International Journal of Future Generation Communication and Networking
Vol. 13, No. 4, (2020), pp. 4978–4985

Cyber Security and Its Importance Due to Continuous Increase of Digital Transactions in COVID Era

Dr. K Ram Chandra[1], Dr. Madhu Singh[2], Dr. M. Padmaja[3], Dr. I. D. Soubache[4]
Dr. K.Sreelatha[5], Dr. V. Nagalakshmi[6]

[1] *Professor and Head, Department of English, VR Siddhartha Engineering College (A), Vijayawada, India*
[2] *Associate Professor Department of Political Science, RBBM College B. R. A. Bihar University, Muzaffarpur, Bihar, India*
[3] *Assistant Professor, Department of Home Science, Ch.S.D.St.Theresa's College for Women (A), India*
[4] *Associate Professor, Department of Biomedical Engineering, Rajiv Gandhi College of Engineering and Technology, Pondicherry, India*
[5] *Associate Professor, Department of Physics, Ch.S.D.St.Theresa's College for Women (A), India*
[6] *Associate Professor, Department of Chemistry, Ch.S.D.St.Theresa's College for Women (A), India*

Abstract

The world today is greatly affected in all ways due to the outbreak of the COVID-19 pandemic. The lockdown situation in many parts of the world as the result of the disease outbreak necessitated people to adopt digital payment methods in many sectors. An increased number of transactions are being carried out through the use of credit and debit cards. Several different contactless payment methods have emerged. This digital payment method also creates an increase in the number of cybercriminals. This necessitates stringent cybersecurity methodologies to protect the people. In recent years the use of public cloud services by both the general public and businesses are on the rise and this approach poses many security breaches to proliferate. Every business is likely to exchange sensitive data with customers, suppliers, and other businesses. This results in several cybersecurity-related aspects namely trust and data protection in different sectors. The technological advancements namely the Internet of Things in which all devices are connected to the Internet are supposed to pose several security-related problems shortly where the number of digital payments will be increased. This paper presents the importance of cybersecurity techniques which is very essential because of the increase in the number of digital transactions carried out in the COVID era.

Keywords— *Cyber Security, Digital Payments-Payment System, Hacking, etc.*

1. INTRODUCTION

Cybersecurity is a branch of computer science that deals with protecting Computer systems and networks from theft or damage to their hardware, software, and data. This also deals with protecting the computer from the misdirection of the services provided by them. In today's world businesses are dependent on computer systems and the Internet for many of their daily activities and due to the wide range of devices namely smartphones, televisions there is a high possibility of data being stolen by hackers to hamper the working of the business. Hence Cybersecurity is a very significant and challenging technology in the present-day world.

Due to the outbreak of the COVID 19 Viral pandemic, there is an increase in the number of cashless payments that are being carried out. The increase in the number of payment methods also gives rise to an increase in a variety of new opportunities for criminals who are interested to steal data provided for payment. These data are very valuable. This necessitated businesses to make sure that their payment security is tight and the customer is safe.

Received:
Reviewed:
Accepted:

ISSN: 2233-7857 IJFGCN

There is an urgent need to identify the various elements of cyber risk focus on the same to target those elements in building an efficient security architecture. It should be understood that cyber risks and cyber threats are not the same. Cyber risks contribute to business loss of all sorts namely financial, reputational, operational, regulatory-related losses in the digital world. It may cause damage to the operation of the equipment. In short, it may be assumed that cyber risks are a form of risk for the business. Cyber threats are the dangers that result in the potential for cyber risks. Privilege escalation, vulnerability exploitation, or phishing are considered cyber threats. Cyber threats result in fraud, financial crime, data loss, loss of system availability. In today's scenario, cyber threats are on the increase both in severity and frequency. The following diagram is a representation of the above-mentioned statement.

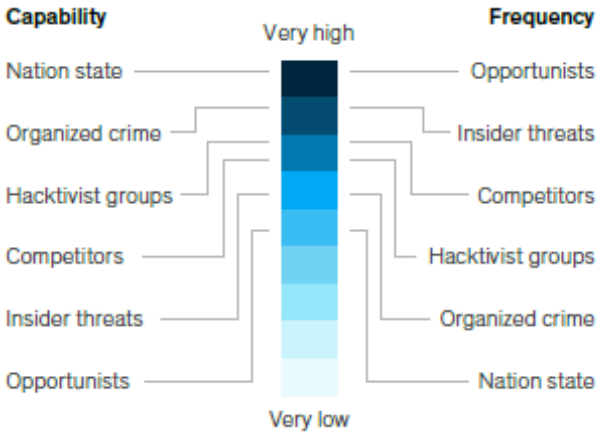


Fig. 1 Cyber Threats Study [1]

