CYBER RISK: A HINDRANCE TO FINANCIAL INCLUSION?

[1]Mohd. Shafeeq, [2] Dr. Sana Beg
[1] Research Scholar, [2]Assistant Professor
[1] Department of Management
[1]Jamia Hamdard, New Delhi, India

Abstract: The concept of financial inclusion gained importance in 2005 in India. Since Census 2011, RBI and Government of India initiated various measures like relaxing the KYC norms, an opening of BSBDs accounts, direct bank transfer, Pradhan Mantri Jan Dhan Yojana, etc. Digitalisation of finance gained momentum after demonetisation which is also evident from a colossal climb in the value of the mobile transaction, which registered an increment from INR 23,794.84 million (2016) to INR 73,124.94 million (2017). Thus India discerned a remarkable paradigm shift towards digitalization; with this shift, a distinct challenge has popped up for financial inclusion. India propelling towards digital financial inclusion has made itself extremely vulnerable to a cyber attack which is also manifest from the report of the International Telecommunication Union (ITU), 2017. Not even in India, cyber risk is a big threat to all institutions globally as well. Thus, this study is undertaken to understand the awareness of Cyber-attacks among the citizens and to assess whether it poses a challenge to financial inclusion. The study exhibits that 7 out of every 10 people receive a fraudulent message, call or e-mail. Awareness of cyber frauds is high in India but the complaint rate is too low. The study concluded that cyber attack will not lead to financial exclusion instead it will lead to a fall in the usage rate of digital financial services and thereby reducing the pace of digital financial inclusion. Thus proactive measures must be taken to combat cyber risks.
Keywords: *Cyber Risk, Cyber-Attacks, Cyber Risk awareness, Digital Financial Inclusion.*

I. INTRODUCTION

The concept of financial inclusion was first featured in 2005 in India, by Dr. K. C. Chakrabarty. Since then, RBI and Government of India are making concerted efforts to achieve financial inclusion in India. In today's era, focus is shifting from financial inclusion to digital financial inclusion. Prior to demonetisation, digitalisation wasn't given much importance. However, post demonetisation effects had shown some signs of digitalization in India leading to a paradigm shift towards digital financial inclusion. Digitalisation brings a revolution in the financial service industry. The growth of digitalization is pushing up. Sudden announcement of demonetization led to a change of gears and people started moving towards cashless mode in a big way. But according to (Bhaskar, 2017), this big push has not happened. However, shifting to cashless mode also provides cybercriminals the opportunity for financial frauds (Raghavendra, 2017). Cybercriminals are individuals or a group of people who uses a computer and a network to perpetrate malicious activities on digital systems to seize sensitive information and to make gains from it or to steal money. These kinds of attack by cybercriminals are known as 'Cyber attacks'.

Cyber risk can be defined as "*operational risks to information and technology assets that have consequences affecting the confidentiality, availability, or integrity of information or information systems*" (Cebula & Young, December 2010).

As per the report of the IMF, June 2018, 91% of the cyber attacks are on banks while 7% of the attacks are targeted on insurance companies. Amongst the banks, retail banking activities and credit card services are the most targeted segment with a share of 39% and 25% respectively.

No financial institution can operate without Cyber risk, (Sunny, 2017) thus it has become necessary to manage the cyber risks. There are many instances worldwide in which the Central Banks of the countries has to face cyber attack, for instance, data breach has been faced by Federal Reserve Bank of Cleveland (Cleveland-based headquarters of the U.S. Federal Reserve system's fourth district) in 2010, Federal Reserve Bank of New York (One of 12 Regional Reserve Bank that make up US central bank) in 2012, Federal Reserve Bank of Saint Louis (One of 12 Regional Reserve Bank that make up US central bank) in 2013, Central Bank of Azerbaijan (Central bank of Republic of Azerbaijan) in 2015 and Bank of Italy in 2017. Business disruption has been faced by Sveriges Riksbank (Sweden's Central bank) in 2012 and Norges Bank (Central bank of Norway) in 2014. Banco Central del Ecuador (Central bank of Ecuador) in 2013, Central Bank of Swaziland (Central bank of Eswatini) in 2014, Bangladesh Bank in 2016 and Bank of Russia in the year 2016 too faced fraud.

