

It is seen that total cyber-attacks in India were approximately 13L till 2022 in which banks have reported 250 cases **only of data breach**. Companies

have stated that of all the cyber-attacks approximately 15% are due to someone outside the company (in short, a third-party vendor). They exploit weak passwords and vulnerabilities in the systems that have control access. If global cyber-crimes rates continue as they are then costs will **increase 15% every year**.

- Best 34% of respondents said they were confident 0.33 birthday celebrations could inform their partners of record violations.
- 43% of respondents said their group 0.33 party control regulationand packages were regularly reviewed.
- more than half of the respondents Participants indicated that they could rely on the 0.33 celebration to inform their business while sharing information with the Nth occasion.

However, it is generally accepted that third-party vendors can be a significant source of cyber security risk for organizations. According to a 2018 study by the Ponemon Institute, 59% of companies surveyed said they had experienced a data breach from a third-party vendor in the past 12 months. Therefore, organizations must have strong security measures and processes in place to manage third-party risks and ensure the security of their data and systems.

A big jump of cyber-attacks in general of banking system was at and from the time of COVID-19, i.e., 17 November, 2019 whose main reason was the increase in digitization (UPI transactions) or highly use of public cloud storage and it is estimated that till 2025 the cyber-attacks will increase up to 43L in only banking sector.

III. LITERATURE SURVEY

The advent of a new era of banking technology has eliminated the need for a physical presence through access to electronic devices for many transactions and other banking services resulting in an increase in cybercrime.

Electronic banking services have greatly and exceptionally contributed to this prosperity as consumers have become more dependent on the Internet for the simplest monetary transactions and major financial transactions. According to the surveys, till March-2022 total cyber-attacks that took place were approximately 11,60,000 and Indian banks had cases were approximately 250. Including banking is always one step higher comparing to other industries in respect to data and information but security system is the same as in later.

For Example: - WhatsApp and imobile (one of the banking apps) and etc.

The proliferation of the online world has played an inevitable role in attracting cyber criminals who target online banking malware, as customers in India have an increasing demand for convenient access from multiple devices to conduct transactions. A 2014 study by showed that India ranks third among the countries most affected by online banking malware, after countries like Japan and the United States.

I. (Marshall, 2010) studied "Online Banking: Information Security vs. Hackers Research Paper" Banks and Savings & Loans were designated as financial institutions, and both are custodians of their customers' money, but a financial institution is even more responsible for their customers' personal and legacy data. Day-to-day transactions, such as deposits, withdrawals, balance amount, social security number, birth date, loan information, partnership agreements related to a loan, year-to-date statements, and a host of other extremely sensitive financial information are examples of information that financial institutions are the custodian of records for their commercial and personal banking customers. All of the above-mentioned records, transactions, and sensitive information are events that happen more than 50% of the time online [3].

II. According to Mahajan and Chatterjee (2019), banks have become increasingly relying in recent centuries on the latest information-based IT schemes that maintain their wealth in the type of data opposed to conventional companies, where actual money and securities are placed in a safe and secure area. Banks have become the component of internet and daily lives. It's anything but a real task to protect these bank procedures, systems from the attackers and minimize the security threats. With these Cyber-assaults increasing day-byday, and this is a challenge faced by countries and organizations like banking where data is basic. In frequency, yet in addition in complexity, cyber threats are increasing. The number of cyber security assaults is increasing and becoming progressively destructive which is targeting and broadening the variety of techniques and attack vectors. The vast majority of such incidents can be avoided by implementing adaptable counter-measures quickly and minimizing risk. The objective of this research is to develop a framework to safeguard and minimize the cyber security issue that exists in banking sector of Nepal effectively and in a timely manner before cyber security incidents become a reality [4].

III. According to a survey by Ponemon Institute, 56% of organizations experienced a data breach caused by a third-party vendor in 2020 [5].

IV. Another survey by Bomgar found that 60% of organizations experienced a security incident caused by a third-party vendor in the past year [6].

V. The same survey by Ponemon Institute found that the average cost of a data breach caused by a third-party vendor was $4.27 million in 2020 [7].

VI. In a report by IBM, the average time to identify and contain a data breach caused by a third-party vendor was 277 days in 2020 [8].

IV. MOTIVATION

Cybersecurity is a rapidly evolving field that is highly relevant in today's digital age. Students interested in technology, computing, or data security may find the topic of cybersecurity interesting and relevant to their interests.

