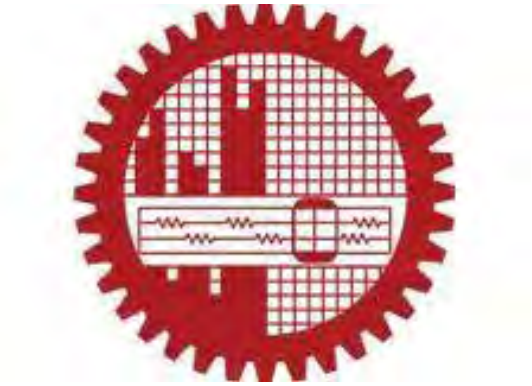
FRAMEWORK FOR EVALUATING FACTORS CONTRIBUTING TO FAILURE OF IT SYSTEM: A CASE OF BANKING INDUSTRY

by

S. M. Nazmul Hoq



MASTER OF ENGINEERING IN ADVANCED ENGINEERING MANAGEMENT

Department of Industrial and Production Engineering

BANGLADESH UNIVERSITY OF ENGINEERING AND TECHNOLOGY

August, 2020

FRAMEWORK FOR EVALUATING FACTORS CONTRIBUTING TO FAILURE OF IT SYSTEM: A CASE OF BANKING INDUSTRY

by

S. M. Nazmul Hoq

MASTER OF ENGINEERING INADVANCED ENGINEERING MANAGEMENT
Department of Industrial and Production Engineering
BANGLADESH UNIVERSITY OF ENGINEERING AND TECHNOLOGY
August, 2020

CERTIFICATE OF APPROVAL

The thesis titled "Framework for Evaluating Factors Contributing to Failure of IT System: A Case of Banking Industry" submitted by S. M. Nazmul Hoq, Roll No.: 1014082130F, Session: October-14, has been accepted as satisfactory in partial fulfillment of the requirement for the degree of Master of Engineering in Advanced Engineering Management on August 26, 2020.

BOARD OF EXAMINERS

1. Dr. Syed Mithun Ali — Chairman
   Associate Professor — (Supervisor)
   Department of Industrial and Production Engineering
   BUET, Dhaka

2. Dr. Abdullahil Azeem — Member
   Professor
   Department of Industrial and Production Engineering
   BUET, Dhaka

3. Dr. Sultana Parveen — Member
   Professor
   Department of Industrial and Production Engineering
   BUET, Dhaka

CANDIDATE'S DECLARATION

It is hereby declared that this thesis or any part of it has not been submitted elsewhere for the award of any degree or diploma.

S. M. Nazmul Hoq

This Work is Dedicated to My Family

Table of content

List of Figures

List of Tables

List of Abbreviations

SCM	: Supply Chain Management
NBFI	: Non-Bank Financial Institution
IT	: Information Technology
ATM	: Automated Teller Machine
TOPSIS	: Technique for Order of Preference by Similarity to Ideal Solution
FMEA	: Failure Mode and Effect Analysis
SC	: Supply Chain
BBS	: Bangladesh Bureau of Statistics
FY	: Fiscal Year
GDP	: Gross Domestic Product
ICT	: Information and Communication Technology
BASIS	: Bangladesh Association of Software and Information Services
LC	: Letter of Credit
SWIFT	: Society for Worldwide Interbank Financial Telecommunication
RTGS	: Real Time Gross Settlement
RPN	: Risk Priority Number
S	: Severity
O	: Occurrence
D	: Detection Difficulty
T	: Time
C	: Cost
CKC	: Cyber Kill Chain
USA	: United States of America
ROA	: Return On Asset
PIS	: Positive Ideal Solution
NIS	: Negative Ideal Solution
CIRT	: Computer Incident Response Team
BCC	: Bangladesh Computer Council
ITIL	: Information Technology Infrastructure Library

Acknowledgement

All praises go to the Almighty Allah who is most merciful, most beneficent, for Allah‟s boundless grace in successful completion of this thesis.

At the very beginning the author expresses his sincere gratitude and profound indebtedness to his thesis supervisor Dr. Syed Mithun Ali, Associate Professor, Department of Industrial and Production Engineering, BUET, Dhaka-1000. His affectionate guidance, valuable suggestions and inspirations throughout this work made this study possible. The author likes to thank all teachers of the Department of Industrial and Production Engineering BUET for their cooperation in performing this research.

The author is also indebted to his life companion and IT consultant, Nishat Afrose for her valuable support, suggestions and inspirations in performing this thesis work. The author would like to express his gratitude to several employees of Banking and IT industry in Bangladesh.

Finally, the author would like to thank all of his friends for their cooperation and suggestions to complete the thesis timely. The author would also like to extend his intense thanks to his parents whose continuous inspiration, sacrifice and motivation encouraged him to complete the thesis successfully.

Abstract

This thesis investigates the factors contributing to the failure in the IT system of the banking industry of Bangladesh. 32 experts having a different level of expertise in the respective field were consulted for their feedback. Based on the experts‟ opinions and weight on the specified evaluating criteria, an analysis was conducted using a rough set theory to produce the framework of the IT system‟s failure factor for managers of the banking sector in order to make a crucial decision. Based on the issues faced by the banking sector lately, various factors were prioritized to facilitate managers with a framework for addressing failures accordingly. In this study, an extended approach with the integration of rough set theory and TOPSIS is demonstrated. The goal is to develop a model using multi-criteria decision-making method for analyzing the failure factors of the IT system in the banking industry. This work addresses effectiveness and accuracy, considering vagueness and subjectivity of experts‟ opinions. The proposed framework is expected to motivate the managers of corresponding fields to identify the factors responsible for the failure of the IT system in the banking industry and hereby, prioritize them accordingly. Financial experts can further raise queries regarding the framework, which can be resolved by discussing with IT personnel.

Chapter 1
Introduction

1.1 Introduction

The economy is the driving force of the modern world, where IT plays a vital role. Incorporation of technology to formulate business is no longer a new concept; in fact the financial market and banking industry largely depends on IT. Research shows that, cost effective banking transactions can be conducted through e-channel only (Nishath & Selvarani, 2015). With the growth of modern IT and its proper utilization, the traditional banking system has experienced radical change. Nowadays, dependency on information technology systems without proper knowledge of execution poses a threat to this sector. As a result, these can incur monetary, reputational as well as information loss (Mohammed et al., 2020) if any failure remains unchecked.

Service Supply chain management (SCM) assists service enterprises by optimizing core business, minimizing expenses, improving service quality and so on (Sun et al., 2015). Moreover, banks and other Non-Bank Financial Institutions (NBFI) have experienced a paradigm shift over the past few years. Even now, IT plays a prominent role in the digitalization of the banking systems, meeting market demands, and maintaining a healthy competition with the competitors (Zhu et al., 2004). Countries around the globe are taking technology based fiscal measures and posing extensive monetary policy to evade plausible economic contraction. As per World Bank report released on August, 2020; the global economy is positively being transformed by the rise in adoption of digital business models and usage of digital financial services.

With the help of modern technology, the management information system in the banking sector has been strengthened. IT systems have significantly improved the business, gradually making it dependent on the system itself (Magklaras & Furnell, 2001). Furthermore, certain incidents of security breach have led to plausible misuse. For better performance and output optimization, adequate training, and counseling for information literacy are inevitable for both service providers and customers.

Experts suggested that identifying and ranking the failure factors could help them to prioritize the issues in the future (Yu et al., 2017).

In this age of IT, banking is not merely confined to the banks; along with the development of information and communication technology, financial institutions are executing transactions via deploying agents as well as smart phone-based applications for their customers. Hence services are no longer limited by distance or physical entity, whereas it is now a matter of coverage only. Considering the case of banks in Bangladesh, versatile transformation in transaction and inauguration of services is observed. For the expansion of digital financial services in order to spur economic growth, the banking sector of Bangladesh has taken multifaceted initiatives. Now, people have embraced internet banking more than ever. For that, the authority encourages fund transfer through internet banking to uplift IT-based banking services. Extended transaction limit, ceiling per transaction and transactions per day are some measures to execute and promote such decision.

