A Brief Study about Security in the Financial Technology Sector

Anirudh Ramesh[1] **Devharsh Toshniwal**[2] **Pratham Sapra**[3]
B.Com F&A, Department of Professional Studies, Christ University, Karnataka, India
Harsh Dhanuka[4]
Department of Professional Studies, Christ University, Karnataka, India

Abstract

India is leap forwarding towards becoming one of the largest economies of the world. It has been the fastest growing country in the world for four years. The unprecedented growth also requires an equal growth in the availability of finance and the advancement of technology. While the advancement of both are highly important, looking at the current trends security of the data becomes a major factor in shaping further growth. Security enables the assurance of privacy of technology and its misuse. The most important step to enable security-first decisions begins with the awareness of it. This research paper looks into this particular aspect with a magnifying glass. The paper studies the attitudes of the consumers towards security and the care they give to their own financial information. The paper tries to understand and explain the different threats we face today, how many and to what extent people are aware of it and understand this information and take steps and actions to enable the expansion of safeguards that can be taken.

Keywords: India, Finance, Technology, Growth, Security

I. Introduction

The financial technology sector has come into prominence in the last decade. Covering various aspects ranging from e-payments to cloud computing for financial institutions, from digital banking to saving a financial institution from malicious cyber threats, the Fintech sector has expanded exponentially. With multiple startups beginning to emerge in this field, the world has started to take notice of this sector. As the world shifts to a paper-less economy, different kinds of issues, never faced before seem to have popped up. Fintech apps have begun to flood the market with 'me-too' approach which makes for a wide variety to choose from and lesser to differentiate. This, although seems healthy in terms of financial inclusion and the idealistic views of choice and lower costs of access, creates pressures and difficulty in terms of survival and performance. This trend seems to have impacted security breaches and poor awareness and campaigns taken out by these firms to inform the consumers of their authentication and security norms, very similar to how the mutual fund industry behaved a few decades ago while introducing new products. The low focus on security has shown its impact in the form of frequent data breaches and subsequent and implied loss of privacy of perhaps the most important aspect of a person – financial. However, the norm of the world and the historic trends have taught us that learnings from mistakes identified and the demand of the consumers for change and better services is what has always been the agent of change in an environment that is generally lax about the importance of security. With the help of this research, the aim to tap an area which is not widely read upon by college students. Everyone makes digital payments and are associated with Fintech every single day. However, the knowledge regarding this sphere is relatively less. The aim of this research is to improve this as there is a lot of potential in the Fintech sector. Awareness is key when it

comes to a sector like Fintech. The research essentially entails an outlook on how the knowledge of others can be improved on this sphere and how information furnished can be carefully dealt with in this particular area.

II. Review of Literature

(Lee & Lee, 2015) in their paper studied the changes in various patterns related with our consumption because of popularization and progress on mobile device and service. We can buy a necessary product anywhere and at any time during 24 hours. Through the change of patterns in our life, in recent years, Fintech attracts a lot of attention. Fintech is the fusion type of finance and technology. Industry fields related with Fintech are now proceeding well in America, England and china. Therefore, we studied the issues of Fintech, and described the industrial technology trends in this paper.

(Thomas, 2014) in his paper says the future of our economic activity is becoming increasingly digital. The significance of digital structural change however is, frequently underestimated. The banks' value-added processes and business models are impacted by digitisation and are not partly affected but comprehensively and they must be comprehensively adapted to the architecture of the digital age. The digitisation of structures, processes or business models is a far-reaching process and not an issue that should only be driven by IT departments. Due to changes in the entire value creation process it is more of a paradigm shift or a strategic core issue in the overall strategy that must involve all the decision-makers within the company. In many sectors and at many traditional firms urgent action needs to be taken in order to remain internationally competitive going forward. This is also the case for the financial sector.

(Ashish, 2013) says that internet security is a pervasive concern for all companies. However, developing the business case to support investments in IT security has been particularly challenging because of difficulties in precisely quantifying the economic impact of a breach. Previous studies have attempted to quantify the magnitude of losses resulting from a breach in IT security, but reliance on self-reported company data has resulted in widely varying estimates of limited credibility. Employing an event study methodology, this study offers an alternative approach and more rigorous evaluation of breaches in IT security. This attempt has revealed several new perspectives concerning the market reaction to IT security breaches. A final component of the study is the extension of the analysis to incorporate e-Security vendors and a fuller exploration of market reactions before and after the denial of service attacks of February 2000. The key takeaway for corporate IT decision makers is that IT security breaches are extremely costly, and that the stock market has already factored in some level of optimal IT security investment by companies

(Lee & Kim, 2015) say that recently in Korea, crowdfunding industry has been receiving a growing attention. Korean government tries to activate crowdfunding industry by increasing venture capital companies and hopes for economic activation as well. However, there are a lot of financial regulations and other related regulations which block their entry and hinder the growth of the market. The related law which could weaken the restrictions is still waiting for a vote. Since there are a lot of stakeholders in crowdfunding industry, it is hard to totally understand the complex and diverse crowdfunding ecosystem and find major factors

Keke Gai, Meikang Qui (2017) says Financial Technology is a new term that has come to the forefront in the Financial Services industry. It covers various aspects such as security and privacy issues, like threats and malicious attacks. This particular research paper talks about a survey that is conducted to find out the general consensus of users regarding FinTech. With a broader perspective in mind, this survey enables people to understand what the FinTech sector entails and how best to utilize it.