Writing a cybersecurity research paper is a great way for BCA students to explore career opportunities in this field. By conducting research and deepening your understanding of cybersecurity issues, students are better equipped to pursue careers in information security, cybersecurity, ethical hacking or other related fields. Writing a research paper is a great way to demonstrate academic skills such as critical thinking, research, and writing.

By writing a cybersecurity thesis, BCA students develop and demonstrate their skills, leading to improved grades, scholarship opportunities, or other academic success. Cybersecurity is a subject with major societal implications. Writing a research paper on the topic helps BCA students understand how cybersecurity My motivation of writing a research paper on cyber-security came up because of my academic background, I am a student of computer science (B.C.A) including subjects such as cyber-security, networks, routing protocols. These subjects make me bend towards the era of new upcoming cyber-attacks, cyber-threats and many more in this field. Now especially choosing the banking sector is one of my personal interests. Explaining this once I had a fraud call through OLX including the payment gateway where I was supposed to accept the payment but it somehow showed that I am giving an amount of Rs.20,000 to the person on the other side after which I stopped the transaction. This made it more interesting and significant to learn about the topic and other vulnerabilities that are still left to be unturned to the public. Spreading awareness is the other side of the interest.

Indians are still on the verge thinking that cyber threats only happen through OTP's, knowing bank details, wrong links that are forwarded but they are unaware that there are many ways now advancing the cyber-attacks including the identity theft, DDOS (one of the most vulnerable), phishing, spoofing, through third party vendors (our main topic), breaking the main CBS (Central banking system as happened in the cosmos banking system).

Through this paper I want to aware the citizens of the upcoming trends of cyber security vulnerabilities and mainly their defence techniques.

V. BANKING PROCESS

A. In Indian Context

Banking processes in India have undergone major transformations over the years and digitalization is playing a key role in changing the way banking services are delivered. Here is a comparison of past and present banking processes in India, including digitization:

Account Opening Process: In the past, opening a bank account required filling out lengthy forms, submitting various documents, and then to wait a few days to receive the account number. However, with digitization, account opening can now be done online and customers can use their mobile phone or computer to complete the process quickly and easily.

Deposit and Withdrawal: In the past, bank account deposits and withdrawals required customers to visit bank branches in person. However, with the advent of digitalization, customers can now transfer, deposit and withdraw money using online banking, mobile banking or ATMs.

Loan Processing: In the past, loan processing involved lengthy paperwork, physical paperwork, and long wait times for approval. However, with digitization, loan processing has become faster and easier, and customers can apply for loans online, submit documents digitally, and get loan approval quickly.

Payments and Transactions: In the past, making payments and transactions required customers to physically go to a bank, write a check, or use cash. However, with digitization, payments and transactions can now be done online through mobile apps or using digital wallets, making the process faster, easier, and more secure.

Customer Service: In the past, customer service meant that customers had to physically visit a bank branch to have their questions resolved.

However, with digitization, customers can now resolve their queries through multiple channels including phone calls, emails, chats, and social media, making the process more accessible and convenient.

Overall, digitalization has transformed banking processes in India, making them simpler, faster and safer for customers. With the adoption of digital technology, banks can now provide a range of services from account opening to loan processing in minutes without customers needing to visit the bank in person. This has significantly improved the customer experience and made banking services more accessible to people across India.

In short this is a comparison of revolunized digitized area to old times
(Picture portraying a general it based banking system) [9]