Although the technology being a propelling factor of the economy, there exist threats and failures to safeguard the business due to its loopholes. Apart from the infamous scam that took place between 2010 and 2012, the 2016 cyber heist and recent automated teller machine (ATM) theft of 2019 corroborate that this financial sector is on the verge of security abuse. Addressing technical issues and business confidentiality is not enough, but a continuous effort to keep an updated security system is essential. Indeed, improving preventive measures can minimize collateral chances rather than regular troubleshooting.

Because of the proliferation in financial as well as the software industry of Bangladesh, escalated demand for technical security is pervasive (Jingxiong, 2020). This study collects information from several banks and software firms of Bangladesh intending to formulate a framework to prioritize the predetermined failure issues. Experts of various disciplines share their experiences focusing on the main essence of the project. The goal is to gather and share valuable experienced knowledge for the development of the IT sector that can assist in minimizing the security risk of the financial sector.

1.2 Research Gap and Motivation

It is observed that although the rest of the world is well aware of financial safety and security, there has been a surprising lack of study in the corresponding field especially in Bangladesh.

There was an incident of burglary by digging a tunnel into a bank‟s vault in 2014, since then embezzlement of money has taken versatile dimension with the inclusion of technology. The Letter of Credit (LC) system scam of Tk 36.48 billion between 2010 and 2012 is an exemplary one. Unscrupulous officials and business people collaborated to exploit the LC system with forged documents in the name of bogus companies. This shook up the trust of customer s on the banking system as a whole. In 2016, another set-back hit the financial sector at the pivot point and eventually transferred US $101 million to two countries by infecting malware. Although, US $20 million has been fully recovered from one country, as of 2018 US $63 million is yet to recover from the other. Initially, the target was to transfer US $951 million, which was discovered later from the SWIFT message. Society for Worldwide Interbank Financial Telecommunication, known as the SWIFT network was connected with Real Time Gross Settlement (RTGS), for local transaction in 2015. Hackers exploited the vulnerable SWIFT-RTGS connection illegally; the incident is commonly known as the biggest ever cyber heist. Unlike traditional hacking of the account holders‟ login credentials, this attack targeted the Bank‟s credentials by infecting with malware. Day by day, just like banks, NBFIs are also planning to launch ATM services. Yet during June, 2019, 9 ATM booths of a bank have encountered a scam. The syndicate has embezzled Tk 14 lakh. Moreover, experts being doubtful of whether the syndicate exploited the server issue or the fault of the bank‟s ATM software prove a lack of their information literacy. Therefore, upgrading the automation and management information systems was one of the critical suggestions to resolve the alarming issue of Banks and NBFIs.

However, literature hardly provides any evidence of work that recognizes and ranks various failure factors of this service supply chain from the context of information technology in Bangladesh. Despite the groundbreaking growth of this

industry, there have been some lacks in previous studies to establish a model to address the problems in the context of Bangladesh.

Hence, this work aims to cover the research gap of the targeted financial sector when it is vulnerable to IT security abuse. The main purpose of this research is to recognize as well as analyze the failure issues of technology in the field of banking and software industry. In this study, a rough Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS) based Failure Mode and Effect Analysis (FMEA) approach has been used for effective identification and prioritization of the most significant failures.

To implement the proposed rough-TOPSIS framework, a case study on several banks and software firms in Bangladesh is carried out.

1.3 Objectives of the Present Work

The purpose of this thesis is to identify and prioritize the IT failures of the service supply chain (SC) in the Banking sector of Bangladesh. The specific objectives of this project are:

1. To identify factors contributing to the failure of the IT system in the banking industry.
2. To propose a rough-TOPSIS framework to evaluate the failure factors of the IT system in the banking industry.
3. To compare the findings with the IT system failures of software support systems as reported in the literature.

1.4 Organization of the Thesis

The thesis is organized into five chapters including this one. The chapters are structured in the following way:

Chapter 1 gives the motivation and objectives of this thesis.

Chapter 2 presents the literature review of information system and banking industry, an overview on top issues of this sector in Bangladesh.

Chapter 3 gives the research methodology. Besides, an overview of rough set theory, rough TOPSIS based FMEA approach and application of rough-TOPSIS method is illustrated in Chapter 3.

Chapter 4 describes the implementation of developed framework. Results, discussions on findings are included in this chapter.

Finally, conclusions, managerial implications and recommendations with the future scope are presented in Chapter 5. At the end of the thesis, references and appendix are presented.

Chapter 2
Literature Review

2.1 Contribution of Service Supply Chain to the Economy of Bangladesh

The introduction of technology has an influence over our everyday life at large. It is a blessing of modern technology that provided us with functional and utility gadgets, which made our life cozy. Technology has brought about noteworthy variation in education, communication, business and commerce, health industry, governance etc. This way technology managed to form global information network that often used to predict human interactions with the help of artificial intelligence (AI) and big data.

According to the Bangladesh Bureau of Statistics (BBS), service sector of Bangladesh comprised 49.22% of total GDP with a growth rate of 6.175% in 2012, whereas in 2015 the contribution was 56.35% and it reached 52.11% by a slight decrease in 2017-18. 2018-19 experienced 51.26% contribution in the Gross Domestic Product (GDP), especially the economic sector, which showed a rise in nature (BBS, 2018). As per the central bank‟s economic trends report of August 2020, credit card and debit card transactions decreased with an exception of its usage increase in e-commerce. Service requires a managerial survey and sector-wise analysis because of its intangibility and diversity which consequently inaugurates the idea of the service supply chain (Choudhury et al., 2020). Whatsoever, the selection of an appropriate mathematical model for the evaluation of service supply chain properties is challenging due to the qualitative nature of supply chain failures (Aliakbari Nouri et al., 2019).

This era of sustainable development urges economic and technological emancipation. The participation of the young generation has paved remarkable success in the software and IT sector of Bangladesh. Although the sector is in its growth phase of the life cycle, its contribution to the economy is yet to be up to the mark. The involvement of mass people and their technological literacy is a prerequisite to flourish the overall economy. According to the BBS latest economic

review 2019, technological services contributed 2.58% of the GDP in FY 2017-18, having an approximate growth of 7.56% for the running year. Information and Communication Technology (ICT) policy of 2002 was indeed a contemporary step taken by the government of Bangladesh. Now country-wide e-governance, e-commerce, banking, software development and major parts of utility services are ICT based. Investment is on the rise, both in terms of monetary as well as intellectual for this sector.

This research takes into account the issues raised by IT/IS based banking. The banking service sector interacts with several other sectors for the growth of the economy. Banks and other Non-Bank Financial Institutions (NBFI) hold the lion‟s share of Bangladesh‟s economy. Including a total of 51 national banks with 9 international banks and 34 NBFI, the sector shows prominent growth in the economy of Bangladesh. The role of financial institutions is undeniable. In recent years as a major part of the service supply chain, banking has spread all around the country by means of various products like online banking, mobile banking, agent banking etc. This vastness has gathered opportunities as well as threats. Fraudulent activities are quite common in the case when the victim has poor technical knowledge.

2.2 Conceptualization of Failure Factors of IT System

Failure, an inseparable part of the supply chain, is mainly occurred due to uncertainty and unfavorable consequences of events. In the case of technically delicate and financially vital sectors, a very narrow margin of error has to be maintained.

Risks can be discussed as potential failure factors. Experts of diversified sectors opine to identify the failure factors. Table 2.1 summarized the failure factors considered in different studies.

