Research Paper

www.eprawisdom.com

# A STUDY ON SECURED CASHLESS ECONOMY IN INDIA WITH REFERENCE TO INITIATIVES TAKEN BY RESERVE BANK OF INDIA (RBI) TOWARDS DIGITAL PAYMENT

Dr. Hemanth Kumar .S[1] — [1]Associate Professor, CMS Business School Jain University, Bangalore, Karnataka, India

Asst Prof. Nagendra .B M[2] — [2]ASC Degree College, Bangalore, Karnataka, India

Asst Prof. Rajesh .M[3] — [3]ASC Degree College, Bangalore, Karnataka, India

## ABSTRACT

*India through its 'DIGITAL INDIA' initiative is looking forward to compete globally, though a growing economy. The transition towards digitalization is full of challenges. The greatest challenge is acceptability from its people. Security is seen as the most concerning factor to people. Thus, this paper studies the initiatives taken by RBI in ensuring safety and security in digital payment among people. It is found that, RBI has taken various initiatives towards regulating banks in ensuring cyber security and safety. However, the study suggests more initiatives have to be intended in creating awareness and thereby educating people followed by its implementation to realize the intended benefits of a 'Cashless Economy'.*

**KEY WORDS:** *phishing, hacking, malware, identity theft, boiler room fraud, keystroke capturing, lottery fraud, pharming*

## INTRODUCTION

Digital payment is a mode of payment which is thru digital modes. In digital payments, payer and payee together use digital modes to send and receive money. It is also called electronic payment. No hard cash is involved in the digital payments. All the transactions in digital payments are completed online. It is an instant and convenient way to make payments.

## TYPES OF DIGITAL PAYMENTS

| | |
|---|---|
| BANKING CARDS | Banking cards offer consumers more security, convenience and control than any other payment method. A wide variety of cards are available such debit, credit and prepaid cards. These cards provide 2 step authentications for secure payments (i.e., secure PIN and OTP). |
| UNSTRUCTURED SUPPLEMENTARY SERVICE DATA (USSD) | The innovative payment service *99# works on USSD channel. This service allows mobile banking transactions using basic feature mobile phone, there is no need for mobile internet banking for using USSD. |
| AADHAR ENABLED PAYMENT SYSTEM (AEPS) | AEPS is a bank led model which allows online interoperable financial transactions at PoS through the bank correspondent/ Bank Mitra of any bank using the Aadhar authentication. |
| UNIFIED PAYMENTS INTERFACE (UPI) | UPI is a system that powers multiple bank accounts into a single mobile application, merging several bank features, seamless fund routing and merchant payments into one hood. Each bank provides its own UPI App for Android and iOS mobile platform(s). |

| | |
|---|---|
| **MOBILE WALLETS** | A mobile wallet is a way to carry cash in digital format. An individual can link ones debit and credit card in mobile device to mobile wallet application or can transfer money online to mobile wallet. An individual's account is required to be linked to the digital wallet to load money into it. Most banks have their e–wallets and some private companies. e.g., Paytm, Freecharge, Oxigen, Airtel money, Jio money, SBI Buddy, Axis Bank Lime, ICICI Pockets etc., |
| **POINT OF SALE (PoS)<br>or<br>MICRO ATM's** | PoS is a place where sale is made. On a macro level, a PoS may be a mall, a market or city. On a micro level, retailers consider a PoS to be the area where a customer completes a transaction, such as a checkout counter. |
| **INTERNET BANKING** | Internet banking is also known as online banking, e – banking or virtual banking, is an electronic payment system that enables customers of a bank or other financial institution to conduct a range of financial transactions through the financial institution's websites.<br>Different types of Internet Banking are:<br>▪ National Electronic Fund Transfer (NEFT)<br>▪ Real Time Gross Settlement (RTGS)<br>▪ Electronic Clearing System (ELS)<br>▪ Immediate Payment Service(IPS) |
| **MOBILE BANKING** | Mobile banking is a service provided by a bank or other financial institution that allows its customers to conduct different types of financial transactions remotely using a mobile device such as a mobile phone or tablet. It uses software, usually called an app, provided by the banks or financial institutions for the purpose. |