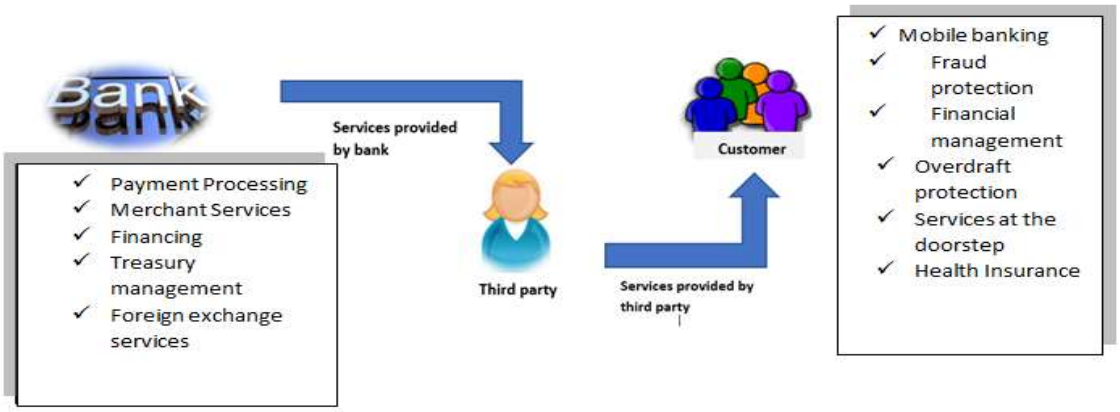
B. Role of Banking Partners/Third Party

Banking partners and third-party vendors play an important role in the banking industry by providing various services and products to banks. These partnerships allow the bank to broaden its offerings, increase its efficiency and improve the customer experience. Third party vendors make the customers feel fully satisfied by helping them at their doorstep and give them services such as loan repayment, loan services, opening any type of account (savings, current or both) as well as auditing and many others. Now from here you can imagine that how much of our information is prone to third party vendors which is sensitive and delicate. Whenever they are given any confidential work like RBI gives their auditing to the CA's or database handling at the end of each financial year they are made to sign a contract (agreement) which states that- "a confidential agreement is a contract whereby the parties involved promise not to divulge secret, confidential, proprietary or protected trade secret information".

Some significant services provided by the third-party vendors-

- Mortgage lending for loan services.
- Credit cards
- Overdraft protection
- Auditors/CA
- Brokerage Services
- Auto dealer Relationships
- Flood insurance

And many more….



Displaying the services from bank to third-party and then to the customer

C. Vulnerabilities Issues and Security Threats in Banking Operations

i. Regulatory Risks

Privacy is a key issue involving third-party vendors. Banks must comply by the regulations to protect consumer data else they will face steep fines and penalties. If a bank experiences a data breach, it's likely because they fail to comply by the data privacy regulations. This will not only affect consumers, but will also have serious national security implications.

If data is loss of their respective customers, then whole responsibility becomes of the bank itself.

ii. Reputational Damage

Working with a third-party provider sometimes means putting the reputation of the bank at risk. Aligning with the wrong vendor can lead to inconsistencies that can have an adverse effect on the banking system. Banks can also face backlash if third-party service providers obtain a negative public image due to security breaches, regulatory violations, or negative press. If banks exercise poor judgment in selecting a service partner, they risk customer dissatisfaction, unexpected financial losses and even counterblast from the public.

iii. Financial Risks

There are also various financial risks associated with working with third-party vendors. Banks and suppliers typically enter into legally binding contracts outlining performance expectations and financial obligations. But the financial situation of all sellers has an immediate impact on banking institutions. Banks may end up paying if third parties fail to meet contractual terms, take out loans beyond approved limits, or are unable to mitigate financial losses.

iv. Operational Risks

Unsecured or immature third-party providers can also expose banks to operational risk. Many banks use third-party services that integrate with their own processes. Some implement third-party services to run a program or financial product. Even the systems that control day-to-day operations are built on third-party platforms. But operations could come to a halt if internal systems are affected by a failure by a third party.

There are many other cyber threats because of small scale banking partners whether it can be intentional or un-intentional as well as there are offline threats also possible such as someone leaking the data publicly by only their words or directly by their systems etc.

Some threats which are done unintentionally include- using a common system among many individuals or sharing the same login id, password frequently or leaving the system unlocked and many other. This can lead to a very big cyber security issue to the National Security of our country.

These days now hackers become active as they know that third-party access is a weak link because third parties often get the same access as employees. That's why they target them so often. That's too much access, and the security around employee access doesn't work for all remote access. When hackers attacking third-party connections gain employee-level access, they are free to take over the network and damage the system internally.
No matter what you think of the security of third-party vendors, there are loopholes; simply granting outside access is a risk. However, third-party vendor management best practices can keep your business and data as secure as possible and without third party vendors bank management becomes a little difficult.

A SUMMARY OF THE RISKS AND THE VULNERABILITY POINTS

S.NO.	RISKS	DESCRIPTION
1	Regulatory Risks	• It refers to the possible legal and security breaches • Because third-party vendors have access to all the database so any cyber-attack that compromises system's data is considered as regulatory violation
2	Reputational Damage	• If a cyber-attack is caused from the side of third-party vendor, then bank /company is considered to be at fault • Lose of trust forever even though the bank is not at fault and then suffer a heavy loss • Moreover, in today's interconnected world a company's/bank's reputation can be weakened quickly and widely though social media platforms and other digital channels.
3	Financial Risks	• Refer to the financial loss a bank incur due to a cyber-attack that is caused by a third-party vendor. • Moreover, cyber-attacks can cause huge penalties and regulatory fines. • To mitigate this proper risk management programs are required to be in place.
4	Operational Risks	• It indicates the disruptions or failures to an organization's operations caused by a cyber-attack that is initiated through a third-party vendor. • Once the business gets disrupted then the whole system or the data gest erased and the system restarts. • Regular vendor risk assessments should be conducted so that critical systems don't get lost or attacked.