In today's COVID era building a very efficient cybersecurity mechanism in addition to the available methodologies gains a prominent place to make the people feel that their digital payments are completely safe and they can rely on the same without any botheration. This paper stresses the importance of cybersecurity mechanisms in the COVID-19 era where a large number of digital payments are being made. The paper is organized into different sections namely a section that presents a review of some of the existing literature related to cybersecurity in digital payments, a section that presents the objectives to carry out this study, a section that presents an overview of the digital payments security mechanism is addressed in which a discussion of major issues in digital payments and the security properties of the electronic payment system is presented, a section that discusses various security threats to the digital payment system and a section that focuses on Various cyber threats about Indian digital payment systems.

2. LITERATURE SURVEY

The authors in [1] present a study on the liability concerns in electronic payments in situations where security and privacy breaches occur. They stressed that the security breaches are a major disturbance to the effective functioning of the businesses. The authors discussed a few of the security breach case studies namely Target corporation's security and payment system that occurred in 2013, the cyberattack of eBay in 2014, the hacking incident of uber in 2016, and Facebook's privacy breach in 2018. Apart from the above said security breaches the authors have also discussed some other breaches. When a security breach happens, the businesses are normally made to be responsible. But the liability varies from country to country. In this work, the authors conclude that if the possibility of a security breach is high then the responsibility is imposed on the firm's side.

ISSN: 2233-7857 IJFGCN

The authors in [2] present a study on e-payment security in the context of e-commerce. They stress the purchase intentions of the customers which ultimately leads to the stealing of valuable information from the users. The data analysis is carried out using structural equation modeling using Wrap PLS. From the study, it is concluded that the ease of use of the eCommerce platforms is found to have a significant indirect effect on e-payment security through the purchase intentions of the customers.

Nowadays mobile payment is used by a large number of people and it has even become a need in present-day life. These mobile payment systems create an ecosystem ranging from regulators, financial institutions, device manufacturers, retailers to the customer. The authors in this research paper [3] uses a qualitative method to focus on the key technological factors in using mobile payments.

In recent years the use of smartphones has grown enormously. This has led to a sharp increase in digital payments throughout the world. In this regard, privacy and security are to be addressed to a larger extent. The authors in [4] make use of digital tokens as a currency equivalent value to provide privacy and security in e-payment systems. An intermediate entity is provided in the research that facilitates the transaction between the payer and payee. The strength of the system lies in building architecture on top of the existing system to protect against fraud.

3. OBJECTIVES OF THIS STUDY

This study is aimed at highlighting the importance of cybersecurity for the digital payments that are on the increase in the COVID-19 era. This study discusses various security threats to the e- payment mechanisms and cyber threats in Indian e-payment mechanisms thereby stressing the importance of building efficient security measures for digital payment systems. This study also addresses the properties of the security mechanism so that one can gain a thorough knowledge of the various aspects that need to be concentrated in building a secure digital payment system.

3.1. DIGITAL PAYMENTS SECURITY-AN OVERVIEW

In recent years particularly in the COVID-19 era, the usage of E-Wallet and online payment has grown many times. This means that electronic payment methods need to ascertain certain protection properties, namely, availability, authorization, integrity, non-repudiation, authentication, and confidentiality.

A report by Statista Fintech [5] puts forth the truth that the number of digital payments is estimated to be at 3,670,864 million euros and by 2023 there is an estimation that this will increase to 5,921,831 million euros. The e-payment systems around the world may be categorized as e-cash, e-wallet, online payment, card-based, etc.

3.2. MAJOR ISSUES IN DIGITAL PAYMENTS

Digital payment methods are a better method to make payments using the Internet. Many alterations in Digital transactions have occurred which in turn has given rise to security risks. It is not a wise idea to alter the protection of the business. Digital payments pay way to steal personal information if no proper security mechanism is built-in. Many reasons can be attributed to the security vulnerabilities that are a consequence of digital payments. The use of charge cards and providing payment details along with other private information by the clients is one major source of security vulnerability. The insecure transmission of such data leads to the stealing of information [2]. Improvements in information technologies have to be done for secure electronic payment methods. In e-commerce sites the perceived ease of use makes some customers provide their payment account details along with their personal information and this is a source of a security breach.