***(Source: http://cashlessindia.gov.in/digital_payment_methods.html)***

Even though there are multiple digital payments types, they come with certain disadvantages such as difficult for a non-technical person who is not versatile with mobile phone, the internet and cards. Also, the risk of data theft associated with the digital payment. Hackers can hack the servers of the bank or the E-Wallet and take personal information. They can use this information to steal money from ones account. Further, overspending generally an individual keeps limited cash in one's physical wallet and think twice before buying anything. But by using digital payment modes, they have limited cash unlimitedly. This can result in overspending.

Digital payments also come with certain advantages such as easy and convenient payments. A mobile phone or Aadhaar number or a card to pay. UPI apps and e-Wallets made digital payments easier. Also, pay or send money from anywhere using digital payment modes such as UPI apps, USSD or e-Wallets. They also provide with discounts from taxes. Government has announced many discounts to encourage digital payments. If digital modes are used to make a payment up to Rs. 2000, one can get full exemption from service tax (pre GST). Further, also get 0.75% discounts on fuels and 10% discount on insurance premiums of government insurers. They also facilitate as written record as they automatically record in one's passbook or e-Wallet app. Thus enable to maintain record, track spending's and budget planning. Further, less risk on losing mobile phone or debit/credit card or Aadhar card a stranger cannot use money without MPIN, PIN or individuals fingerprint in the case of Aadhar. But it is advised to block card if lost.

The future of digital payments is very optimistic. India is experiencing a notable progression in digital payments. In 2015-16, a total of Rs. 4018 billion transacted through mobile banking as compared to Rs. 60 billion in 2012-13. The percentage of the digital payments through other modes is also increasing in a momentous speed. Digital revolution has provided an easy way to go for digital payments. India has more than 100 crore active mobile connections and more than 22 crore smartphone users. This number is going to increase further with a faster internet speed. The reach of mobile network, internet and electricity is also expanding digital payments to remote areas. This will surely increase the number of digital payments. Further, the Government is supporting digital payments through their various initiatives one such being BHIM app.

As the future for online / digital payments looks positive, the paper attempts to discern the various initiatives towards safety and security in digital payments taken by the Central Bank of India or the Reserve Bank of India (RBI).

## LITERATURE REVIEW

(CH. B. V. L. Sudheer & Ashrefunnisa, 2017) ascertained the extent to which electronic payment affect cashless economy of India. The study indicated that the electronic system of payment will have a great implication in cashless economy of India but it will led to significant decrease in deposit mobilization and credit extension by Indian deposit money banks. Consequently, the authors concluded that cashless system of payment will be examined and develop the e-payment system first, so that people will be used to it before talking of cashless economy.

The study suggested the improvement in infrastructural development so as to enhance e-payment system.

(Rachna & Singh, 2013) Study aimed to identify the issues and challenges of electronic payment systems and offer some solutions to improve the e-payment system quality. With respect to the payments methods they have analyzed, it is impossible to say that any one of them is perfect, although each one of them has advantages as opposed to others. If the client wants to maintain privacy, then they choose those payment methods which guarantee a higher level of privacy such as e-cash or Net Bill Checks. If the priority is security, they should use, smart cards. The study concludes on the note that, successful implementations of electronic payment systems depends on how the security and privacy dimensions perceived by consumers as well as sellers are popularly managed , in turn would improve the market confidence in the system.

(Rathore & Shweta, 2016) Study tries to examine the various factors that can affect a consumer's decision to adopt digital wallet as a mode of online payment. Apart from this, the study also attempts to find out the various risks and challenges faced by users of digital wallet. The study concluded with the remarks digital wallets are quickly becoming mainstream mode of online payment, since shoppers are adopting digital wallets at an incredibly rapid pace, largely due to convenience and ease of use. Tech-savvy shoppers are increasingly demanding seamless, omni-channel retail experiences and looking for solutions that deliver this.