1.1 Common Types of Cyber Attacks

- **DoS AND DDoS Attacks:** These attack leads to suspension of service. Denial of service (DoS) uses one computer and one internet connection to disrupt the services without any use of malware while Distributed Denial of Service (DDoS) attacks uses multiple machines to launch an attack and uses malware.
- **MitM Attack:** It stands for Man in the Middle attack and hacker comes in communication which is taking place between the client and a server.
- **Phishing:** It is the practice of sending the mail in the name of some organization in order to get the details of the target or to influence the target to do something.
- **Drive-by Attack:** It is a common method of spreading malware either by redirecting the target to the malicious website or by planting a malicious script into HTTP of an insecure website.
- **Password Attacks:** It is carried out in order to make use of the password to steal information or money.
- **Cross-Site Scripting (XSS) attack:** It uses third-party web resources to run scripts in the victim's web browser.
- **Eavesdropping attack:** It occurs through the interception of network traffic. In this type of attack the hacker tries to steal information that computers, mobile phones or devices transmit over a network.
- **Malware Attack:** Used to install unwanted software without the consent in the target's computer.

1.2 Major Incidents of Cyber Attacks in India

By December 2017, overall 53,081 incidents of cyber attacks have been reported to the Indian Computer Emergency Response Team (CERT-In), few of the financial frauds are being discussed which depicts challenges faced by the Indian Financial System:

2008: In June 2008, ICICI Bank suffered a loss of INR 12.85 lakh on account of phishing. The complaint was registered by an Abu-Dhabi based NRI, and ICICI Bank was held responsible for such phishing and they paid INR 12.85 lakh including the amount of loss suffered and expenses involved in the case to the Abu-Dhabi based NRI.

2016: On 19th October 2016, SBI blocked six lakh debit cards to ward off security threat. Axis bank filed a complaint to the RBI regarding the malware attack and card network companies NPCI, Mastercard and Visa had informed various banks regarding the data breach. Because of this SBI blocked several cards, as a precautionary measure. Beside SBI and Axis bank, there were many other banks which were affected by this malware which includes ICICI, YES Bank and HDFC bank. These were the five banks which were severely affected by the malware. Overall 3.2 million debit cards were affected.

2016: On 2nd August 2016, cyber attackers tried to insert a malicious page and also tried to block some of the e-payment services of Canara Bank.

2018: On 17th February 2018, a cyber attack was initiated on City Union Bank which compromised the SWIFT messaging system. This resulted in a theft of about $2 million although 50% of the amount was recovered within a span of one hour.

2018: On 11th August 2018, INR 80.5 crore was siphoned off from the Cosmos Cooperative Bank Ltd, which is the second oldest and second biggest cooperative bank in terms of financial set-up. The amount of INR 80.5 crore was siphoned off in two parts, in the first part INR 78 crore was withdrawn from the ATM's of 28 countries simultaneously through VISA cards and in the second part INR 2.50 crore was transferred within India from Rupay card. Later on 13th August, another amount of INR 13.92 crore was transferred to the account of "ALM trading Ltd.", Hong Kong through SWIFT transactions. Thus, the total amount which was siphoned off from the Cosmos amounted to INR 93.42 crore.