Table 2. 1 Summary table of failure factors considered and their sources

No.	Failure factors	Source
FM1	Database Hack	(Nakatani et al. 2018), (Mukherjee and Sengupta 2016) and (Lu and Huang 2013)
FM2	Server failure	(Randazzo et al. 2005)
FM3	Virus Effect	(Lin & Lin, 2019) and (Boyson, 2014)
FM4	Cipher to Plain Text Malfunction	(Khanna, 2015)
FM5	Character Misspelled	Proposed in this research
FM6	Wrong Message Transcription	Proposed in this research
FM7	Peripheral Error	Proposed in this research(Figge et al., 2002)(Figge et al., 2002)(Figge, Hahn, Schaltegger, & Wagner, 2002)(Figge, Hahn, Schaltegger, & Wagner, 2002)(Figge, Hahn, Schaltegger, & Wagner, 2002)(Figge, Hahn, Schaltegger, & Wagner, 2002)(Figge, Hahn, Schaltegger, & Wagner, 2002)
FM8	Broadcast Data Error (Up/Down) link Failure	(Wu et al., 2009)(Wu et al., 2009)(Wu, Tzeng, & Chen, 2009)(Wu, Tzeng, & Chen, 2009)(Wu, Tzeng, & Chen, 2009)(Wu, Tzeng, & Chen, 2009)(Wu, Tzeng, & Chen, 2009)(Wu, Tzeng, & Chen, 2009) (Molero et al., 2002)
FM9	Cyber Attack	(Lai et al., 2017)
FM10	Third Party Intervention	(De Gusmão et al., 2016)
FM11	Network Interruption	(Zhu et al., 2004),

- **Database Hack**

For any service, the supply chain database comprises of comprehensive links, which can be used to analyze organization based risks (Nakatani et al., 2018). Amway-an American service organization revolves around its centralized database server. Serving the business points simultaneously with negligible slack, the IBM iSeries database is considered as part and parcel of the company (Mukherjee & Sengupta, 2016). Any hindrance to the process can compromise an efficient information system.

Loss of login credentials, settings, and logistics information may pose a threat to the business. Hereby, routine back up of database can abate the impact of database hack (Lu & Huang, 2013).

- **Server Failure**

Server is one of the vital parts as potential hackers sneak into it or infect it for their interest. In 2002, an international financial services company of the United States lost its 10 billion files that eventually affected more than 1300 companies‟ servers (Randazzo et al., 2005). Such a failure may often lead to another one. Prompt preventive measures, timely backups and proper recovering maneuvers can minimize the impact of loss. Failure of the server may yield to loss of information and thus pose a vital threat to the business.

- **Virus Effect**

Now-a-days organizations related to IT as well as financial sectors are susceptible to virus attack. Malware can broadly be of network-based and non-network based categories. In fact, 2016 cyber heist was initiated through malware.

Moreover, a cloud-based supply chain management system is getting popular even-though there is a chance of data storage damage through viruses (Lin & Lin, 2019). In order to scan viruses, a wide range of surveillance on IT systems and mechanisms similar to proxy server code repositories can be implemented (Boyson, 2014), which has evidentially found effective for steady SC control.

- **Cipher to Plaintext Malfunction**

Improper interpretation of cipher-text may lead to wrong decryption of a message. Though, cryptography protects sensitive data by encryption (Khanna, 2015), if deciphering is not executed according to the key, plaintext remains unearthed; hence, the main goal of encryption will hardly serve.

- **Character Misspelled**

Misspelling character of a message can often create great confusion: a commercial bank of Bangladesh misplaced decimal which ultimately resulted in enormous financial loss.

- **Wrong Message Transcription**

Unlike other significant failures, message transcription may seem trivial, yet it has a significant impact on proper communication among business sectors. Especially, the IT and software industry, including the financial sector of a country, is highly sophisticated; hereby, miscommunication can create a huge loss in the economy.

- **Peripheral Error**

Unintentional errors occurred due to input and output devices that can create failure of the IT system in the Banking or Financial industry. It is observed that unskilled and reluctant users, often being unaware of the importance of IT or software, continue the traditional practice, which is a major reason for peripheral errors.

- **Broadcast Data Missing (Up/Down) link Failure**

For a large network of storage area networks, chances of link failure increases, which may seem negligible in case of moderate loads (Molero et al., 2002). Accidental disconnections and electromagnetic interferences confront the network‟s reliability; hence, up/down link failure worsens performance.

- **Cyber Attack**

In the era of rapid globalization, cyber supply chain failure needs to be managed to assist IT as well as business executives for addressing various pitfalls. IT integration businesses like software industries, IT companies, and financial institutions emphasize on cyber security with utmost weight. Infected malware can be triggered unanimously for unauthorized action (Lai et al., 2017). Cyber criminals with an ill intention of financial benefits are an imminent risk to the service supply chain all over the world. 2016 cyber heist was a dark chapter for Bangladesh's economy.

- **Third Party Intervention**

An analysis of information system risk identifies deliberate external database attacks as of vital risk (De Gusmão et al., 2016). Human failure is the prime reason for middleman intervention, which can be categorized as security abuses. IT companies or software organizations are dependent on vendors, and some other third party to some extent. A security breach is possible when the financial benefit is involved, let alone be it for financial institutions.

- **Network Interruption**

Although a survey on the United States of America (USA) based bank yields return on asset- ROA and network system variables as mutually independent (Zhu et al., 2004), banking activities nowadays are mostly dependent on Information System. Indeed online transactions rely upon the network. Hence, even a slight failure of the network can create confusion for a large number of transactions.

Chapter 3
Methodology

3.1 Research Methodology

This research work focuses on identifying the failure factors and prioritizing them in the context of the banking industry of Bangladesh. Figure 3.1 illustrates the methodology of this research. The proposed research consists of five steps, as mentioned below.

Step 1: Identification of failure factors

The objective of this step is to generate a comprehensive list of failure factors of the IT system based on the events that might have an adverse impact on the banking industry. In this step, relevant service supply chain failure factors are identified from experts‟ input. A total of 11 failure factors of the IT system in the banking industry are identified from surveying the experts on the corresponding field (Table 2.1). After that, the crisp weights of failure factors are determined.

Step 2: Conversion of rough interval form using rough TOPSIS method

In this step, the crisp importance of failure factors is converted into a rough interval form. Then rough TOPSIS based systematic FMEA approach is implemented by converting constructed group decision matrix into the rough interval. Onwards, a weighted rough interval decision matrix is determined. The decision matrix goes through weighted normalization to be formulated in a rough number.

Step 3: Determination of closeness coefficient

In this stage, identification of positive ideal solution (PIS) and negative ideal solution (NIS) is executed. Then separation from PIS and NIS for failure modes is calculated, and afterward, the closeness coefficient is determined. To determine the

ranking order of all failure modes, a closeness coefficient is then defined. It is determined with respect to the criterion Severity (S), Occurrence (O), Detection Difficulty (D), Time (T), and Cost (C).

Step 4: Ranking of failure modes

Failure factors are ranked according to their importance. The closeness coefficient (CC) is the basis of this ranking. Risks are ranked so that managers can address issues accordingly.

Step 5: Conclusions, managerial implications and recommendations

Implementation of this thesis is mainly applicable when banking managers use it for problem-solving that generated from IT failures. Future scope and limitations of this work are also discussed in this section.