D. Existing Methods to Handle these Type of Security Issues

Defending third party vendor cyber-attacks is not easy and is a multi-layered approach which involves a combination of technical policies, security policies or confidential agreements with the companies etc. Some of them are mentioned below:

- ***Signing a Confidential Agreement (CA)***-

Many companies abide by a very strict policy/law of signing a contract with a new individual under some terms and conditions. This type of agreements generally states that whatever is the information that has been shared with the individual is not going to be shared with someone else. This is implemented in the banks as well as by the educational centres so as to secure the lectures or the study materials from their respective competitors. This type of agreement is also known as Service-Legal Agreement.

- ***Implementing Access Controls***

Access controls, such as multi-factor authentication, help prevent unauthorized access to your organization's systems and data by third party vendors. Restricting access to sensitive data and systems also reduces the risk of a data breach. Giving the access to the vendors only till the extent it is necessary like accessing the company's cloud services, databases or backend servers and many more. To counterpart this almost every big company stores its databases in approx. six to seven different geographical locations.

- ***Establishing Vendor Security Requirements***

It's important to have clear security requirements for your vendors, such as mandatory security controls, data protection standards, and incident response procedures. This ensures that the vendor has appropriate security measures in place to protect your organization's data and systems and also to keep them aware that if they are found to be involved in some type of data breach then they will be highly penalized.

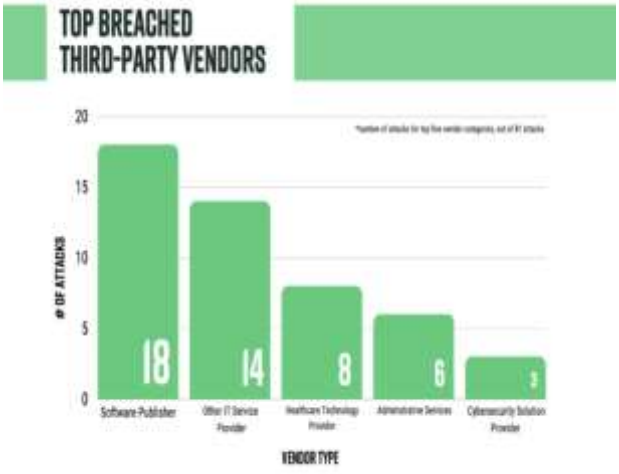
- ***Collaborate with your Vendors***

While you can never completely protect yourself against unauthorized third party access, cyberattacks, and security breaches, it's important to work with, not against, vendors to reduce risk and resolve security issues quickly. Create a friendly environment with the third-party vendors but at the same time telling them the pros and cons of a cyber-attack by a third party vendor.

By implementing the above methods, organizations have come to a point where they are now able to defend third party cyber-attacks and data breaches or tried to lessen them than in the past. More such methods are existing in this scenario and more will be introduced in the upcoming future of the Internet industry.

E. Overview of Cyber-attacks that have been Happened Since Past Few Years

According to a Ponemon Institute report, 59% of businesses have experienced a databreach caused by a thirdparty vendor or contractor. Additionally, 22% of these breaches were classified as "critical" and resulted in the loss of sensitive or confidential information. The report also revealed that the average cost of a data breach caused by a hird-party vendor was $370,000. Another report from cybersecurity firm CrowdStrike found that 18% of all cyberattacksin 2020 involved thirdparty vendors. The report also revealed that 43% of organizations experienced a databreach caused by a third-party vendor in the past year.



The Discussion section of this document focuses on the main findings and implications of the study. From the research or the topic till now we have seen that third party vendors provide us with a big help and support but at the same time they are prone to major data breach or any form of cyber-attack intentionally or unintentionally . Keeping in mind their helpfulness best method that I have personally seen is signing the Service-Legal Agreement with the company as well as providing the individual with all the procedures and standards of the work. Our findings provide you with some methods to deal with "Cyber-security vulnerabilities with small scale banking partners" and precisely more information on an untouched part of this topic i.e., the statistics. The paper further argues that discussion can play an important role in facilitating secure communication in the field of cybersecurity. However, it also highlights the challenges and limitations of using discussion as a communication tool in this context. For example, dialogue requires a high level of trust and cooperation between participants, which is difficult to achieve in practice. Additionally, the discussion may not be appropriate for all types of cybersecurity issues, especially those that require a high degree of confidentiality or sensitivity.