III. Research Design

The rationale behind choosing the aforementioned topic was to educate the researchers' peers and those reading this about the security measures in place in the Fintech sector. While there are a lot of issues that do arise, the research ideally focuses on increasing user awareness and help in mitigating security risks. The researchers' interest was always focused on developments in the financial sector and the financial technology was a new arena that garnered a lot of attention. With a lot of developments happening in the sector, especially in the security segment of it, the research was aimed to be focused on it.

To analyze the results of our research, the Shannon Index and Simpson Index have been used, which are frequently used in calculating biodiversity amongst species with qualitative data. The data that has been collected is highly qualitative. This has been further condensed into quantitative means by seeing the number of responses for a few specific patterns that have been identified. Before going into the details, a brief about the Shannon and Simpson indices are as follows:

Shannon Index - The Shannon Index is an informative statistic index. Shannon Index (H) assumes that all species are represented in a sample and that they are randomly sampled.

$$\text{Shannon Index (H)} = -\sum_{i=1}^{s} p_i \ln p_i$$

Where,

P stands for proportion

ln stands for natural log

n/N stands for individual and total number respectively.

Simpson Index - The Simpson Index is a dominance index, it gives higher weight to the common/dominant species. Simpson Index (D) grants rather less consideration to extreme values (rarer species).

$$\text{Simpson Index (D)} = \frac{1}{\sum_{i=1}^{s} p_i^{\,2}}$$

Usage of the indices –

The aforementioned indices have been used to calculate the diversity with the proportion of patterns found in the responses. After having calculated the diversity the top 7 patterns will be selected and indices will be computed.

Limitations –

1. The Shannon Index (H) assumes that all species are represented in a sample and that they are randomly sampled.
2. The Simpson Index grants less consideration to the extreme values/rarer species.
3. The research is based on a small sample size.
4. The sample size for the research was 450.

Research Questions:

What are the different security threats?

What is the general user awareness regarding security threats in the financial technology sector?

How much knowledge are the researchers going to gain to pass around to their peers when this particular research paper is completed?

Objective:

To understand, assess and form solutions to the threats the consumers of financial technology are exposed to in the current world scenario.

Alternate hypothesis (H_{mu}) –

- There is a relation between the location of the respondent and the awareness level of the respondent.

  People living in Bangalore are more aware about security in the Fintech sector in comparison to respondents from other locations.

Null hypothesis (H_0) –

- The hypothesis that there is no difference between the specified variables, in this case the fact that the existence of a relationship between the location of the respondent and awareness level is nonexistent.

Sampling:

The research has been conducted with the help of cluster sampling. Clusters are going to be chosen amongst our peers and amongst the public. Within these clusters, random sampling was used.

The questionnaire was the main research methodology to understand how aware users are.

Source of Data:

The source of data used in the research is primary in nature. The questionnaire has been linked below for references:

https://docs.google.com/forms/d/e/1FAIpQLSd8N8WQE9w3to03ZIwknTYWkhuk4KX4HSmV2NmwLkZYsuQ2yg/viewform?usp=sf_link

Data Analysis:

The major source of data crunching and analysis would be Microsoft Excel. The use of Shannon and Simpson indices enable us to analyze the data. The basic source of data is **primary** in nature. The Google form mentioned above was the questionnaire that was sent out to collect responses. The questionnaire contains the following questions:

Q1. How often do you use a mobile wallet/net banking/debit or credit card to make payments?
(Mobile Wallet eg: Paytm, Google Pay, PhonePe, etc.)

Particulars	Number of Responses	Code
Almost always	279	A
Only when there is no physical cash available	142	B
Never	29	C

Q2. Do you read all the authentication norms when using a FinTech app?

Particulars	Number of Responses	Code
Yes	55	A
No	154	B
Sometimes	181	C
What are authentication norms?	60	D

Q3. Are you comfortable with companies knowing your payment history and using those to advertise offers to you?

Particulars	Number of Responses	Code
Yes, as long as they are not too intrusive.	96	A
No, I deserve complete privacy.	198	B
Both, as long as I am in control of what gets used.	156	C

Q4. Is time taken to complete a payment important to you? Would it be okay if for small ticket purchases (Bills below Rs. 2000), there is lesser authentication and security measures provided?