3.3. ONLINE BANKING THREATS

In this section let us appreciate the differences between the different security threats namely phishing, pharming, man-in-the-middle attack, man-in-the-browser, malware attacks [6], and Spoofing. Phishing may be defined to be the activity that focuses on making the users provide their personal information. This activity is performed by the way of using fake websites. The activity that

ISSN: 2233-7857 IJFGCN

involves modification of the entries in the Domain Naming service is categorized as pharming [7]. As a result of this threat, users are made to enter into incorrect websites. The valuable user credentials are made to be given by the users and in this way security breach happens. Many of the cyber-attacks that happens through the Internet is through the methods of phishing and pharming. In Man-in the middle attack hackers attempt to listen to the communication that is happening between the client and the server. The hacker comes in between the client and the server, assesses the traffic, modifies the traffic and the modified traffic is sent to the client as if it is sent by the server [8]. Man in browser attack is similar to Man in middle attack but in this case, the users are directed to duplicate sites where the user information and credentials are gathered by the hackers [9]. Spoofing is a cyber-threat where malicious actors mimic the URL of a bank's website. This website of the cybercriminal will function similarly to that of the original bank's website and by doing so the cybercriminals steal the information about the user and uses the same at a later time [10].

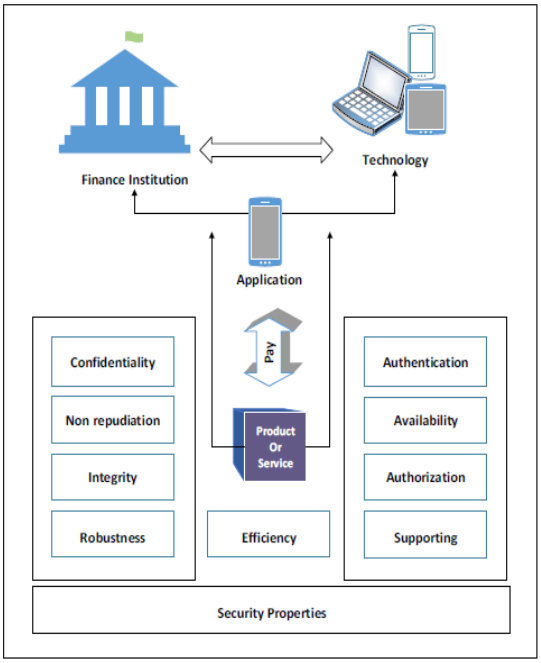
4. SECURITY PROPERTIES (ELECTRONIC PAYMENT)

Protection is a major concern in Electronic payments otherwise no one will believe that electronic payments are safe. Confidentiality, authentication, data integrity, and non-repudiation are the different properties for secure transactions [12].

It is important to ensure that only authorized customers are permitted to do electronic payments. It is equally important that only the authorized details are exchanges during the transaction. If authorization is not provided then there is a great possibility for hackers to intercept the information.[13] Confidentiality is a property that is very much essential in an e-commerce scenario as hackers can get sensitive information from people. Confidentiality is a guarantee that the information is shared only among authorized entities. That means only an authorized receiver can decode the message.[11]

Accurate information is needed by the digital payment system to prevent malfunction. Integrity [16] is related to accurate information. The information needs to be complete and authentic and should not be altered during transactions. User credentials may be taken as examples of accurate information.

The figure below is a depiction of the security properties of the Digital Payment system.



ISSN: 2233-7857 IJFGCN

Fig. 2 Diagram depicting the properties of security [16]

4.1. VARIOUS SECURITY THREATS TO DIGITAL PAYMENT SYSTEM

In this section let us have a sense of some of the security threats to the digital payment method [17]. It is accepted worldwide that 90 percent of frauds are due to the employees of an organization. These employees have excess access and privileges to the data.

Fig. 3 An illustration of Internet of Things Architecture [15]

At times of Layoff, there is a possibility that these employees hack digital payments. In the era of the Internet of Things, security needs to be tightened because all your devices from the refrigerator to toy are connected to the Internet and there is a possibility of a security breach. Changing passwords often and factory security settings can help to some extent. Encryption should not be over trusted. That is encryption may be employed as a part of the entire solution and not as the only solution. These days everyone chooses to place their data in the cloud. This migration to clod has to be done with utmost care. One must be aware of facts like what data can be put in the cloud and what data need to be omitted from the cloud. Mobile devices are used by the people in a company. Not all mobile devices are issued by the company. Non-Compliant devices can be easily hacked.

