# A ROBUST MOVE TOWARDS DIGITALIZATION, THREATS AND SOLUTIONS

K. Vinitha[1], Dr. S. Vasantha[2]
[1]Ph.D. research scholar, School of Management studies, Vels University, Chennai, India.
[2]Professor& Research Supervisor, School of Management Studies,
Vels University, Chennai, India.

**ABSTRACT**

**The Digital India programme is an interstellar programme of the Indian Government with a dream to transform India into a digitally empowered society and knowledge economy. "Faceless, Paperless, Cashless" is one of a sworn role of Digital India. The robust move towards cashless economy paved a way for digital payments. Numerous aspects led to the growth and propagation of digitalisation Some of the aspects include: Swelling mobile phone penetration, Economical service delivery, and the most vital one demonetisation. The growth of digitisation has led to the path for cyber crimes also to boost simultaneously. As many as 11,592 cases of cybercrimes were reported across India in 2015. Apart from the initiatives put forward by the Indian Government towards Digitalized transactions consumers are still sceptical about safety and security issues, they are concerned about their data, that chances of it being hacked or attacked by virus are there and hence they step back. This paper highlights the analysis of some of the cyber attacks and prevention to them in relationship with fraud vulnerability, and determine how this relationship affects or boosts the confidence of the users. The aim is to provide the users information that sheds light on key aspects of safeguarding their relevant data being hacked. The findings are based on various news reports and references from websites which provides solutions to the issues and recommends secure measures against cyber hacking.**

**Keywords: cyberattacks, cyber crimes, Digitalization, Hacking.**

## INTRODUCTION

The network of networks which is the "Internet" acts as the medium of cyberattacks which are done with social or political motive. Attacks aims the public or national and corporate organizations and are transmitted through the spread of malicious programs (viruses), unauthorized web access, fake websites, and other means of looting personal or institutional information from targets of attacks, causing far-reaching damage. Cyber attacks include cyber terrorism, cyber warfare, and cyber espionage. Technologies which are designed to safeguard the networks, systems, programs and data from attack, destruction or unauthorized access is termed as cybersecurity. The goal of cyber threats can be stated to be the most troublesome form which targets at confidential, political, martial or infrastructural wealth of a country, or its citizens. Thus we can say that Cybersecurity[15] plays a vital role in any Government's security strategy. For instance we can take U.S. federal Government which has granted over $13 billion annually to cyber security since late 2010. The demonetisation move by the government has threw a mass effort to create India starts using maximum digital payments instead of cash. Initiatives put forward by India Government includes unified payment Interface(UPI), e-wallet, cards, Aadhaar-enabled payment system, Unstructured supplementary service Data(USSD) [5] .

## METHODS

The findings are based on various news reports and references from websites which provides solutions to the issues and recommends secure measures against cyber hacking. News reports

and reviews indicates people to go through many digital payment related issues and how you can attain solutions for the same, so that you can indulge in transactions without any fear of hacking by gaining more knowledge about the technology.

## REVIEW OF LITERATURE

Princewill Aigbe and Jackson Akpojaro [17] in their study observed a complete review of the various sorts of electronic payment systems in terms of online payment processes, authentication mechanisms, and authentication types. The application of the different authentication mechanisms and the categories of the electronic payments system is highlighted in the study. The final results threw light that electronic payment systems with authentication mechanisms which involves two or more than two factors inclined to give optimum security, minimum fraud vulnerability, and boost users' confidence in using electronic payment systems. Ajeet Singh et., al [1]observed that the Digital payment system should be secure for Internet transaction contributors such as Payment gateway server, Bank sever and Merchant server. The security construction of the system is designed by using many Security Protocols and techniques, which eliminates the scam that occurs today with pilfered credit card/debit card payment information and customer information. Electronic commerce comprises of exchange of some form of cash for goods and services over the Internet but today, Internet is an uncertain and untrustworthy media. The asymmetric key cryptosystem Methodology with help of Security Protocol, secure communication tunnel techniques can protect conventional transaction data such as account numbers, amount and other information.