1.3 About CERT-In

It is an Indian Computer Emergency Response Team (CERT-In) which was founded in the year 2004 in order to deal with cyber-security threats like phishing and hacking. It works under "Ministry of Electronics and Information Technology" and its motto is to handle cyber-security incidents in the country. The table below provides the overall cyber attacks in India in the corresponding year:

Table 1 Overall Cyber attacks

Security Incidents	Year		
	2015	2016	2017
Phishing	534	757	552
Network Scanning / Probing	3673	416	9383
Virus/ Malicious Code	9830	13371	9750
Website Defacements	26244	31664	29518
Website Intrusion & Malware Propagation	961	1483	563
Others	8213	2671	3315
Total	49455	50362	53081

Source: CERT-In Annual Report

If we look at the table above showing the cyber attack incidents in India, it is quite clear that cyber attacks are on the rise in India. In the year 2015, total reported cyber attack incidents were 49455 which increased to 50,362 in the year 2016 and in the year 2017 this figure was reached to 53,081.

II. CYBER ATTACKS AND FINANCIAL INCLUSION

The term "Financial Inclusion" is defined as the *"The process of ensuring access to financial services and timely and adequate credit where needed by vulnerable groups such as weaker sections and low-income groups at an affordable cost"*.

The World Bank Group (WBG) president Jim Yong Kim has established an initiative to achieve Universal Financial Access by 2020 and our current Prime Minister Shri Narendra Modi is also focussing on achieving financial inclusion through mobile and e-banking. However, increasing cyber attacks can hamper the pace of financial inclusion in any economy it is because of the involvement of the various banking services like Debit card services, Credit Card services, Internet Banking etc which are highly prone to cyber attacks and it is quite clear from the incident that was happened with the Cosmos Cooperative Bank Ltd and State Bank of India, that any negligence in ignoring cyber attacks can lead to colossal loss. According to Durai & Stella, (2019) security has negative impact on digital financial inclusion.

Thus it has become necessary to provide a hassle-free framework for achieving digital financial inclusion because it is expected that mobile payment transaction value will reach INR 2,205 trillion while mobile wallet transaction will reach INR 275 trillion by 2022 (ASSOCHAM, 2017).

III. RESEARCH METHODOLOGY

The study uses a descriptive research design to analyze cyber risk awareness. The study uses two sources of data: primary data and secondary data. Primary data was collected with the help of a questionnaire to analyze the awareness of cyber risk and its influence on financial inclusion while secondary data was used to gain insights about the cyber risk and recent attempts of cyber attacks on India. A survey was conducted on a group of 100 people which included people from different sections of the society, emphasis more on lower segments of the society. Convenience sampling was used for the study.

Objective:

1. To study the awareness of Cyber Risk while conducting a banking transaction.
2. To analyze the influence of Cyber Risk on digital financial services.
3. To analyze the importance of understanding cyber risk in increasing Financial Inclusion in India.

IV. DATA ANALYSIS AND INTERPRETATION

4.1 Demographic Profile of the respondents

Table 2 demographic profile of the respondent

Gender		**Marital Status:**		**Religion:**			
Male:	62	Married:	48	Muslim:	48	Christianity:	7
Female:	38	Unmarried:	52	Hinduism:	44	Hinduism:	1

Educational Qualification:		**Profession:**		**Family Income:**	
Illiterate	15	Business	12	INR 0 to INR 1lac	43
Up to High school	14	Service	36	INR 1lac to INR 2.5lac	29
Intermediate	2	Self-employed	19	INR 2.5lac to INR 5lac	21
Under-Graduate	5	Student	15	INR 5lac to INR 10lac	7
Graduate	20	Scholar	5		
Post-Graduate	44	Unemployed	1		
		Housewife	12		

4.2 Interpretation of the People not having a bank account

In the survey, it is found that 91 people are having a bank account while the remaining 9 people don't have a bank account. Out of those 9 people, 4 were male and 5 were females. Out of these 5 females, 4 were housewives and most of them were facing difficulties in handling banking services either due to their illiteracy or no receipts and payments. While, in the case of a male it is found that illiteracy, too much documents requirement and their income level prevents them from opening a bank account. It is also found that out of those 5 women 4 were of the Muslim religion and all these 5 women were housewives. In total there were 38 females and out of these 38 females, 16 were of the religion Muslim.