Fig. 4 Using unauthorized mobile phones [15]

Many companies allot less money for cybersecurity. Many companies underestimate the occurrence of a security breach and they give less priority to cybersecurity. This may lead to cyber-attacks. Many companies are dependent on third-party players to save the cost of the company. The primary companies in many cases trust too much on the third party companies and the third party companies are granted access to sensitive data. This process contributes much to the data breach.

ISSN: 2233-7857 IJFGCN

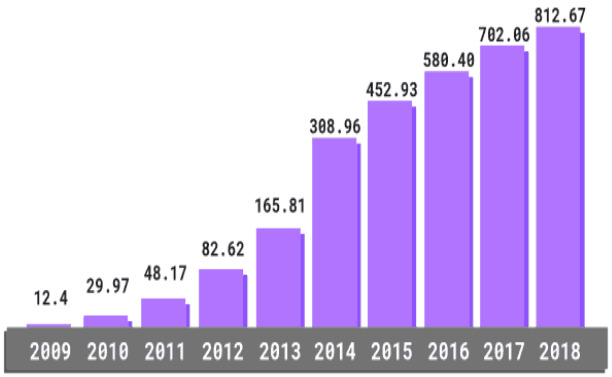


Fig. 5 Total Malware infection growth rate in millions [18]

The present-day malware is capable of tracking everything. The keystrokes can be learned, passwords can be identified, infiltrate cameras present in laptops. Even URLs are scrapped. This mandates the need for the installation of highly secure software. Also, one has to be very careful about the link you press when you are online. The following graph is an indication of the total malware infection growth rate from 2009 to 2018.

4.2. CYBER THREATS TO INDIA'S DIGITAL PAYMENTS

In this section, we present an overview of the vulnerabilities and cyber threats to the digital payment system of India. [17]. Statistics from the National Payments Corporation of India showed that digital payment services have been rapidly expanding, with UPI crossing 1 billion transactions in October 2019. Some of the initiatives that played a key role in making more number of Indians rely on digital payments may be attributed to the introduction of Unified Payments Interface, IndiaStack, Aadhar-Enabled Payment Systems, and mobile wallets [7]. Reserve Bank of India (RBI), National Payments Corporation of India (NCPI), Payment service providers (PSPs), Infrastructure Providers, and other supply-side participants are the various supply-side participants in the digital payment domain in India [19]. Here digital payments encompass both online payments and mobile payments. NEFT and RTGS transactions which stand respectively for National Electronic Funds Transfer and Real-Time Gross settlements are facilitated by RBI.NEFT and RTGS are the major Digital Transfer system mechanisms.

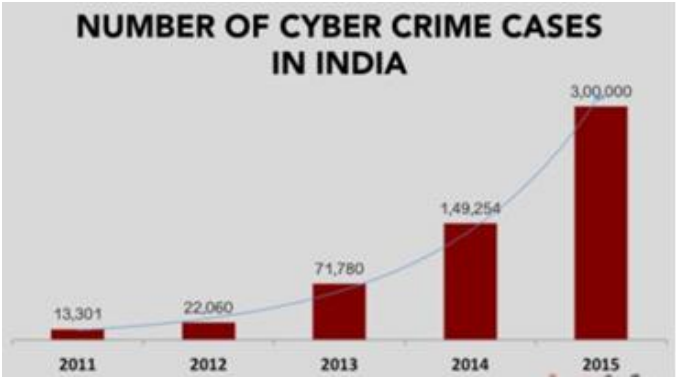


Fig. 6 Illustration of cybercrime in India [18]

NPCI looks after the retail payments methods and controls the National financial switch for ATMs. PSPs comprises of banks, payment banks, companies that provide mobile wallet, service providers that enables online payment and companies that deal with card networks. ATM networks, Point of

ISSN: 2233-7857 IJFGCN

sale providers, and mobile device providers fit into the category of Infrastructure Providers. Third-party vendors and companies that handle connectivity are grouped under other supply-side participants. An explanation of the different supply chain participants was presented to gain knowledge of the various entry points for hackers. This indirectly stresses the fact that these factors need to be kept in mind when one designs a security algorithm. The cyber-attacks have happened in various parts of the world and India is not a survivor of these. The malware attack on Hitachi payment services in 2016 made many Indian banks replace more than 30 lakh debit cards. These days' attackers are targeting individual users to gain illegal access. Union Bank of India Breach in 2016 resulted in the hackers siphoning 170 million dollars. But the bank intervened promptly and saved the bank. City union bank breach in 2018 and Cosmos Bank fraud of 2018 are other cases. The use of unsecured mobile phones, deficiency of updated systems, and lack of cyber hygiene are attributed to the vulnerabilities in the digital payment system. Cyber hygiene is using best practices when working online. Storing the data in a centralized database, the threat by insiders, and inefficient encryption are other vulnerabilities for the digital payment system. Some of the threats for digital payments are cyber-attacks, injection of malware, Distributed Denial of Service, and Man in Middle attacks. The following figure is an illustration of the increase in the number of cybercrime cases in India.