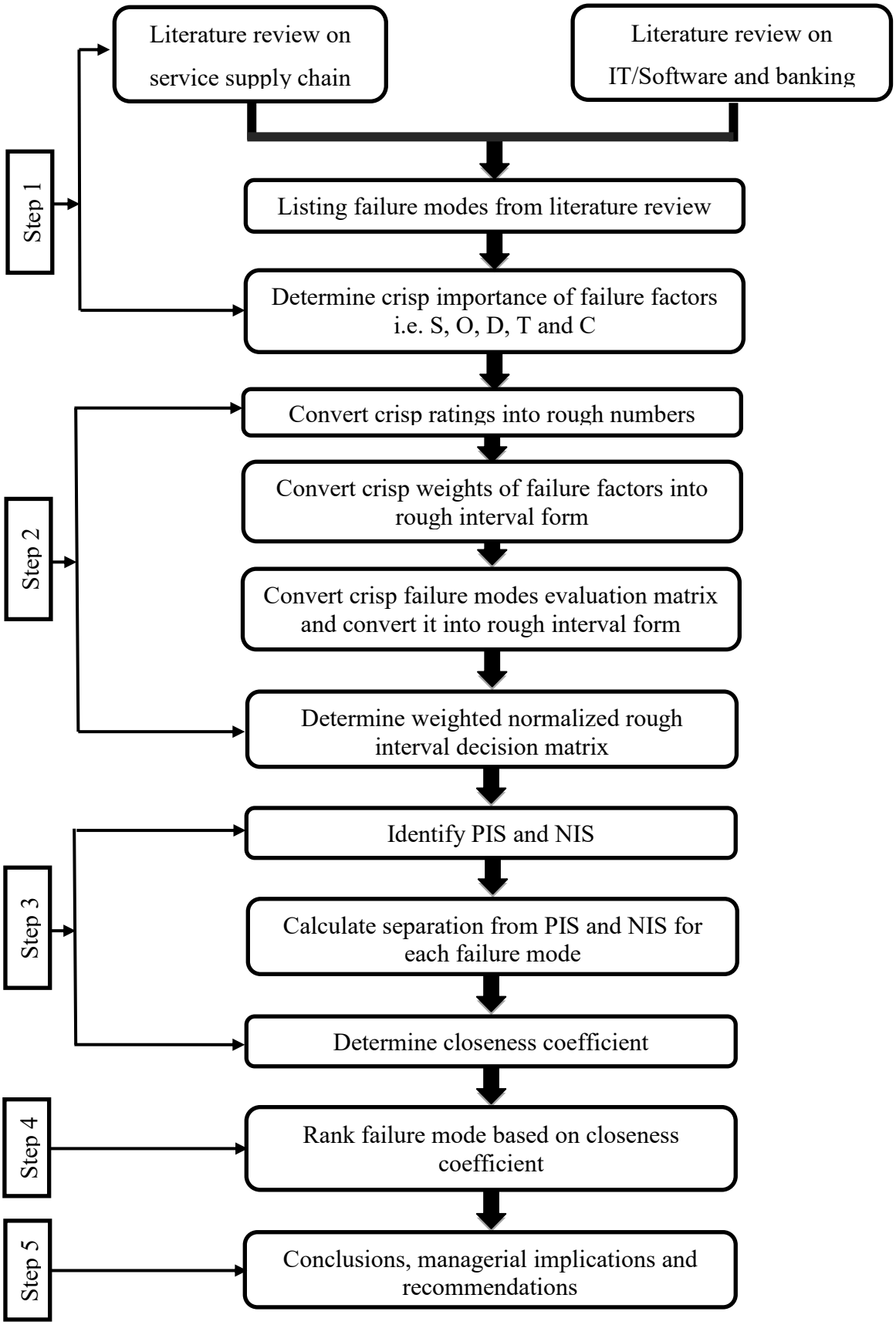


Fig. 3. 1 Overall approach of research methodology

3.2 Solution Methodology

In this section a novel framework on FMEA based rough TOPSIS method is presented.

3.2.1 FMEA approach based on rough TOPSIS Method

To prioritize the failure modes of IT system in banking sector, a flexible FMEA approach is presented. The rough TOPSIS method combines rough set theory with group TOPSIS. Subjectivity including uncertainty of failure mode evaluation is addressed by rough set theory. Whereas, rough TOPSIS solves crisp multiplication problems of conventional FMEA.

3.2.1.1 Determining rough interval weight of failure factors S, O, D, T and C

(1) Subsequently determining the failure modes, the experts are required to choose the crisp importance of criterion (S, O, D, T and C) among the scores 1–10. A score of 1 represents practically insignificant, while the score of 10 demonstrates practically relevant. Different scores are characterized similarly. Therefore, a crisp evaluation value can be achieved for failure factors weight.

$$w_j = \left[w_j^1, w_j^2, \dots, w_j^k, \dots, w_j^l\right]; j\text{= S, O, D, T and C} \quad 3.1$$

Where w_j^k represents the k^{th} expert assessment on the significance of the criterion of j. l represents the number of experts in the decision matrix.

(2) The rough number form is then derived from crisp importance with the formula in the appendix. By the following works rough interval form of w_j^k can be determined.

$$\text{RN}(w_j^k) = [w_j^{kL}, w_j^{kU}] \quad 3.2$$

Where L and U represent lower limit and upper limit of rough number RNw_j^k

The following works can help to determine the rough weight of criterion j $\overline{RN(w_j)}$.

$$w_j^L = \frac{(w_j^{1L} + w_j^{2L} + \cdots + w_j^{lL})}{l} \quad 3.3$$

$$w_j^U = \frac{(w_j^{1U} + w_j^{2U} + \cdots + w_j^{lU})}{l} \quad 3.4$$

j= S, O, D, T and C; w_j^L and w_j^U are lower limit and upper limit of rough weight $\overline{RN(w_j)}$ respectively.

3.2.1.2 Rough TOPSIS based framework of FMEA approach

(1) Construction of crisp failure modes evaluation matrix: At first, it is assumed that there are m failure modes FM_i (i = 1,2, … ,m) which is to be evaluated against assigned criteria C_j (j = S, O, D, T and C). Failure modes ratings with respect to criteria are then evaluated from multidisciplinary experts‟ input on conventional scores, in this case (1,2,3, … ,10). Assuming that l experts of an FMEA team are making decisions, considering as a multi-criteria decision-making problem the failure modes ranking in FMEA can be expressed in the form of evaluation matrix D as follows:

$$D = \begin{array}{c} \\ FM_1 \\ FM_2 \\ \vdots \\ FM_m \end{array} \begin{array}{c} \begin{array}{ccccc} S & O & D & T & C \end{array} \\ \begin{bmatrix} X_{1S}^k & X_{1O}^k & X_{1D}^k & X_{1T}^k & X_{1C}^k \\ X_{2S}^k & X_{2O}^k & X_{2D}^k & X_{2T}^k & X_{2C}^k \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ X_{mS}^k & X_{mO}^k & X_{mD}^k & X_{mT}^k & X_{mC}^k \end{bmatrix} \end{array} \quad 3.5$$

Where k=1,2,. . .,l and X_{ij}^k(i=1,2,. . .,m) is the rating of the k^{th} expert for the i^{th} failure mode with respect to the criterion j.

(2) Obtaining Rough group decision matrix: To obtain rough group decision matrix R, the crisp element X_{ij}^k in group decision matrix D can be converted into rough number form. Rough number form RN (X_{ij}^k) of X_{ij}^k can be executed with the help of equations listed in the appendix.

$$\mathrm{RN}\,(X_{ij}^{k}) = \left[X_{ij}^{kL}\ ;\ X_{ij}^{kU}\right] \tag{3.6}$$

Where L and U represent the lower limit and upper limit of rough number RN

Hence, a rough number form can be achieved as follows.

$$\mathrm{RN}\left(X_{ij}\right) = \left\{\left[X_{ij}^{1L}\ ;\ X_{ij}^{1U}\right],\left[X_{ij}^{2L}\ ;\ X_{ij}^{2U}\right],\cdots,\left[X_{ij}^{lL}\ ;\ X_{ij}^{lU}\right]\right\} \tag{3.7}$$

Using rough computation principles, the average rough interval can be acquired.

$$\overline{\mathrm{RN}\left(\mathrm{X_{ij}}\right)} = \left[\mathrm{X_{ij}^{L}}\ ;\ \mathrm{X_{ij}^{U}}\right] \tag{3.8}$$

$$\mathrm{X_{ij}^{L}} = \frac{(\mathrm{X_{ij}^{1L}} + \mathrm{X_{ij}^{2L}} + \cdots + \mathrm{X_{ij}^{lL}})}{\mathrm{l}} \tag{3.9}$$

$$\mathrm{X_{ij}^{U}} = \frac{(\mathrm{X_{ij}^{1U}} + \mathrm{X_{ij}^{2U}} + \cdots + \mathrm{X_{ij}^{lU}})}{\mathrm{l}} \tag{3.10}$$