(Pakojwar & Uke, 2014) The paper explores several of technologies and security standards the different researchers have recommended to banks for safe internet banking and comparison of number of security systems based on the recommendations given by these authors for secure online banking. From an operational perspective, this study indicates that internet banking allows customer to conduct transaction at any time and thus it reduces the number of physical visit to a bank and it has reduced the cost per transaction. It is studied that, an effective authentication program should be implemented to ensure that authentication tools are appropriate for all of the financial institutions, internet based products and services.

(Sudent, 2017) The paper focuses on the SWOT analysis of "CASHLESS ECONOMY" from an Indian perspective describing the strengths, weaknesses, opportunities and threats for India from going cash to cashless. The study is of the opinion, every new habit introduced in life needs at least 21 days to get used to and the way Indian society pay for a thing is a cultural pattern which is hard to change, however not impossible. The author is of the outlook that, in order to go cashless, the phased implementation could have been worked upon i.e. choosing few districts or sectors to go cashless rather than sprinkling the idea upon entire society, or it could have been introduced as a pilot mechanism in few areas for a testing purpose whether Indian society is ready for such a move or not.

(Agrawal & Singh, 2016) The study examines the working efficiency of the principles stated by Basel norm III in high digitized banking environment in India. The paper contributes to the fact that how these principles are standing from business electronization to massive business digitization in today's Indian Banking industry. Moreover it will also provide suggestion to what extension and addition to these principles are required as per the managers' point of view. The study found that indeed the Basel Committee's risk management principles are applicable in today's scenario are extra-ordinarily going to benefit e-banking business if it is framed locally as per country's need, time, demand and situation responding. This paper also conclude that even II tire cities of India is experiencing e-banking and managers are known with the fact that the consumer of today is much more aware about the latest trends. These principles are indeed the lightening torch to e-banking but as a policy maker and as operations provider we have to look into the need of the hour and respond accordingly.

(Shendge & Shelar, 2017) focused on impact and importance of cashless policy in India. According to Government of India the cashless policy will increase employment, reduce cash related robbery thereby reducing risk of carrying cash. Cashless policy will also reduce cash related corruption and attract more foreign investors to the country, leads to modernization of payment system, reduction in the cost of banking service, reduction in high security and safety risk and also curb banking related corruption. The financial safety over the digital payment channel is important for pushing the cashless economy idea. The retail sector still has predominance of cash transaction and payment through cash is yet to pick up and card is the one of the most secure, convenient mode of cashless payment in retail market. Digital transactions are traceable, therefore easily taxable, leaving no room for the circulation of black money. The whole country is undergoing the process of modernization in money transactions, with e-payment services gaining unprecedented momentum.

## STATEMENT OF PROBLEM

The Indian Government is constantly working to create a new challenging and opportunistic economy which is essentially 'cashless'. For a developing country like India, the transition towards digitalization is never so easy. Various researchers have studied across various domain to understand and implement a secured cashless economy. However, many studies have been conducted to know the need for cashless economy, its advantages and disadvantages, opportunities and treat, some studies have concentrated towards online payment its safety and security. At this point of time, where the Government of India is promoting the digital payment under its 'Digital India' initiative, it is imperative to study the initiatives taken by Central Bank of India (i.e., RBI) and Government of India jointly. Hence, this paper focuses on initiatives taken by Reserve Bank of India (RBI) towards digital payment.

## SCOPE OF THE STUDY

India has initiated for cashless economy by empowering its digital services. Government is taking various initiatives to realize its benefits. However, the transition of India towards cashless economy is time consuming and more risky. A careful planning is required to absorb the intended benefits. This is possible only when the people feel they are secured, hassle free and are immensely benefited. The Government of India through, Information Act 2000, Information Act 2008 and other cyber laws under the Ministry of Electronics and Information Technology is regulating the cyber security and safety. However, when it comes to banking and digital payments, RBI role is vital for framing policies, providing guidelines and for regulation of financial institutions. Thus, the role of RBI is pivotal both in short and long run.