7. CONCLUSION

From the above said details about the security issues in digital payments or e-payments it is apparent that efficient cybersecurity techniques are a major challenge in the present day COVID-19 era in which the number of digital payments has increased in large numbers. Having gained significant knowledge about the growth in the security threats every year it is imperative to build more secure architectures for digital payment systems. Businesses need to invest much in the security aspects in such a way that the user is safe to use digital payments. Apart from building secure software architectures and protocols, it is equally important to educate people about cyber hygiene and they must be trained to use the Internet safely. Particularly in countries like India where digital payments have increased in huge volumes due to the COVID-19 Pandemic educating the people about cyber hygiene is of paramount importance. These could reduce cyber risks to a considerable amount.

REFERENCES

[1] Chun S.H "E-Commerce liability and Security breaches in mobile payment for e-business sustainability", 2019.

[2] Ardianash, M.Chariri, A.Rahardja, S.Udin. "The effect of electronic payments security on e-commerce consumer perception: An extended model of technology acceptance", Management Science Letters

[3] Karsen.M, ChandraY.U, Juwitasary H "Technological factors of mobile payment: A systematic literature review". Proceedings of Computer Science, 2019.

[4] Rajendran B, Pandey A.K, Bindhumadhava B.S. "*Secure and Privacy-Preserving Digital Payment*". Proceedings of the 2017 IEEE Smart world Ubiquitous Intelligence and Computing. Advanced and Trusted Computed, Scalable Computing and communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation San Francisco, CA, United States of America, August 2017

[5] Handelsblatt Statista Fintech Report. "*Digital Payments"*, 2019

[6] Mahmadi F.N, Zaaba Z.F, Osman. A, (2016)." *Computer Security issues in Online Banking: An Assessment from the context of Usable Security"*. IOP Conference in Material Science Engineering.

[7] Eriksson, M. "*An Example of a Man-in-the-middle Attack Against Server Authenticated SSL-sessions"*, International Conference on Applied Cryptography and Network Security, 2003.

[8] Cain C. "*Analysing on man in the browser attack". SANS* Institute InfoSec Reading Room pp.1-23,2014.

ISSN: 2233-7857 IJFGCN

[9] Sidharth Deb., "*Towards a cybersecurity Roadmap for Digital Payments: Best Practices and Recommendations*".

[10] Ashish M.Shaji(Jun 17 2 020). "*Cyber Security in Digital Banking: Threats, Challenges and Solution.*" enterslice.com

[11] Breshkovsky's (2016). "*The Future of the Mobile Payment as Electronic Payment System"*, European Journal of Business Management, Malone, T. W. (1984). *"Toward a theory of intrinsically motivating instruction",* In D. F. Walker, & R. D. Hess, Principles and perspectives for design and use.

[12] Kang J. *"Mobile Payments in Fintech environment: Trends. security, challenges, and services"*.Human-Centric Computer Information Science.2018.

[13] Karim N.A, Shukur Z. "*Review of user authentication methods in online examination"*.Asian Journal of Information Technology, 2015.

[14] Gene Scrieven (April 26, 2018). "*The 12 biggest security threats to payments",* Fraud Management, Bill Pay, Payments and Industry Trends, Verizon Data Breach Investigations Report

[15] Sameer Patil, Sagnik Chakraborty(16 Jan 2020), *"Growing Cyber Threats to India's digital payments",* Gateway House: Indian Council on Global Relations.

[16] "*Cyber Security Statistics, The Ultimate List of stats, Data & Trends*", purplesec.us, 2020.

[17] Sameer Patil, Sagnik Chakraborthy *"Cyber Security Agenda For India's Digital Payment Systems"*.Gateway House., September 2019.

[18] Assocham(Jan 2015), Mahindra SSG Report.

ISSN: 2233-7857 IJFGCN