Thus, the rough group decision matrix R can be obtained as follows:

$$R = \begin{bmatrix} [1,1] & [X_{12}^{L}, X_{12}^{U}] & \cdots & [X_{1m}^{L}, X_{1m}^{U}] \\ [X_{21}^{L}, X_{21}^{U}] & [1,1] & \cdots & [X_{2m}^{L}, X_{2m}^{U}] \\ \vdots & \vdots & \ddots & \vdots \\ [X_{m1}^{L}, X_{m1}^{U}] & [X_{m2}^{L}, X_{m2}^{U}] & \cdots & [1,1] \end{bmatrix} \tag{3.11}$$

(3) Determination of weighted normalized decision matrix in the form of rough number: Following normalization method is used to transform different criteria scales into a comparable scale:

$$X_{ij}^{'L} = \frac{X_{ij}^{L}}{max_{i=1}^{m}\{\max[X_{ij}^{L}, X_{ij}^{U}]\}} \tag{3.12}$$

$$X_{ij}^{'U} = \frac{X_{ij}^{U}}{max_{i=1}^{m}\{\max[X_{ij}^{L}, X_{ij}^{U}]\}} \tag{3.13}$$

The method mentioned earlier regarding normalization is designed to preserve the property of normalized interval numbers‟ ranging between [0, 1]. Afterward, the weighted normalized rough matrix can be calculated as follows:

$V_{ij}^{L} = W_{j}^{L} \times X_{ij}^{'L}$, i=1, 2, …, m; j= S, O, D, T, and C 3.14

$V_{ij}^{U} = W_{j}^{U} \times X_{ij}^{'U}$, i=1, 2, …, m; j= S, O, D, T, and C 3.15

(4) Now, Positive Ideal Solution (PIS) and Negative Ideal Solution (NIS) can be obtained as

$$V^{+}(j) = \left\{max_{i=1}^{m}\left(V_{ij}^{U}\right), if\ j \in B; min_{i=1}^{m}\left(V_{ij}^{L}\right), if\ j \in C\right\} \quad 3.16$$

$$V^{-}(j) = \left\{min_{i=1}^{m}\left(V_{ij}^{L}\right), if\ j \in B; max_{i=1}^{m}\left(V_{ij}^{U}\right), if\ j \in C\right\} \quad 3.17$$

Where $V^{+}(j)$ and $V^{-}(j)$ are PIS and NIS value with respect to criterion j. B and C are associated with benefit criterion and cost criterion respectively.

(5) Using the n-dimensional Euclidean distance equation, the separation of individual failure mode from the PIS can be calculated as follows

$$d_i^{+} = \sqrt{\left\{\sum_{j \in B}\left(V_{ij}^{L} - V^{+}(j)\right)^2 + \sum_{j \in C}\left(V_{ij}^{U} - V^{+}(j)\right)^2\right\}} \quad 3.18$$

Likewise, the separation from the NIS can be calculated as

$$d_i^{-} = \sqrt{\left\{\sum_{j \in B}\left(V_{ij}^{U} - V^{-}(j)\right)^2 + \sum_{j \in C}\left(V_{ij}^{L} - V^{-}(j)\right)^2\right\}} \quad 3.19$$

Once the d_i^{+} and d_i^{-} of individual failure modes FM_i have been calculated, a closeness coefficient is defined for determining the ranking order of identified failure modes. The closeness coefficient CC_i of the failure modes FM_i with respect to selected criterion (S, O, D, T, and C) is defined as

$$CC_i = \frac{d_i^{-}}{d_i^{-} + d_i^{+}} \quad 3.20$$

As CC_i approaches to 1, failure modes FM_i gets closer to the d_i^{+} and farther from d_i^{-}. The smaller the CC_i is, the severe risk of failure mode becomes. After that, the risk priority of identified failure modes can be determined in consistent with the closeness coefficient.

Chapter 4
Data Collection and Analysis

4.1 Data collection

The proposed methodology has then been applied to a real case study in order to rank the service supply chain factors associated with IT system failure of the banking industry in Bangladesh. Experts on the IT and software industry with years of experience in the banking industry have been selected unanimously for the survey. Existing literature, as well as 32 experts of versatile fields, have identified major failure factors. Eventually, they participated in ranking them as per the proposed methodology of the previous section. Experts spontaneously participated in the non-disclosure survey.

In this research, two steps have been followed for collecting the necessary data and information. In Step 1, based upon literature and managers‟ opinion, factors contributing to failure modes of IT system in the banking industry were identified, and in Step 2, the analysis of the identified failure factors with the help of experts‟ input was performed.

Prior to the phase of collecting data, specialists‟ panel of the pertinent industry having multidisciplinary professional experience was formed. Experts were selected of various range of experience and diversified field, that includes professionals of bank and other NBFI, software engineers, IT specialists and academics as well. Afterwards, the required data have been collected from the experts. The survey was initially conducted, using a questionnaire, over both online and offline as per the professionals‟ convenience. The respondents‟ professional summary is listed in Table 4.1. Their feedback was documented to develop and clarify the questionnaire. The analysis shows that majority of the experts are IT specialist of financial institutions, and most are having in depth professional experience.

Table 4. 1: The domain of experts and their professional overview

Domain of Work	Years of Experience			
	Up to 5	5-10	More than 10	Total
IT specialist of Financial Institutions	7	7	3	17
Financial Institutions	2	3	1	6
Software, IT professionals and academics	2	4	3	9
Total	11	14	7	32

The two-step data collection process is explained as below:

Step 1: Recognizing factors responsible for IT system failure in banks and NBFI

At first, from previous history and reports of relative organizations, eleven factors responsible for IT system failure in banks and NBFI have been identified. During the primary phase, the experts‟ panel was requested to make necessary modification or inclusion of any risk relevant to the failure of the IT/software system in the Bangladeshi financial sector. Subsequently, the responses were gathered from experts in order to finalize the list. Therefore, eleven possible factors were identified that are responsible for IT system failure of the financial sector in Bangladesh. The failure modes are listed in Table 4.2.

Step 2: Analysis of identified failure modes with the help of experts‟ opinion for ranking

The identified failure factors were ranked by implementing rough set theory and TOPSIS. For the analysis, a meeting with the expert panel was arranged at the very beginning to generate a basic idea. With the help of their feedback, crisp importance criteria and failure modes were listed in a table for the survey. After that using the experts‟ input, the ranking of failure modes was performed.

Table 4. 2 Potential IT system Failure modes for financial sector of Bangladesh

No.	Failure factors
FM1	Database Hack
FM2	Server failure
FM3	Virus Effect
FM4	Cipher to Plain Text Malfunction
FM5	Character Misspelled
FM6	Wrong Message Transcription
FM7	Peripheral Error
FM8	Broadcast Data Error (Up/Down) link Failure
FM9	Cyber Attack
FM10	Third Party Intervention
FM11	Network Interruption

Once the major potential failure modes are determined, subjective assessments of 32 experts in crisp variables are utilized to obtain the importance of failure factors (S, O, D, T, and C), which is determined according to the basic formula of rough set theory and rough number. The experts‟ perspectives on crisp ratings about failure modes regarding each failure factor are then determined.

4.2 Using Rough TOPSIS-based FMEA Ranking of The Failure Modes Risks

4.2.1 Failure factors' rough interval weight determination

At first the evaluating criteria are rated based upon the opinion of experts. Ratings were allotted on a scale of 1-10. Score 1 means least important, while score 10 is most important, other scores bear similar weight. Failure modes are then rated on the basis of different criteria based upon the opinion of experts.