## OBJECTIVES

- To analyze the various risk involved in digital payments.
- To understand the initiatives undertaken by RBI.

## METHODOLOGY

The study is exploratory in nature, aiming to get insights and familiarity for later investigation and data collected for the present study is mainly through secondary sources.

## OPERATIONAL DEFINITION OF STUDY

| | |
|---|---|
| **Phishing** | Phishing is a kind of scam where the scammers masquerade (trick) as a trustworthy source in attempt to gain private data such as PINs, and credit card data, etc.., through the internet. Phishing normally happens through prompt messaging, email etc., |
| **Internet scams** | Attackers use internet as medium. Internet scams are patterns that betray the user in several ways in attempt to take benefit of them. These attacks are created to make the fraud with private assets of customer directly rather than personal data through deceitful undertakings, assurance tricks and more. |
| **Malware** | Malware, mainly spyware, is malicious software disguised as genuine software planned to accrue and transmit private data, such as PINs, without the customer's consent or knowledge. They are often spread through software, e-mail and files from unofficial places. |
| **Identity theft** | Identity theft is a crime in which a fraudster obtains key pieces of personal data, such as bank information, date of birth or driver's license numbers, in order to impersonate somebody. The personal data exposed is then used criminally to apply for credit, buying goods and services, or gain right of entry to bank accounts. |
| **Investment or share sale (boiler room) fraud** | Boiler room fraud is an attack in which illegal or aggressive mis- selling of bogus, valueless or massive expensive stocks take place by share fraudster. If the victim mistakenly invest money with this fraudster, he will certainly lose his all money invested. |
| **Keystroke capturing/logging** | Keystroke capturing or logging attacks take place with the help of software or hardware key logger. Anything that user type on system can be captured and stored in a storage. This attack mainly takes place at internet cafes. |
| **Lottery fraud** | In this type of fraud, attacker send fake letters or e-mail messages, which recommend the user that he have won a lottery. To take the benefits of this, they are asked to respond email message with some private banking information of victim, this include his bank account details, complete personal information. |
| **Pharming** | In Pharming attack, fraudster creates false website, so that people will visit them by mistake. This attack takes place when user mistype a website or a fraudster can redirect traffic from genuine website to a fake one. The main purpose of pharmer is to obtain victims personal information for further frauds. |

## LIMITATIONS OF THE STUDY

- The study is restricted to secondary data.
- The study is limited to authentic published reports.
- Due to time constraint only few initiatives are considered.

## CRITICAL STUDY

Reserve Bank of India has taken several distinguished and vital initiatives to regulate banks and ensure online safety and security. However, the cause for any cyber threat is not only due to banks but also due to the people who are less aware or unaware about this.

## I.RISK PERTAINING TO DIGITAL PAYMENTS

- The hardware used in the mobiles and Automatic Teller Machine (ATM) are not safe and do not provide safe digital transactions. As per the reports given by American Chipset maker, Qualcom, digital apps used in India are not secure as the wallets and mobile banking applications are not using hardware level security that is mandatory for secure online payments. They run on Android mode and use password that can be stolen. Fingerprints that some users use, can also be captured and used to sneak into the account.
- Hackers are present both in home country and host country, and if the host country is technologically sounded the risk of cyber-attack is very certain. Hackers everywhere (i.e., from one's own country to neighboring country). It has been in broadcast for now and always where ATM uproar disturbed a lot of people who lost money and had to wait for quite long time to get it reimbursed from bank.
- Many Indians are becoming the victims of some of the cyber-attacks. As per the reports of Norton Cyber Security Insights, Indians are the most susceptible to falling into ploys of phishing and hacking. The ads are not always protected and by clicking randomly that is not known to most people who are either using digital wallets or digital payments or smartphone are more vulnerable for such traps.
- The regulations governing the digital wallets are not adequate. Lack of security standards is yet another concern of risk. The standards prescribed by RBI for e – wallets in India are not passable. The circulars only require e – wallets to have 'adequate' data security infrastructure. Security issues comprises of multiple fake accounts, psychological manipulations (known as phishing), weak device authentication, hacking of servers and stealing of data.