4.3 Digital Financial Services and its usage:

It is found that the use of internet banking is more popular amongst the male with 59% approving to the usage of internet banking, as compared to 39% in the case of a female. Same was the case for mobile wallet services. Female dominantly using the ATM services with 93% usage rate while this figure was 83% in the case of a male. The usage rate for RTGS/NEFT was very low in the case of female i.e. 13% while this figure was 38% in the case of a male.

The usage rate of internet banking was 0% amongst the illiterate people and 58% amongst the literate people. For mobile wallet services, it is 10% amongst the illiterate people while for literate people it is 50.61%. The usage rate of ATM amongst the illiterate people was the highest with a figure of 80% while for RTGS/NEFT it is 20%. Amongst the literate people usage rate of ATM is 86.42% while for RTGS/NEFT it is 32.1%. The average use of these services in a month is 5.63 times with an average expenditure of INR 10,000 per month.

4.4 Cyber Risk: A threat?

Around 60% of the target group has felt the dread when sharing their bank account information while using services like internet banking, mobile wallet services, ATM services, and RTGS/NEFT services. The figures for both male and female were around 60%. Approx 60% of literate people has faced fear while sharing their bank account information as compared to 40% of illiterate people. The figure for illiterate people is low because of their low usage rate of internet banking, mobile wallet services, and RTGS/NEFT services.

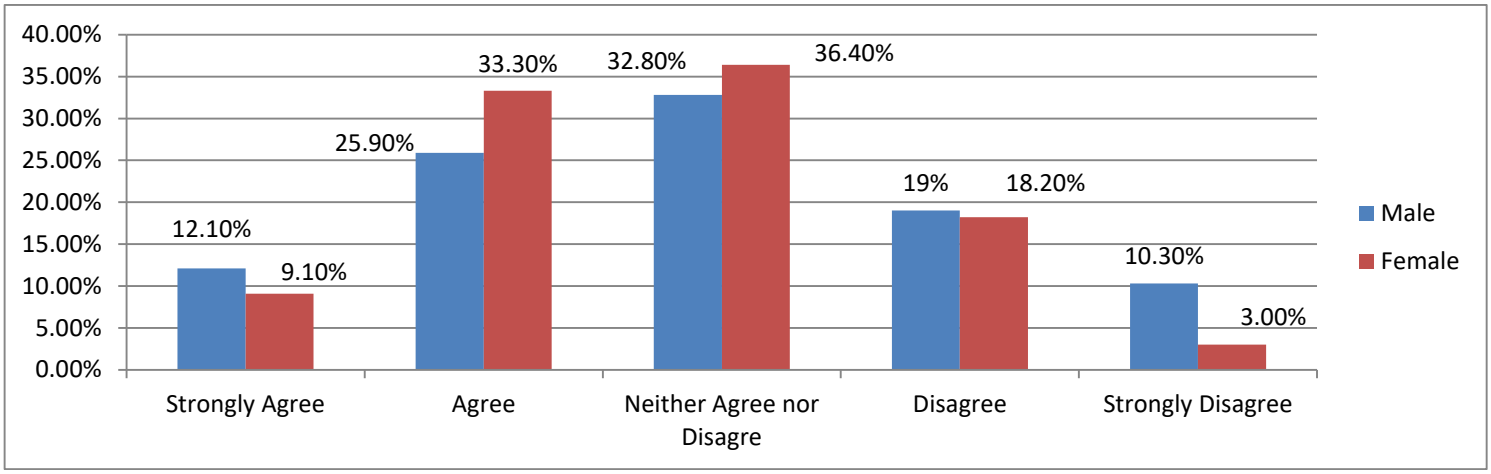

Fig. 1 Gender Wise agreement level on the statement "Internet banking is the safest mode of making payment"

From the Figure 1 it can be observed that the answers of the male and female were quite similar, thus in order to prove it statistically chi-square test was conducted between gender and the agreement level on "Internet banking is the safest mode of making payment". After running the chi-square test P sig value obtained was 0.712 which is greater than the P sig value of 0.05. Thus it can be concluded at a 95% confidence interval that there is no association between the Gender and the agreement level on "Internet banking is the safest mode of making payment". From Figure 1, it can be clearly seen that percentage of people agreeing to the said statement is quite high while the percentage of people who neither agreed nor disagreed is also quite high which reveals that either they have a lack of knowledge regarding the given statement or they are unaware of it.