In a survey among random people asking about cyber-attacks (all numbers are estimated approximately)

- 77.5% respondents only heard about the cyber-attacks.
- 16.6% knew a little about cyber-attacks.
- As well as 6% of the respondents don't know about the cyber-attacks yet.

This shows an urge to conduct awareness among people of every country of the emerging cyber trends.

VI. CONCLUSION

Information technology has become the backbone of the banking system. It provides excellent support for the ever-increasing banking challenges and requirements. Currently, banks cannot think of launching financial products or creating an infrastructure of cyber security experts without the presence of information technology. However, information technology is also having a detrimental impact on our banking sector, where criminal activities such as phishing, hacking, forgery, fraud, etc. occur frequently to commit. When a person carries out any type of banking transaction on an electronic medium, it is necessary to prevent cybercrime by providing authentication, identification and verification technologies (some of the basic tools). The growth of cybercrime and the complexity of its investigative procedures require appropriate measures. According to the National Criminal Records Bureau, the number of cybercrimes in India has increased significantly over the past three years. The Indian banking sector has been doing all banking electronically since a study showed an increase in the number of payments in online banking (turning India into digitization area). However, the changes in the banking sector should suit the Indian market. The only beneficial step is "to establish awareness of rights and obligations among the people, and to make firmer and stricter the implementation of the cyberlaw to fight crime." In the fight against cyber insecurity, banks in India are also asked to maintain their attitude and be mentally prepared to deal with cybercrime and criminals on high alert. The orthodox process that runs through must be abandoned and the modern technology of the agile and aggressive combat demand system must be adopted. A review of the network security landscape and emerging threats is also required. Indian banks are the financial backbone of the country and instruments in the hands of individuals and institutions. Strong Banking Institutions / Trust The dignity of the bank should not be compromised at any cost. Now is the time for banks to move away from traditional banking frameworks and work as a team with new technologies and a new vision to eliminate or minimize cyber threats in the system. With internet penetration increasing every day. Nowadays, electronic banking transactions increased significantly. At the same time, the risk of cybercrime also increases. Internet Security is important for many reasons. First, the increase in transactions means high demands on privacy and data protection. Second, a data breach can cause enormous reputational damage to a bank. Third, correcting violations can cost a lot of time and money. Fourth, privacy breaches can do a lot of damage, and some are not just simple financial fraud. Finally, banking is different from other industries in that retains a large amount of customer data, so requires a higher level of protection. Cybersecurity is of paramount importance. Every bank is required to create it's own infrastructure to keep up with a Team(expert in cyber-security) Various protections against cyber threats exist. Firewalls, antivirus and antimalware applications, multi-factor authentication, biometrics are some of the tools and techniques that can help prevent cybercrime. A detailed security audit is required to assess the strengths and weaknesses of the system. Additionally, user education is the single most important step can take to help prevent potential cybercrime.

REFERENCES

[1] https://www.darkreading.com/attacks-breaches/target-breach-hackers-broke-in-via-hvac-company/d/d-id/1141390
[2] https://www.bbc.com/news/business-29524693
[3] Cyber security analysis in banking sector by "Neelam Sethi" published in International Journal of Advanced Research in Commerce, Management & Social Science (IJARCMSS) on July-September,2021.
[4] Importance of cybersecurity in banking by "D.S. Jana, A.E. Khedkar and C.E. Khedkar" in Vidyabharati International Interdisciplinary Research Journal 13(1).
[5] Al-alawi, P. A. I. (2020). The Significance of Cybersecurity System in Helping Managing Risk in Banking and Financial Sector. Journal of Xidian University, 14(7). https://doi.org/10.37896/jxu14.7/174
[6] Baur-Yazbeck, S., Frickenstein, J., & Medine, D. (2019). Cyber Security in Financial Sector Development: Challenges and Potential Solutions for Financial Inclusion, (November). Retrieved from https://www.findevgateway.org/paper/2019/11/cyber-security-financial-sector-development- challenges-and-potential-solutions
[7] Ojeka, S. A., Ben-Caleb, E., & Ekpe, I. (2017). Cyber Security in the Nigerian Banking Sector: An Appraisal of Audit Committee Effectiveness. International Review of Management and Marketing, 7(2), 340–346.
[8] https://www.ponemon.org/
[9] https://www.beyondtrust.com/resources/reports/
[10] https://www.ponemon.org/
[11] https://www.ibm.com/security/data-breach
[12] https://www.idfcfirstbank.com
[13] https://blackkite.com