- As the usage of internet for payment is increasing largely, the risk associated with that is also increasing at an alarming rate. According to RBI, cases concerning ATM, credit, debit card and net banking fraud were reported to be 13,083 and 11,997 in the year 2014–15 and 2015–16 respectively. However, in October 2016, breach of 3.2 million card were reported which was the single largest of its kind in India.
- Further, according to Juniper Research the online fraud transactions is expected to reach $25.6 billion by 2020 (i.e., $4 in every 1000 of online payments will be fraudulent). Also, A study from Assocham – PwC identifies a surge of about 350% in cyber cases registered under the IT Act,2000 between 2011 and 2014.
- People's awareness towards multiple ways for threat in digital payment is less. People are less aware of types of risks with respect to online payments. There are three kinds of risks unique to e – payments. One is device related (i.e., on losing a device which is not protected by any password or any other means, thereby giving open access to various apps, money in wallet etc.,) Second type of risk is from rights to access (i.e., by connecting the e – wallet or other fintech app with other apps like social networks could pose a risk of data leakage). Third type is due to sharing of passwords or OTP (one time passwords) with others especially when using these modes publicly.
- People are not much aware of the consequence of using the same password or vital personal information among different websites. The responsibility of being secured has to be equally shared by both the customers and banks. However, most of the customers, though are not aware of this. They become susceptible when they use the same passwords frequently or same passwords for different accounts (such as net banking, Facebook, Twitter etc.,). Similarly the banks should regularly update software and fraud detection systems. It is important to note that credit card, debit card, mobile wallets, net banking fall into two distinct buckets. Though card companies such as Visa, Mastercard, Amex do this banks want to control customer information and hence vulnerability can exist in their end. Though the banks have transformed from 40kb encryption to 128kb encryption, it is to be noted that as customers deal with variety of people with varying ability to transact digitally, the chance of a hacking opportunities are more. At present, in India the network is robust and is maintained by RBI with National Payments Corporations of India (NPCI) as nodal agency, the leaks could be at banks end or users end.
- According to Basudev Banerjee, banking expert at Microsoft, the system managing the links from origin of settlement of a transaction are robust and secured, yet the probability of fraud exists at every stage. A small purchase of an article can help the hacker in five different stages such as origin, transmission, transaction, settlement and reconciliation.
- Most of the users fail to keep their Bluetooth switched off, to not access public Wi-Fi, install antivirus software especially with smartphone and not download suspicious files from the internet. Three out of five people fail to install anti-virus a study says.
- Users are not aware many apps which ask for access to location and personal details are harmful and thus should not be installed. Most apps now– a–days seek access to personal info stored on the smartphone including documents, media files, contacts etc., users must be cautious before allowing it.
- People are not aware of the consequence of not changing the passwords frequently and also storing the bank details in their device. The online payment habit of the user must be changed. According to a study, two out of three people admitted of allowing their smartphone or personal computer to store their billing or card details for easier future transactions.