Nearly the same results were obtained when we tried to analyze the gender and the agreement level on "Indian Banks are highly efficient and has a robust payment system". In this case P sig value was 0.322 which was greater than P sig value 0.05, therefore it can be concluded at 95% confidence interval that there is no association between the gender and the agreement level on "Indian Banks are highly efficient and has a robust payment system". Majority of the people were either agreed or they were neutral on the statement "Indian banks are highly efficient and have a robust payment system".

Almost the same results were obtained when we tried to analyze the agreement level on the statement "Banks provides me all the information related to the safety of the account and helps in preventing from any cyber attack".

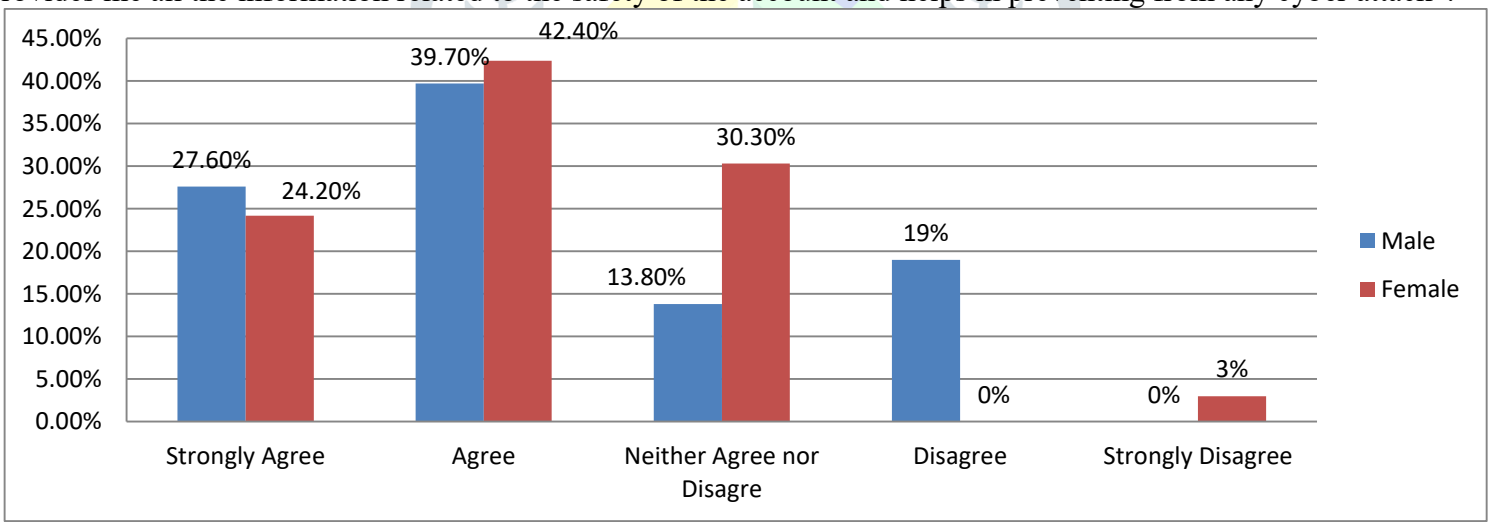

Fig. 2 Gender Wise agreement level on the statement "Cyber attack will discourage you in using the banking services"

When we tried to analyze the gender and the agreement level on the statement "Cyber attack will discourage you in using the banking services", the results were different in this case, nearly 67% of the people agreed that cyber attacks will discourage them in using the banking services while around 20% were neutral on this and the rest disagreed to the said statement. Then we ran a Chi-square test between the gender and the agreement level on the said statement, we obtained a P sig value 0.026 which is less than the P sig value 0.05, thus at a 95% confidence interval we can say that there is an association between the gender and the agreement level on the statement "Cyber attack will discourage you in using the banking services".