Theodosios Tsiakis, George Sthephanides,[19] analysed the security and trust issues that are essential for every electronic payment mechanism inured to be accepted and established as a common medium of financial transactions. Security regarding electronic payment is categorized into three areas Systems security, Transaction security, and legal security. Three basic building blocks of security mechanisms are used: Encryption, Digital signatures, Checksums/hash algorithms. Cryptography and Public key cryptography which ought to be trustworthy to generate confidence in the use of information and communication systems.

## OBJECTIVES

1. To analyse the various incidents of cyber-attacks happened in India.
2. To provide suggestions for secured measures to be taken to safeguard data from cyberattacks.
3. To analyse the reasons behind the reluctance of accepting Digital payments
4. To find out the steps taken by the Government to encourage Digital payments

### Incidents of cyber attacks

According to a report published in THE ECONOMIC TIMES [3] on 13th May 2017 A group of Indian companies were hit by the ransomware Wannacry as a massive cyber-attack has infected PCs across 99 countries. Two south Indian banks, two Delhi based Indian manufacturing companies, one manufacturing unit of a MNC, corporate headquarters of a Mumbai-based conglomerate and a Mumbai-based FMCG company were hit by the malware [7] in India. More than 100 PCs of Andhra Pradesh police were also hit. It is found that the attacks are intended to cause disruption and financial gain. Those PCs which doesn't have a patch to prevent the malware will be infected and once infected it spreads quickly. The next step of ransomware is that it locks down the PCs and the encrypted data on computers insist for payments to re-establish access.

The Reports on Reuters [16] published in 28th June 2017 that India's largest container port got disrupted by global cyber-attack. India s' largest container port Jawaharlal Nehru port near the commercial hub of Mumbai was hit by the Petya ransomware attack, the functions at one of three terminals got disrupted. The affected terminal is operated by Danish shipping giant AP Moller-Maersk, reported that the attack had triggered outages in its computer systems globally. Customers were informed that the vessel operations at the terminal had got affected. Due to the impact, the containers got piled up outside the port because of the delay in loading and unloading at Gateway Terminals India.

The Economic Times reported [4] on 14th May 2017 that the cyber attackers haunt 70 per cent of ATMs in India. A malware named Wanna Decryptor or WannaCry was used for carrying International cyber-attack. This ransomware locks the system by encrypting the data on it, you can grant access after releasing a bulk amount.

The most pathetic fact is that the outdated Windows XP version which is the weak link is used by most ATMs in our country. Their control is vested with vendors who render banks with the said systems. In 2014 even Microsoft halted providing support-security patches and other tools for Windows XP. But after the cyber-attacks which frequently haunts the ATMs in our country Microsoft reported it had released updates for Windows XP, Windows 8, and Windows Server 2003.

As per the reports of Zee news on 9th June 2017 Ransomware [12] has attacked SMS hospital in Jaipur due to the disruption on the online system of the hospital a wide range of services, like the registration, blood test and lab reports were affected. As per the report of the hospital staff, the day began in normalcy but the systems stopped functioning all of a sudden. Later the IT team investigated the situation and found that it was a ransomware virus attack. The situation affected many patients as they had to leave the hospital without getting treatment. However, the IT team, reported that the files in most computers were not corrupted even though the access to them were denied.

On 28th Dec 2016 The Economic Times reported Debit card hack which resulted in the loss of Rs 1.3 crore nearly 32 lakh debit cards which belongs to various Indian banks were compromised in the massive hack transaction as per NPCI (National Payment Corporation of India). Reports said that ATMs operated by Japanese Hitachi payments were hacked with malicious software allowing hackers to pool money from consumer accounts.