Particulars	Number of Responses	Code
Yes, I do not like the time it takes to complete a payment through OTP or similar authentication methods for small purchases	85	A
No. Security is of utmost importance and the amount does not matter.	365	B

The responses to the above questions have been assessed and the input has been branched into responses from

a) Bangalore and
b) Other than Bangalore

Post branching, the Shannon and Simpson index were used. The top 7 patterns have been selected and the indices were computed.

Indices Calculation

Pi is Proportion
In is Natural Log
n/N being Individual and Total Number
In Bangalore

Pattern Examined	Number of individuals	n/N	Pi	$(Pi)^2$	In Pi	Pi In Pi
ACBB	27	27/144	0.1875	0.035156	(1.6740)	-0.31387
ABBB	27	27/144	0.1875	0.035156	(1.6740)	-0.31387
ACCB	22	22/144	0.1528	0.023341	(1.8786)	-0.28701
ABCB	19	19/144	0.1319	0.017409	(2.0257)	-0.26728
BCCB	18	18/144	0.1250	0.015625	(2.0794)	-0.25993
BBBB	18	18/144	0.1250	0.015625	(2.0794)	-0.25993
BCBB	13	13/144	0.0903	0.00815	(2.4046)	-0.21708
Total	**144**	**-**	**1.0000**	**0.1505**	**(13.8158)**	**(1.9190)**

Number of Patterns (s)= 7

N(Total No. of individuals)= 144

Σ (sum) of Pi^2= 0.1505

Sum of pi In pi= -
=1.9189

H=-(-.3138+-.3138+-.2870+-.2672+-
.2599+.2599+.2170)
=1.919

D= 1/(0.3516+0.3516+0.2334+0.01741+0.0156+.0156+.0081)
=6.6461

Outside Bangalore

Pattern Examined	Number of individuals	n/N	Pi	$(Pi)^2$	In Pi	Pi In Pi
ACBB	20	20/69	0.2899	0.084016	(1.2382)	-0.3589
ABBB	12	12/69	0.1739	0.030246	(1.7493)	-0.30422
ACCB	13	13/69	0.1884	0.035497	(1.6692)	-0.31448
ABCB	6	6/69	0.0870	0.007561	(2.4418)	-0.21233
BCCB	6	6/69	0.0870	0.007561	(2.4418)	-0.21233
BBBB	8	8/69	0.1159	0.013443	(2.1550)	-0.24986
BCBB	4	4/69	0.0580	0.003361	(2.8473)	-0.16506
Total	**69**	**-**	**1.0000**	**0.1817**	**(14.5427)**	**(1.8172)**

Number of Patterns (s)= 7

N(Total No. of individuals)= 69

Σ (sum) of Pi^2= 0.1817

Sum of pi In pi= -
=1.8172

H=-(-.3589+-.3042+-.3144+-.2123+-.2123+-.2498+-
.1650)
=1.8172

D= 1/(0.2899+0.3025+0.0355+0.0075+0.0075+.0134+.0033)
=5.5040

IV. Findings and Suggestions

The research has been conducted keeping in mind the patterns mentioned below:

ACBB	ABBB
ACCB	ABCB
BCCB	BBBB
BCBB	

The most common combination/pattern that has been identified is ACBB which is as follows:

The respondent is someone who uses a mobile wallet almost always, reads authentication norms sometimes, wants complete privacy from companies who aim at knowing the respondent's and values security over time taken while making a payment. The findings suggest that this pattern is the most common amongst respondents in Bangalore and in the other locations as well.

The second most common pattern is ABBB, which entails respondents stating there are not aware authentication norms at all. Although being the second most common pattern, it is understood that this is far from the ideal pattern expected, whereby respondents are expected to read up authentication norms. A major suggestion is for awareness to be increased on authentication norms.

Only 55 out of 439 respondents had answered to the awareness question in an affirmative way. This highlights that only a mere 12.5% people out of the sample (which is mostly people from major cities), read authentication norms. This is a real problem, which needs to be tackled since the focus is on well-educated people who are not well read on the different platforms through which there money is transferred.

V. Conclusion

We can conclude that since the indices are greater for Bangalore, the pattern answer of Bangalore is more diverse.

The unawareness of the consumers on their part of not reading the authentication norms could mean the Fintech apps could misuse these norms/conditions in a variety of ways. Not limited to certain hidden conditions, which protect them from any liability even in case of misdoing in the future or misuse of money.

The two variables taken into consideration is the location of the respondent (Bangalore and "Other than Bangalore") and the ACBB pattern is the ideal pattern to be followed. There is no existence of a relationship between the location of the respondent and the awareness level. There is not sufficient evidence to reject the null hypothesis.

VI. Bibliography

1. Ashish, G. (2013). *Internet Security*.
2. Lee, S.-H., & Lee, D.-W. (2015). *Changes in Various Patterns.*
3. Lee, T.-h., & Kim, H.-W. (2015). *Crowdfunding.*
4. Thomas, F. D. (2014). *Furure of our Economic Activity.*