Nearly 70% of the people agreed that increasing cyber fraud will lead to a decrease in the usage of online banking services while 15% were neutral on this and the rest disagreed. When running a Chi-square test, no association was found between the gender and the agreement level on the statement "Increasing cyber fraud will lead to a decrease in the usage of online banking services".

4.4 Chi-square test results for different statements based on the demographic profile of the respondents.

Table 3 chi-square test results:[1]

Statement	Demographic Profile					
	Gender	Marital Status	Religion	Educational Qualification	Profession	Income
Internet banking is the safest mode of making payment.	.712	.023	.469	.46	.134	.486
Indian Banks are highly efficient and have a robust payment system.	.322	.508	.171	.310	.000	.326
Bank provides me all the information related to the safety of my account and helps me in preventing myself from any cyber attacks.	.144	.352	.021	.042	.347	.090
Cyber attack will discourage you in using the banking services.	.026	.222	.789	.516	.459	.792
Increasing cyber fraud will lead to a decrease in the usage of online banking services.	.514	.004	.801	.802	.081	.737

4.5 Awareness of the term 'Cyber Risk':

In our survey, around 88% of the people are aware of the term Cyber Risk, while this figure reaches 93% in the case of the female. Even the illiterate people are also aware of the term Cyber risk the figure was around 60%, though the figure is less but not too less from the context of India where the literacy rate is only 74%. The survey also revealed that in India, 7 out of 10 persons receives a call/message/e-mail, etc asking them about their personal information and bank account details by making false claims like a lottery winning, etc. Nearly 3 out of 100 person files a complaint to the police or bank while rest believes in ignoring the attempt. It was also found that nearly 6 out of every 91 people has become the victim of the cyber attacks.

V. FINDINGS AND CONCLUSION

5.1 Findings:

- 9 out of 100 people are still financially excluded either because of unemployment or low income or transactions taking place mostly on a cash basis.
- Financial exclusion is high in case of women who are not financially independent. It is more dominant in the Muslim community.
- It is also found in the survey that people who are availing the banking services face difficulty in handling the banking transactions because of their literacy and they even tend to avoid using banking services because of this reason. Thus measures must be taken to provide facilities like less document requirement, assistance in filling the documents, etc to those who are illiterate and can't handle documents requirement while availing banking services. It is because, in India, the literacy rate is still far behind from the good, at present; this figure is around 74%.
- People are now using more of the services which are based on either internet or technology like Internet banking, mobile wallet services, ATM services, & NEFT/RTGS, etc. and they are also very much prone to cyber attacks as 7 out of 10 people receives a fake call or fraudulent messages seeking their personal and bank account details.
- The study reveals that increasing cyber attacks may discourage them from using digital financial services.
- High awareness about the cyber risk and continuous efforts of the commercial banks in creating awareness about the cyber risk, has kept the victims of the cyber attacks to a low i.e. 6 out of 91 people.

[1] If Chi-square P-sig value is greater than .05 in the table it implies that there is no association between the two variables and if P-sig value is less than .05 in the table it implies that there is an association between the two variables, corresponding to 95% Confidence Interval.

- Although people have full faith on the Indian Banking system, but increasing cyber attacks on India in the last few years may lead to a fall in the usage rate of the banking services along with the decline in the usage of online banking services.
- In India, a majority of the people are aware of the term cyber attacks but the problem that was found is that people tend to prefer ignoring the fraudulent messages or any such attempts rather than complaining it to the bank or to the police station. The possible reason for this is to avoid legal hassles and wastage of their times. However, this can become a big threat because ignoring, such attacks may indirectly be promoting those attackers. Another reason can be the lack of knowledge about the measures available to them when someone tries to attack them.
- It is found that people who file a complaint to the banks regarding the cyber attacks or any cyber fraud are never entertained in a manner they must have been entertained. It is because when the amount of cyber fraud is low, banks keep either minimal or no interest in looking into it.