## II. KEY INITIATIVES BY RBI TOWARDS DIGITAL PAYMENT

| | | |
|---|---|---|
| 1 | **IT Governance** | The banks are emphasized on the information technology risk management. It includes accountability on a bank's board of directors and executive management. Focus includes creating an organizational structure and process to ensure that a bank's IT security sustains and extends business strategies and objectives. |
| 2 | **Information Security** | Banks are also directed to create and maintain framework to guide the development of a comprehensive information security program, which includes forming a separate information security function to focus exclusively on information security and risk management, distinct from the activities of an information technology department. These guidelines specify that the chief information security officer needs to report directly to the head of risk management and should not have a direct reporting relationship with the chief information officer. |
| 3 | **IT Operations** | The information technology operations should include specialized organizational competences that provide value to customers, including IT service management, infrastructure management, application lifecycle management and IT operations risk framework. |

| | | |
|---|---|---|
| 4 | **IT Services Outsourcing** | RBI places bank the ultimate responsibility for outsourcing operations and management of inherent risk in such relationships on the board and senior management. Focus includes effective selection of service provider, monitoring and control of outsourced activities and risk evaluation and management. |
| 5 | **Information Security Audit** | RBI has initiated the need for banks to re-assess IS audit processes and ensure that they provide an independent and objective view of the extent to which the risks are managed. It focuses on defining the roles and responsibilities of the IS audit stakeholders and planning and execution of the audit. |
| 6 | **Cyber fraud** | RBI through 'cyber fraud' plan, defines the need for an industry wide framework on fraud governance with particular emphasis on tackling electronic channel based frauds. Focus includes creating an organizational structure for fraud risk management and a special committee for monitoring large value fraud. |
| 7 | **Business Continuity Planning** | Central Bank has directed banks to focus on policies, standards and procedures to ensure continuity, resumption and recovery of critical business processes. Further, emphasize implementing a framework to minimize the operational, financial, legal, reputational and other material consequences arising from such a disaster. |
| 8 | **Customer Education** | RBI has channelized the banks, the need to implement consumer awareness framework and programs on a variety of fraud related issues. |
| 9 | **Legal issues** | Banks need to put effective processes in place to ensure that legal risks arising from cyber laws are identified and addressed at banks. It also should focus on board's consultation with legal department on steps to mitigate business risks within the bank. |
| 10 | **Cyber Security Policy** | It was mandate for Banks in India to formulate Cyber Security Policy and report the same before September 30, 2016. Banks should immediately put in place a cyber-security policy elucidating the strategy containing an appropriate approach to combat cyber threats given the level of complexity of business and acceptable levels of risk, duly approved by their Board. A confirmation in this regard may be communicated to Cyber Security and Information Technology Examination (CSITE) Cell of Department of Banking Supervision, RBI. |
| **11.** | **RBI Ethical Hacking** | To make sure whether banks in India are prepared to face such challenges or not, Reserve Bank of India (RBI) has opted to use ethical hacking to test the cyber security vulnerabilities of banks. |

## CONCLUSION

India is taking a lot many vital initiatives exclusively post – demonetization which in a while is capable of transforming it from developing to a developed country. One such initiative which is making India competitive against developed economies is 'Cashless Economy'. Under the initiative of 'Digital India' the country is making its people transact digitally (online). But the transition from developing country to developed country through digitalization as tool is ever challenging. To reap the benefit of cashless economy, it has to be widely accepted by its people. For the people to accept, the concerning factor has been safety and security. Thus, the role of the Central Bank (i.e RBI in India) is vital. RBI is dynamically regulating the banks. However, it is also imperative that they educate the people or users which will ensure security in digital payment and get wide acceptance.

## RECOMMENDATION

It is suggested that the RBI jointly with banks take profound initiatives to create awareness and thereby educate the people by use of social media and other platforms in the following matters –

- People/ Users should be educated and be made aware of falling into traps of phishing, hacking, Internet scams, malware, identity theft, investment or share sale (boiler room) fraud, keystroke capturing, lottery fraud, pharming, spyware and other viruses.
- Users should be made aware to protect devices with passwords else one should not store the passwords or other details that give open access on losing the device.
- Users should be educated to change password (ATM PIN, transaction PIN) frequently. (atleast for every six months once)
- Users should not use same password or vital details to multiple accounts (i.e same password for banking and social networking).
- People should be educated to switch off Bluetooth, Wi – fi and others when on public domain.
- People should be encourage to install anti-virus in mobiles.
- One should be aware when installing the apps. Most of the apps seek access to personal stored information.
- The online payment habit of storing their billing or card details to smartphone or personal computer for easier future transactions by the user must be changed.
- RBI should constitute a special team for constant or surprise visit to bank for routine banking software or hardware scrutiny.
- RBI should adopt new / updated training modules to all bank employees for ethical issues related to e – transactions arising frequently.