**Suggestions for secured measures to safeguard data from cyberattacks**[9]

- ***Secure with End Security*** [11] – End security is the process of safeguarding the corporate network when retrieved through remote devices like laptops or other wireless and mobile devices. Each device with a remote connecting to the network generates a potential entry point for security threats. Endpoint security can safeguard web browsing, control outbound traffic, shield system settings, proactively halt Phishing attack which means to procure relevant information like usernames, passwords, and credit card details (and, indirectly, money), frequently for spiteful reasons, by concealing as a truthful unit in an electronic communication and continuously observe for irregular system behaviour. And thereby it will give assurance for safeguard of servers, laptops, tablets, and mobile devices.
- ***Uphold Backups of relevant data***[13] – Backups of data is essential to safeguard the data from ransomware, malware, theft, fire, inundation, or accidental deletion. The task didn't end up with data protection alone but the data protected need to be translated into a confidential code which is called as encrypted data. To go through an encrypted file, entry to the confidential key or password that provides you to decrypt it is essential. Until it is not encrypted it is called as plain text and the data which is converted into encrypted data is called cipher text. If the Backups are stored in an offsite location it will assure you the protection of data.
- ***Avoid Anonymous emails or messages*** – An alert user should be away from anonymous email attachments and phishing attacks. As the ransomware variants used to hack your system through dubious emails. Extreme alertness in handling these dubious emails will prove to be an effective way in battling ransomware attacks.
- ***Patching of system is vital*** – Hackers can easily attack the systems which are not patched. Once the system is patched it should be kept up to date. WannaCrypt vulnerability patch was available since March but the slack approach of the users used to put them in trouble. But the reality is that systematic testing should be done on time.
- ***Avoid Macros if possible*** – Microsoft office documents also acts as an intermediary for ransomware attacks, the users get hoaxed to enable macros. There are various tools which bound the functionality of macros by restricting them from being access to the files downloaded from the internet.
- ***Be cognizant and wary*** - Conducting an information security awareness program plays a pivotal role in enlightening security. Even subscriptions to mailing lists will deliver information on common vulnerabilities and exposures. Thereby the common assumption that only tech savvies have the knowledge on all the recent malware and trends can be rectified.

**Reasons behind the reluctance of accepting Digital payments**

In order to make digital payments, smart phone is required. India's smart phone number is around 25 crores. So, most users will not be able to shift all of a sudden. Tech support is not robust enough to support even the existing number of cards -some 26 crore credit cards and 69.7 crore debit cards.[20]. Another deterrent to a mass move to cashlessness is upgradation needed at the end of banks and payment gateways. Some people fear of using net banking. Some people feel scary[10] that using their computer for internet banking will lead them to obsess over money[14]. They feel that if the information is available to them always, they will have a hard time ignoring it. They think they will be consumed about every little thing that is happening with their account. The other fear is that they think that only written proof transactions will be secured for proof even though you can print out the transactions.

**Steps taken by the Government to encourage e-payment**

In a big drive to encourage online transactions and e-payments, Our Prime Minister Narendra Modi has announced removal of service charge and surcharge applicable on cashless payments. This is also a move towards eliminating parallel economy[19] as the use of digital transactions will be transparent for the authorities to suggest if the individual or a company are on the income rolls of the Government or not. And there by the major cause also gets fulfilled by doing so which forms a paradigm shift from physical transaction to virtual transactions. In fact, the government was encouraged to undertake by coming to know that electronic payment methods have accounted for more transactions in India than the traditional methods like drafts, and cheques. This was a green signal to government's plan to provide incentives for virtual transactions in the country. Besides, more cashless payments will convert to higher tax payments and more financial inclusion[17]. The Central Government has declared incentives and measures to encourage Digital payments by making use of credit/debit cards and mobile phone applications/ e-wallets etc. Banks and Prepaid Payment Instrument (PPI) not to levy any charges on customers for transactions upto ₹ 1000 made through Immediate Payment Service (IMPS), USSD-based *99# service and Unified Payment Interface (UPI) systems from 1st January 2017 to 31st March 2017. Lower rate of Income Tax on digital turnover (from 8% to 6%) for small businesses under Section 44AD of Income Tax Act, 1961. Oil Marketing Companies, viz Indian Oil, BPCL & HPCL have offered a discount of ₹ 5/- on every LPG refill to all LPG customers who make use of Digital transactions. Dated Inorder to give assistance to the users 14444 Toll-Free Helpline for Digital Payments.