5.2 Conclusion:

"We have to act proactively against the cyber attempts instead of waiting firstly for cyber fraud to happen."

It can be concluded that cyber attacks are not the reason for the financial exclusion but increasing cyber attacks in India will lead to a decrease in the usage of digital financial services thereby reducing the pace of digital financial inclusion. Thus, it is not a hindrance to financial inclusion rather it's a hindrance to the pace of digital financial inclusion.

"Cyber attacks don't impact the financial inclusion directly rather it impacts the financial inclusion indirectly"

5.3 Suggestion:

- To increase the usage of banking services amongst the illiterate and uneducated people a different window can be operated in the bank for the assistance of the illiterate people or a biometric facility can be provided in the bank to these peoples so that they just have to use their thumb impression to do transactions in the bank with ease.
- Continuous up gradation of technology is required, which is also a guideline in the RBI "Cyber security framework in India".
- Measures must be taken to provide a hassle-free framework for filing complaints not only against the cyber frauds but also against the cyber attempts.
- Need to shift from 'paper based banking' to 'green banking'.

REFERENCES

[1] ASSOCHAM. (2017). *M-Wallet: Scenario Post Demonetisation.* Hyderabad.
[2] Bansal, M., & Kumar, D. S. (2016). *Relevance of financial inclusion, financial frauds and financial literacy in indian context: the present scenario.* International Journal of Science Technology and Management.
[3] Bhaskar, S. (2017, April). Digital Banking-Transforming Inida? *Digital Banking new horizon in a Cash-light India* , pp. 5-7.
[4] Canara Bank **https://cio.economictimes.indiatimes.com/news/digital-security/pakistan-hacker-defaced-canara-bank-site-tried-to-block-e-payments/53646969** website accessed on 2/1/2019.
[5] Cebula, J. J., & Young, L. R. (December 2010). *A Taxonomy of Operational Cyber Security Risks.* Software Engineering Institute. Carnegie Mellon University.
[6] Chakrabarty, K.C.(2011), *"Financial Inclusion"*, Presentation at St. Xavier's College, Mumbai on September 7, 2011
[7] City Union Bank https://economictimes.indiatimes.com/industry/banking/finance/banking/city-union-loses-2-million-in-cyberattack-retrieves-half/articleshow/62956557.cms website accessed on 2/1/2019.
[8] Cosmos Bank news https://tech.economictimes.indiatimes.com/news/corporate/punes-cosmos-bank-loses-rs-94-cr-to-cyber-attack/65410241 website accessed on 1/1/2019
[9] Durai, T., & Stella, G. (2019). *DIGITAL FINANCE AND ITS IMPACT ON FINANCIAL INCLUSION.*
[10] ICICI News https://economictimes.indiatimes.com/industry/banking/finance/banking/icici-bank-told-to-pay-rs-13-lakh-to-nri-customer/articleshow/5798944.cms
[11] IMF. (June 2018). *Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment.*
[12] International Telecommunication Union (ITU). (2017). *Global Cybersecurity Index.*
[13] IMF. (June 2018). *Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment.*
[14] Raghavendra, B. M. (2017, April). Digital Banking-An Indian perspective. *Digital Banking new horizon in a Cash-Light India* , pp. 12-14.
[15] Sunny, K. (2017, April). Managing Banking More Human. *Digital Banking new horizon in a Cash-light Inida* , pp. 15-17.
[16] Tariq, N. (June 2018). *IMPACT OF CYBERATTACKS ON FINANCIAL INSTITUITIONS.* Pakistan: Journal of Internet Banking and Commerce.
[17] Website CERT-In https://www.cert-in.org.in/