- RBI app should include the do's and don'ts in e – transaction to all the users. This app should be constantly updated with latest developments for all e – financial transactions.

## REFERENCES

1. *Agrawal, D., & Singh, G. (2016, February). An Analysis of Risk Management Principles for Electronic Banking using Basel III Norms. International Journal of Engineering Technology, Management and Applied Sciences, 4(2), 107-115.*
2. *CH. B. V. L. Sudheer, & Ashrefunnisa, M. (2017, February). Electronic Payment in Cashless Economy of India: Problems and Prospect. International Journal of Scientific Engineering and Technology Research, 6(7), 1398-1402.*
3. *Goel, S. (2016). Cyber-Crime: A Growing Threat To Indian Banking Sector. Recent Innovations in Science, Technology, Management and Environment, 13-20.*
4. *Niranjanamurthy, M., & Chahar, D. D. (2013, July). The study of E-Commerce Security Issues and Solutions. International Journal of Advanced Research in Computer and Communication Engineering, 2(7), 2885-2895.*
5. *Pakojwar, S., & Uke, D. N. (2014, October). Security in Online Banking Services –A Comparative Study. International Journal of Innovative Research in Science,Engineering and Technology, 3(10), 16850-16857.*
6. *Prakash, V. (2016, August). E-Commerce In India: Its Growth And Cyber Challenges. International Journal of Science Technology and Management, 5(8), 796-802. Retrieved from www.ijstm.com*
7. *Rachna, & Singh, P. (2013, December). Issues and Challenges of Electronic Payment Systems. International Journal for Research in Management and Pharmacy, 2(9), 25-30.*
8. *Rathore, & Shweta, D. H. (2016, April). Adoption Of Digital Wallet By Consumers. BVIMSR's Journal of Management Research, 8(1), 69-75.*
9. *Shendge, M. A., & Shelar, M. B. (2017, April). Impact and Importance of Cashless Transaction in India. International Journal of Current Trends in Engineering & Research (IJCTER), 3(4), 22-28.*
10. *Sudent, M. M. (2017, May). Cashless Economy: Swot Analysis From Indian Perspective. International Journal of Science Technology and Management, 6(5).*

## WEBSITE DETAILS

1. *http://www.business-standard.com/article/finance/rbi-steps-up-focus-on-cyber-security-of-banks-116082901301_1.html*
2. *http://www.legallyindia.com/views/entry/cybersecurity-in-the-financial-sector-an-overview*
3. *http://economictimes.indiatimes.com/news/economy/policy/rbi-announces-setting-up-of-standing-committee-on-cyber-security/articleshow/57039290.cms*
4. *https://ccgnludelhi.wordpress.com/2017/03/24/law-enforcement-initiatives-towards-tackling-cyber-crime-in-india/*
5. *http://indianexpress.com/article/business/banking-and-finance/cyber-crime-with-vulnerability-rising-rbi-calls-for-a-safety-net-2928565/*
6. *https://www.pwc.in/consulting/cyber-security/banking.html*
7. *http://indianexpress.com/article/explained/digital-payments-cyber-security-data-theft-hackingdemonetisation-4422513/*
8. *https://www.rbi.org.in/SCRIPTs/PublicationReportDetails.aspx?UrlPage=&ID=243*
9. *https://rbi.org.in/scripts/PublicationVisionDocuments.aspx?Id=678*
10. *http://cashlessindia.gov.in/CERT-In%20Advisory%20NotesMobile%20and%20Cloud%20Data%20Security.pdf*