Using formula of lower limit and upper limit listed in appendix, a rough number form of the crisp importance rating is calculated. A sample calculation, for better comprehension, is presented below. Let the crisp ratings for failure factor „Severity" according to 4 experts are [2, 4, 7, 7]

Lower Limit	Upper Limit	Rough Interval
$\underline{Lim}(2) = 2$	$\overline{Lim}(2) = \frac{1}{4}(2 + 4 + 7 + 7)$	[2,5]
$\underline{Lim}(4) = \frac{1}{2}(2 + 4)$	$\overline{Lim}(4) = \frac{1}{3}(4 + 7 + 7)$	[3,6]
$\underline{Lim}(7) = \frac{1}{4}(2 + 4 + 7 + 7)$	$\overline{Lim}(7) = 7$	[5,7]
	Average Rough Interval	[3.75,6.25]

As per equations, the average rough intervals are determined. Likewise, for different failure factors, rough number forms and average rough intervals can also be acquired as shown in Table 4.3. The rough failure modes evaluation matrix is presented in Table 4.4.

Table 4. 3 The rough interval and normalized weights for S, O, D, T and C

Risk Factor	Rough interval	Normalized rough weight
	$[Low \quad High]$	$[Low \quad High]$
Severity	[6.422 8.949]	[0.680 0.947]
Occurrence	[6.619 9.446]	[0.701 1.000]
Detection Difficulty	[6.356 8.880]	[0.673 0.940]
Time	[6.080 8.418]	[0.644 0.891]
Cost	[4.985 7.626]	[0.528 0.807]

4.2.2 Using rough TOPSIS-based FMEA ranking of the failure modes risk

The failure modes‟ crisp decision matrix is converted as a rough group decision-making matrix; hence the failure modes‟ rough interval evaluation is determined as shown in Table 4.4.

Afterward, the rough form of a weighted normalized decision matrix is obtained. The evaluation matrix of rough failure modes is normalized in Table 4.3, and the weighted normalized rough matrix is then determined. In Table 4.5, eleven failure modes‟ rough weighted normalized matrix is depicted.

Table 4. 4 The evaluation matrix of rough failure modes

No.	S	O	D	T	C
FM1	[7.989 9.178]	[5.566 8.946]	[6.200 9.467]	[6.726 9.458]	[5.320 8.671]
FM2	[7.225 9.480]	[5.866 8.719]	[5.486 8.911]	[6.246 9.326]	[5.790 9.169]
FM3	[5.728 7.779]	[4.693 7.613]	[5.389 8.077]	[5.797 7.896]	[5.110 8.073]
FM4	[4.521 7.406]	[4.556 7.230]	[4.719 7.256]	[4.336 7.127]	[3.744 6.600]
FM5	[4.415 7.629]	[4.479 7.207]	[4.302 6.496]	[3.929 6.815]	[3.489 6.386]
FM6	[5.451 7.965]	[4.121 7.190]	[4.335 6.876]	[4.822 7.605]	[3.917 6.735]
FM7	[4.491 6.868]	[4.251 6.986]	[3.639 6.886]	[3.914 6.377]	[3.493 6.353]
FM8	[5.647 8.331]	[5.027 8.366]	[4.290 8.302]	[5.001 7.653]	[4.129 6.791]
FM9	[8.334 9.598]	[6.249 9.207]	[7.596 9.496]	[6.374 8.870]	[6.402 9.079]
FM10	[5.682 8.209]	[4.794 7.591]	[3.999 8.137]	[5.331 7.724]	[4.676 6.939]
FM11	[6.628 8.709]	[6.121 8.463]	[5.507 8.354]	[5.677 8.221]	[4.444 8.281]

Table 4. 5 The rough weighted normalized matrix of failure modes

Weighted Matrix	Severity		Occurrence		Detection		Time		Cost	
	Low	High	Low	High	Low	High	Low	High	Low	High
FM1	0.566	0.906	0.424	0.972	0.439	0.937	0.458	0.891	0.306	0.763
FM2	0.512	0.936	0.446	0.947	0.389	0.882	0.425	0.879	0.333	0.807
FM3	0.406	0.768	0.357	0.827	0.382	0.800	0.395	0.744	0.294	0.711
FM4	0.320	0.731	0.347	0.785	0.334	0.718	0.295	0.672	0.215	0.581
FM5	0.313	0.753	0.341	0.783	0.305	0.643	0.267	0.642	0.201	0.562
FM6	0.386	0.786	0.314	0.781	0.307	0.681	0.328	0.717	0.225	0.593
FM7	0.318	0.678	0.324	0.759	0.258	0.682	0.266	0.601	0.201	0.559
FM8	0.400	0.822	0.383	0.909	0.304	0.822	0.340	0.721	0.238	0.598
FM9	0.590	0.947	0.476	1.000	0.538	0.940	0.434	0.836	0.368	0.799
FM10	0.402	0.810	0.365	0.824	0.283	0.806	0.363	0.728	0.269	0.611
FM11	0.469	0.860	0.466	0.919	0.390	0.827	0.386	0.775	0.256	0.729

PIS and NIS are identified using the formula presented in the appendix. The failure factors S, O, D, T, and Care all related to cost criterion according to the framework that the FMEA approach proposed. In Table 4.6, the Positive Ideal Solution and Negative Ideal Solution are recorded.

Then the segregation of each failure mode from the Positive Ideal Solution and Negative Ideal Solution is calculated.

Table 4. 6 The PIS and NIS of the rough weighted normalized matrix

	Severity	Occurrence	Detection	Time	Cost
PIS	0.313	0.314	0.258	0.643	0.266
NIS	0.936	1.000	0.940	0.458	0.891

4.2.3 Result & Comparisons

According to the RPN method based conventional FMEA, the weights of five failure factors are considered to be of equal crisp value. In the process of determining the weights of failure factors, the crisp value-form of weights lacks the subjectivity and ambiguity inherent in it. Software experts‟ opinion delivers the same result as well.

Table 4. 7 d_i^+, d_i^-, closeness coefficient and rank of each failure mode

No.	Failure mode	d_i^+	d_i^-	CC_i	Rank
FM1	Database Hack	1.116	0.848	0.432	2
FM2	Server failure	1.086	0.889	0.450	3
FM3	Virus Effect	0.874	1.003	0.534	6
FM4	Cipher to Plain Text Malfunction	0.781	1.083	0.581	9
FM5	Character Misspelled	0.750	1.107	0.596	10
FM6	Wrong Message Transcription	0.788	1.083	0.579	8
FM7	Peripheral Error	0.715	1.142	0.615	11
FM8	Broadcast Data Error (Up/Down) link Failure	0.965	1.036	0.518	5
FM9	Cyber Attack	1.157	0.746	0.392	1
FM10	Third Party Intervention	0.899	1.058	0.541	7
FM11	Network Interruption	0.995	0.897	0.474	4

However, the literary work of developing countries regarding failure factors is not in abundance, unlike the developed one (Amid et al., 2012). Contemporary evaluation is essential to analyze such a pristine scenario. It is identified from the case study of the IT/IS industry that qualitative factors such as suppliers, human resources, management, process, institution, and specialties are responsible for the failure. The synchronization of IT/software with the business is undoubtedly an essential strategy to prevent failures from occurring. For any tech industry, there are challenges to meet deadlines, and for that team, the effort has no alternative.

Dependence on the suppliers or supporting business stakeholders of the supply chain is inevitable. For a country like Bangladesh, where intra-organizational or even inter-departmental co-ordination is tough to achieve, it is quite frequent to face threats from the external part of the supply chain. Managerial, technical and processing flaws are responsible for failures as well.

Furthermore, a study on software development teams reveals that booming farms are supposed to develop cutting edge products while retaining maximum satisfaction among team members with respect to the products and the team (Tsirakidis & Felix, 2009). Lack of consistency in methodological progress and unprocessed data of mail lists are found as the failure factors of the software teams. The research found no evidential link between unsuccessful project rate and work volume (Emam & Koru, 2008), though, on the contrary, software industries believe otherwise. In reality, change of objective is vitally responsible for most project failures. Apart from that, poor management and lack of synchronization between IT and management were found to be responsible for failures.