## DISCUSSION

Prime Minister Narendra Modi[8] addressed the nation on 25th December, Christmas Day, with his 27th and final edition of 'Mann Ki Baat' for 2016. Inorder to promote mobile banking and e-payments he launched two short-term schemes – Lucky Grahak Yojana and Digi Dhan Vyapaar Yojana for customers and traders alike. He narrated the difficulties crossed by the people due to the ban of legal tender notes and also he described the benefits of Digital economy. Since the currency swap was announced on November 8, according to Reserve Bank of India data there has been a strong growth in digital payments and transactions. Digital transactions have amplified and expanded in volume and value across various modes from wallets to cards and interbank transfers from a year earlier. Card transactions at point of sale (pos) terminals at merchant locations have surged, reflecting a positive for the economy as more people start using their debit cards for payments rather than for withdrawing cash at ATMs [6].

## RESULTS

The findings of the study after reviewing various literatures, websites, news reports reveal that electronic system with a higher number of authentication factors may have higher secure level. Beyond all the existing security features it is in the part of the users to act prudently with his own system and while using the so called "network of networks" it ensures the safety of relevant data by following the above mentioned secured measures against cyber-attacks.

## CONCLUSION

Technology keeps on changing day by day which aids financial services and commerce industry. Today's world running with shortage of time we need all the transactions within a split of second and assured with security. It is understood that e-payment system comes with lot of advantages

but along with lot of security issues. E-payments systems should have trustworthy and safe methods to authenticate their customers thus reducing the intrinsic risks. The level of authentication used should be appropriate to the risks associated with them. And the users themselves should be alert while using their system, being an alert user will help him secure his data from being hacked. Today's technology apart from tech savvies, a normal individual can get to know how a person's relevant data gets hacked by his own fingertip.

**REFERENCES:**


1. Ajeet Singh et.,al(2012) A Review: Secure Payment System for Electronic Transaction International Journal of Advanced Research in Computer Science and Software Engineering Volume 2, Issue 3, March 2012 ISSN: 2277 128X Research Paper Available online at: www.ijarcsse.com
2. http://cashlessindia.gov.in/promoting_digital_payments_people.html
3. http://economictimes.indiatimes.com/articleshow/56212448.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst
4. http://economictimes.indiatimes.com/articleshow/58666596.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst
5. http://economictimes.indiatimes.com/industry/banking/finance/banking/governments-effort-to-move-india-towards-digital-payments-era/articleshow/55736480.cms
6. http://economictimes.indiatimes.com/industry/banking/finance/banking/digital-payments-indias-new-currency-debit-card-transactions-surge-to-over-1-billion/articleshow/58863652.cms
7. http://searchsecurity.techtarget.com/definition/malware
8. http://www.firstpost.com/politics/narendra-modis-mann-ki-baat-focus-on-digital-payments-e-banking-schemes-3172834.html
9. http://www.nec.com/en/global/solutions/safety/info_management/cyberattack.html
10. http://www.techrepublic.com/article/are-people-scared-of-mobile-payments/
11. http://www.webopedia.com/TERM/E/endpoint_security.html
12. http://zeenews.india.com/health/ransomeware-virus-strikes-sms-hospital-in-jaipur-2013564
13. https://www.internetsociety.org/blog/tech-matters/2017/05/6-tips-protecting-against-ransomware
14. https://www.linkedin.com/pulse/20140725002456-55850400-why-some-people-fear-internet-banking
15. https://www.paloaltonetworks.com/cyberpedia/what-is-cybersecurity
16. https://www.reuters.com/article/us-cyber-attack-india-idUSKBN19J0DI
17. Princewill Aigbe and Jackson Akpojaro(2014) Analysis of Security Issues in Electronic Payment Systems International Journal of Computer Applications (0975 – 8887) Volume 108 – No. 10, December 2014
18. Theodosios Tsiakis et., al(2005) The concept of security and trust in electronic payments Elsevier Computers & Security (2005) 24, 10-15
19. http://www.dailyo.in/business/demonetisation-black-money-cashless-economy-/story/1/14091.html(7-11-2016)