4.3 Managerial Implications

Reducing various failures in the service supply chain is a crucial task for achieving the company‟s success, especially when the market is of a competitive financial industry. For that reason, it is essential for managers to recognize the failures and, thus, take proactive measures to minimize the impact. The primary contribution of this study is the identification and evaluation of service supply chain failure factors of the IT system in the financial sector. This study will assist the managers in identifying the crucial factors contributing to the failures of the IT system in the banking industry and hereby, will guide the managers to minimize the effects of the failures. It will be easier for the managers to take proactive policies for reducing failures in the financial sector once failure factors are identified and prioritized. Some issues for assisting managers in reducing the occurrence of IT failures can be listed as follows:

- Interdepartmental differences of the organization may lead to a lack of proper co-ordination. Personal issues of top management impede largely to mass development. Moreover, the company‟s dependence on managers having a tech-phobic mentality ruins the culture of digitalization and automation for unconditional security.
- From the managerial context, it is suggested to take appropriate measures and proper caution of IT security to minimize the loss of potential threats.
- Moreover, managers need to apprehend multidisciplinary failure factors for improving supply chain efficiency and effectiveness. This research will assist in the context of preferences of failure factors. The ranking established by this research would be useful for identification of failure factor as well as prioritization process, and thus, it will also be handy as a model for evaluating and comparing failure factors using FMEA based rough TOPSIS in an uncertain environment for the augmentation of the efficiency of the supply chain in multidisciplinary sectors of Bangladesh.

4.4 Discussion and Validation

From Table 4.7, it is observed that cyber-attack, database hack risks, server failure, network interruption, broadcast data error, and virus effect possess the top six positions among the failure factors of the IT system in the financial sector of Bangladesh.

For flexible multi-criteria decision modeling, the framework integrates the strength of rough set theory to tackle vagueness and the merit of the TOPSIS assessment structure. The proposed rough TOPSIS based on FMEA evaluated the failure modes except for prior information and made the execution of the FMEA process easy (Song et. al. 2013). In order to deplete process diversity FMEA is proven to be useful in recognizing opportunities (Christopher & Lee, 2004).

Cyber-attacks pose a threat to the multidimensional sector, while most of the financial activities are largely dependent on the internet. Though efficient business management and automation of processes may induce operational virtue (Subramani, 2012), cloud computing is likely to secure credentials, yet making it vulnerable to

some extent. To detect and mitigate banking Trojan, a Cyber Kill Chain (CKC) based taxonomy can be implemented (Kiwia et al., 2018). Software and other IT industries of Bangladesh are susceptible to such attacks as well, hence to protect both financial and IT sector, combined effort is a must.

Moreover, the database of a financial institution is considered as the organization's information assets having financial value. Human intervention and ill motives are responsible for database failure. Information of the service supply chain industry is the key to several access levels. Loss of information may yield to ineffective business (Mukherjee & Sengupta, 2016). Researchers previously dealt with accurate information but due to the ambiguous nature of human verdict, experts prefer rhetoric over deterministic data (Roy et al., 2018). Although different organizations maintain data-center on their own responsibility, the risk of security and data loss still sustains.

Server failure can create major impedance in banking operations. Such risks must be addressed tactfully to minimize service supply chain failure. Server failure holds the third position with a closeness coefficient value near to the value of database hack. Report on economic review and Bangladesh Bureau of Statistics (BBS) shows an upward trend in online banking. Monthly economic trends of February 2020 issued by Bangladesh Bank show an upward tendency of banking transactions through the internet, mobile phones and nominated agents. Indeed, among private commercial banks, the popularity of ATM is sky-high. It is suspected that the ATM fraud of 2019 was conducted through a server hack. While determining the consequences of factors like cyber-attack, database hack or server failure, vagueness is a common trait. Hence, the uncertainties were addressed according to preferences, whence the fickleness of assessment was controlled by the proposed framework (Pamučar et al., 2018).

The banking sector has made significant progress in the cyber security sector. However, this sector lacks self sustaining capability of identifying, assessing, and forecasting such threats. Only a few financial organizations use locally developed core banking software, rather depend on foreign software which compels them to outsource IT services yielding to augmented cyber security risks. Third parties involved in financial technological infrastructure management could be a weak link

for many banks. The banks do not have adequate manpower to bolster IT and cyber security. Patronizing in-house skilled IT personnel could assist reducing this threat.

With the growing usage of technology, introduction of new financial technology has become frequent. Hence there is no alternative of collaborative measures on using up-to-date technology and IT audit. Cloud based data storage is also susceptible to hacking. Suspicious e-mail, unauthorized USB usage, malicious site access, pirated software usage are identified as prime sources of cyber security breach. Computer Incident Response Team (CIRT) of Bangladesh Computer Council (BCC) investigated potential threats in late 2020 according to Bangladesh Bank‟s warning to the local banks for a potential hack. The result of the investigation brings forth malwares found in three of the Internet Service Providers (ISPs) that provide network support to multiple banks. However, there is an alarming rate in the rise of ransomeware virus attack in Bangladesh (Haque & Bhuiyan, 2017), almost 2500 IPs of Bangladesh are already infected with ransomeware. Exact sources of a cyber attack are often hard to identify as it can happen from multiple sources simultaneously (Li et al., 2019). Staying vigilant and adhering to all the standardized protocol, updating virus signatures, updating firewall, cleaning endpoints regularly are the only way to thwart such attacks.

The financial market is growing faster than ever all around the globe. This business is no longer confined by the border. Threats of loss have always circumvented around this sector. With the development of technology, the threats took over new dimensions. Ardent measures to prevent such failure are required.

Chapter 5
Conclusions and Recommendations

5.1 Conclusions

Even though this one of a kind work delineates integral aspects of a multidisciplinary context, there lie inevitable challenges like a competitive market, insatiable customer, local as well as universal economic instability moreover, globalization. The potential risk of embezzlement and security breach in automation can pose a threat to the efficiency of one of the largest sectors of the service supply chain. Hence, the urge to know about failure factors, prioritize them accordingly, and check the potential threat is just demand of time.

- A rough-TOPSIS based FMEA model is proposed for evaluating the service supply chain failures in the context of multidisciplinary sectors like banking and IT/software industry.
- Existing literature review and experts‟ feedback help identifying of eleven relevant service supply chain failure factors in the context of the banking and IT/software industry. Subsequently, TOPSIS and rough-TOPSIS methods were used to rank these failures.
- The results show that cyber-attack, database hack, and server failure are the top three failures among the eleven failure factors.

5.2 Recommendations

Identification and segregation of failures from the incident can be executed according to the Information Technology Infrastructure Library (ITIL) report. Maintainability is one of the risk factors that, has not been considered as a basis in this study while analyzing the impacts of service supply chain failures. Therefore, there is a scope of further research on the impact of maintainability risks on the overall supply chain of the financial and/or software industry. However, the study is limited by the literature review and the factors assigned by the experts, which can be

developed by brainstorming. In fact, failure modes could be identified through prior multidisciplinary consensus without confining it by the experts‟ panel. Considered factors are mostly reactive type; proactive factors could also be taken into account. Moreover, design flaws and impact analyses have not been carried out in the study. Apart from the monetary point of view, cost criteria can also be of reputation or information type. Lack of literature in the corresponding field of Bangladesh leaves evident research gaps.

The thesis has demonstrated a framework implementing integrated TOPSIS and rough set theory for IT failure assessment in the context of the banking sector. Nevertheless, this framework can be used for failure assessment in other sectors as well, such as pharmaceuticals, health sector, telecom industry, airlines, processed food industry etc.

References

Aliakbari Nouri, F., Shafiei Nikabadi, M., & Olfat, L. (2019). Developing the framework of sustainable service supply chain balanced scorecard (SSSC BSC). *International Journal of Productivity and Performance Management*, *68*(1), 148–170.

Amid, A., Moalagh, M., & Zare, A. (2012). Identification and classification of ERP critical failure factors in Iranian industries. *Information Systems*, *37*(3), 227–237.

BBS, B. B. of S. (2018). *GDP report by Bangladesh Bureau of Statistics*. 1–10.

Boyson, S. (2014). Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems. *Technovation*, *34*(7), 342–353.

Choudhury, T. T., Paul, S. K., Rahman, H. F., Jia, Z., & Shukla, N. (2020). A systematic literature review on the service supply chain: research agenda and future research directions. *Production Planning and Control*, *0*(0), 1–22.

Christopher, M., & Lee, H. (2004). Mitigating supply chain risk through improved confidence. *International Journal of Physical Distribution and Logistics Management*, *34*(5), 388–396.

De Gusmão, A. P. H., E Silva, L. C., Silva, M. M., Poleto, T., & Costa, A. P. C. S. (2016). Information security risk analysis model using fuzzy decision theory. *International Journal of Information Management*, *36*(1), 25–34.

Emam, K. E., & Koru, A. G. (2008). A Replicated Survey of IT Software Project Failures. *IEEE Software*, *25*(5), 84–90.

Figge, F., Hahn, T., Schaltegger, S., & Wagner, M. (2002). The Sustainability Balanced Scorecard - linking sustainability management to business strategy. *Business Strategy and the Environment*, *11*(5), 269–284.

Haque, S., & Bhuiyan, T. (2017). Rise of Ransomware and the Readiness of Bangladesh. *International Journal of Computing, Communication and Instrumentation Engineering*, *4*(1), 0–4.

Jingxiong, D. (2020). *Analysis of Cyber Security Threat Environment and Information Security Analysis of Cyber Security Threat Environment and Information Security System of Financial Industry Under New Situation*. *January*.

Khanna, V. K. (2015). Implantable medical electronics: Prosthetics, drug delivery, and health monitoring. *Implantable Medical Electronics: Prosthetics, Drug Delivery, and Health Monitoring*, 1–453.

Kiwia, D., Dehghantanha, A., Choo, K. K. R., & Slaughter, J. (2018). A cyber kill chain based taxonomy of banking Trojans for evolutionary computational intelligence. *Journal of Computational Science*, *27*, 394–409.

Lai, C., Lai, C., Jacobs, N., Hossain-mckenzie, S., Carter, C., Cordeiro, P., Onunkwo, I., & Johnson, J. (2017). *Cyber Security Primer for DER Vendors , Aggregators , and Grid Operators*. *December*.

Li, X., Liu, Y., Ji, H., Zhang, H., & Leung, V. C. M. (2019). Optimizing resources allocation for fog computing-based internet of things networks. *IEEE Access*, *7*, 64907–64922.

Lin, C., & Lin, M. (2019). The determinants of using cloud supply chain adoption. *Industrial Management and Data Systems*, *119*(2), 351–366.

Lu, H.-C., & Huang, Y.-H. (2013). An Optimal Method for Developing Global Supply Chain Management System. *Journal of Optimization*, *2013*, 1–14.

Magklaras, G. B., & Furnell, S. M. (2001). Insider threat prediction tool: Evaluating the probability of IT misuse. *Computers and Security*, *21*(1), 62–73.

Mohammed, A.-M., Idris, B., Saridakis, G., & Benson, V. (2020). Information and communication technologies: a curse or blessing for SMEs? *Emerging Cyber Threats and Cognitive Vulnerabilities*. 163-174.

Molero, X., Silla, F., Santonja, V., & Duato, J. (2002). *On the effect of link failures in fibre channel storage area networks*. 102–111.

Mukherjee, S., & Sengupta, S. (2016). *The Role of Information Technology in Managing Global Supply Chain of 21 st Century- CASE AMWAY*. 46–53.

Nakatani, J., Tahara, K., Nakajima, K., Daigo, I., Kurishima, H., Kudoh, Y., Matsubae, K., Fukushima, Y., Ihara, T., Kikuchi, Y., Nishijima, A., & Moriguchi, Y. (2018). A graph theory-based methodology for vulnerability assessment of supply chains using the life cycle inventory database. *Omega (United Kingdom)*, *75*, 1339–1351.

Nishath, A. S. ., & Selvarani, A. (2015). a Study on E – Channels Service Quality in Private Bank Tiruchirappalli. *International Journal of Management*, *6*(2), 976–6502.

Pamučar, D., Stević, Ž., & Zavadskas, E. K. (2018). Integration of interval rough AHP and interval rough MABAC methods for evaluating university web pages. *Applied Soft Computing Journal*, *67*, 141–163.

Randazzo, M. R., Keeney, M., Kowalski, E., Cappelli, D., & Moore, A. (2005). Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector. *Networked Systems Survivability*, *38*(7), 3–14.

Roy, J., Chatterjee, K., Bandyopadhyay, A., & Kar, S. (2018). Evaluation and selection of medical tourism sites: A rough analytic hierarchy process based multi-attributive border approximation area comparison approach. *Expert Systems*, *35*(1), 1–19.

Subramani, M. (2012). How Do Suppliers in use technology information Supply Chain Relationships ? *Management Information Systems*, *28*(1), 45–73.

Sun, C., Xiang, Y., Jiang, S., & Che, Q. (2015). A supply chain risk evaluation method based on fuzzy topsis. *International Journal of Safety and Security Engineering*, *5*(2), 150–161.

Tsirakidis, P., & Felix, K. (2009). *Identification of success and failure factors of two agile software development teams in an open source organization*. 2–3.

Wu, H. Y., Tzeng, G. H., & Chen, Y. H. (2009). A fuzzy MCDM approach for evaluating banking performance based on Balanced Scorecard. *Expert Systems with Applications*, *36*(6), 10135–10147.

Yu, T. K., Lin, M. L., & Liao, Y. K. (2017). Understanding factors influencing information communication technology adoption behavior: The moderators of information literacy and digital skills. *Computers in Human Behavior*, *71*, 196–208.

Zhu, Z., Scheuermann, L., & Babineaux, B. J. (2004). Information network technology in the banking industry. *Industrial Management and Data Systems*, *104*(5), 409–417.

APPENDIX A

Table A1 Basic equations rough set theory and rough number

Name of the formula	Formula
Lower approximation	$\underline{Apr}(C_i) = U\{Y \in U/R(Y) \leq C_i\}$
Upper approximation	$\overline{Apr}(C_i) = U\{Y \in U/R(Y) \geq C_i\}$
Boundary Region	$Bnd(C_i) = U\{Y \in U/R(Y) \neq C_i\}$ $= \{Y \in U/R(Y) > C_i\} \cup \{Y \in U/R(Y) < C_i\}$
Lower Limit	$\underline{Lim}(C_i) = \frac{1}{N_L}\sum R(Y)\|Y \in \underline{Apr}(C_i)$
Upper Limit	$\overline{Lim}(C_i) = \frac{1}{N_U}\sum R(Y)\|Y \in \overline{Apr}(C_i)$
Rough Number	$RN(C_i) = \left[\overline{Lim}(C_i), \underline{Lim}(C_i)\right]$
Interval of boundary region	$IBR(C_i) = \overline{Lim}(C_i) - \underline{Lim}(C_i)$

Table A2 Questionnaire

Failure factors in IT system of banking industry

Rating Method: Ratings are provided on priority basis. The higher the rating the more important the impact is. Score 1 means almost unimportant, while score 10 indicates absolutely important, other scores are defined similarly. Several criteria can be marked the same rating. Rate the following criteria on a scale of 1-10.
At first the evaluating criteria are rated based upon the opinion of experts.

Criteria	Rating (1-10)
Severity- [importance if Failure turns to severe situation]	
Occurrence- [importance if Failure takes place frequently]	
Detection Difficulty- [importance if Failure is difficult to detect]	
Time- [importance of Time duration for detection & Solution]	
Cost- [importance of Cost incurred to solve the problem]	

Failure modes are then rated on the basis of different criteria based upon the opinion of experts. (rated from 1-10)

Failure Mode	Severity	Occurrence	Detection Difficulty	Time	Cost
Data-Base Hack					
Server failure					
Virus Effect					
Cipher to Plain Text Malfunction					
Character Misspelled					
Wrong Message Transcription					
Peripheral Error					
Broadcast Data Missing (Up/Down) link failure					
Cyber Attack					
Third Party intervention					
Network interruption					