An Integrated Model for Risk Assessment of using RFID Technology in Baggage Management

SAADIA KHUSHNUD

MS L&SCM 2k20

A thesis submitted to NUST Business School for the partial fulfillment of the degree of Master of Science in Logistics & Supply Chain Management

2023

An Integrated Model for Risk Assessment of using RFID Technology in Baggage Management

SAADIA KHUSHNUD

MS L&SCM 2k20

Supervisor: Dr. Waqas Ahmed

A thesis submitted to NUST Business School for the partial fulfillment of the degree of Master of Science in Logistics& Supply Chain Management

2023

THESIS ACCEPTANCE CERTIFICATE

It is certified that the final copy of MS LSCM thesis written by Mr. /Ms Saadia Khushnud Registration No. 00000328205 of MS L&SCM 2K20 has been vetted by undersigned, found complete in all aspects as per NUST Statutes/Regulations/MS Policy, is free of plagiarism, errors, and mistakes and is accepted as fulfilment for award of MS degree. It is further certified that necessary amendments as pointed out by GEC members and foreign/local evaluators of the scholar have also been incorporated in the said thesis.

Signature of Supervisor with stamp: _____

Date: _____

Program Head Signature with stamp: _____

Date: _____

Signature of HoD with stamp: _____

Date: _____

Countersigned by

Signature (Dean/Principal): _____

Date: _____

I hereby state that no portion of the work referred to in this dissertation has been submitted in support of an application for another degree or qualification of this or any other University or other institute of learning.

Student's Name Saadia Khushnud

Signature _____

Date _____

Dedication

I dedicate this thesis to my father whose courage and life has always acted as a guiding light for me.

Acknowledgements

This research thesis has become possible by first the help of Allah Almighty, who bestowed wisdom upon me, gave me strength and direction to finish the research.

I would like to express my deep sense of thanks and gratitude to my thesis supervisor Dr. Waqas Ahmed, whose dedication and support at every stage of research helped me to carve out this thesis into a reality. The utmost encouragement and space provided by Dr. Waqas Ahmed for diving deep into the research interests and exploring it has not only helped me complete this thesis but also has developed a newfound dedication for research.

I also owe a deep sense of gratitude and thankfulness to my GEC members Dr. Faran Ahmed and Dr. Abdul Salam who provided direction and valuable suggestions at every stage of research that helped in strengthening the thesis.

I would also like to express gratitude to my family for trusting and supporting me throughout the thesis tenure. Their understanding and prayers provided me the support that was needed to accomplish the set deadlines for completion of thesis.

I also appreciate the constant support extended by my friends through knowledge-sharing sessions and their prayers. Without them, this thesis would have never become a reality. Lastly, I would like to appreciate myself for not giving up when at time I felt I should.

Table of Contents

List of Figures

List of Tables

Abstract

The digital transformation through Internet of Things taking place in the businesses today is proving to be of paramount significance both in terms of competitive advantage and profitability. Radio frequency identification detection technology is one such internet of things application that is vastly being adopted on a broad scale by industries. It is a surveillance technology being incorporated into various industries for visibility and tracking purposes. The technology uses radio frequency to detect digital-tagged objects, items and humans across a supply chain. One of the many industries using radio frequency identification detection technology effectively in its operations is the aviation industry. Airports, as a result, improve their infrastructure intelligence and progress as smart facilities to promote growth by providing a pleasant travel experience. The volume of logistics flow at airports is huge and for real time monitoring of these flows radio frequency identification detection technology is being used. Although, radio frequency identification detection has its benefits yet there are risks associated with it that can disrupt the operational flow at airports and pose privacy and security issues. Extensive research is available on studying the optimality of using radio frequency identification detection technology in aviation industry; however, the risks analysis is almost nonexistent in literature. This research aims to assess and minimize the risks involved in using the radio frequency identification detection technology in the logistics operations of an airport. One of the major high value logistics flow through an airport is baggage management. Radio frequency identification detection is used here to detect items, objects, and luggage across the supply chain from point of origin to point of delivery. It although has immense benefits, yet research shows that radio frequency identification detection devices can be targeted easily and are thus can be exposed to security and privacy risks. This research proposes a new risk assessment framework which uses a fuzzy based hybrid multicriteria decision making technique for risk prioritization followed by a minimization of risk by selecting optimum mitigation strategies that minimize the risk under risk reduction and cost minimization constraints.

Chapter 1. Introduction

This chapter establishes the foundation of the research by stating the research background and problem description. The research objectives and research questions are also clearly defined in this chapter which guide the overall research study for the thesis. Moreover, an appropriate research methodology to achieve those objectives is stated comprehensively. The chapter also discusses the contributions made by this study to the field of knowledge. Furthermore, a step wise description of the different stages of the research thesis is provided in this chapter which would be further described in extensive details in the coming chapters. Finally, the research flow and structure is described that is used for the study.

1.1Background

With the surge for increased efficiency, businesses across the world are incorporating technologies in to their systems. Technological incorporation not only enables the businesses to achieve operational efficiency but also provides them with a competitive advantage. Of all the industries that are becoming smart by using technologies, aviation industry is at the forefront of this technological innovation (Lykou et al., 2018). This is because the number of air travel passengers is exponentially increasing over the years. According to International Air Transport Association (IATA), the air travelers are projected to hit 8.2 billion by 2037. To ensure smooth flow of operations for such large number of passengers, it is vital for airports to make their processes error-free and fast. A vast number of technologies provide airports with both strategic and operational excellence (SITA Baggage IT Insights Report, 2019). SITA lists them as business intelligence, interactive navigation, biometric ID management, digital tags and artificial intelligence.

Radio Frequency Identification Detection (RFID) or digital tags is one such technology that has gained a lot of attention over the years and is thought to be the next big thing in the information technology (IT) revolution (Kaur, 2017). There are various industries that are employing RFID technology in to their systems such as hospitals, railways, FMCGs, food tracking, logistics, and inventory management etc. (Abugabah et al., 2020). One such industry that is rapidly employing RFID in its operations to digitize its logistics management is the aviation industry (Tikhonov at el, 2019). The aviation industry is the worldwide transportation network that transports products and passengers by air. Airports are a part of it. Airports around the world carry millions of passengers

and cargo each year across the world. According to IATA, over 55 million bags and millions of tons of cargo is handled each year at airports around the world. Hence, airports being region of high flow of logistics and personal require real time monitoring of these value flows using RFID as it enables identification at a long distance, storing more information and has a low price (T Datta, 2008).

RFID is an automated identification technology that uses radio waves to convey the identity of items and persons in the form of a unique serial number. The tag is made up of a microprocessor -that saves data- as well as an antenna. To identify the object item, it uses a unique serial number which has stored information of the user depending upon the purpose it is being used for. The reader is made up of an RF (radio frequency) module, a control unit, and a coupling element that allows it to interrogate tags through radio communication. It also provides a supplementary interface for communicating with backend systems and transmitting the data contained in tags (Zhang, 2008). Despite the benefits of integrating RFID in business operations, naive deployment of such technology can generate risks that must be evaluated and handled during the design phase and throughout the application lifecycle (Fritsch, L, 2009).

In the airports, the two major activities of logistics flow are baggage handling and cargo management. Because the cargo is frequently high-value and/or perishable, air freight clients expect fast deliveries. Any delays at the airport may result in unmet consumer demand, expensive inventory-in-transit costs, and deterioration of perishable commodity quality. An airport delay or error may result in unfulfilled consumer demand and storage or degradation charges. Similar is for baggage as agile operations at airport require quick baggage sortation and passenger-baggage matching. A baggage has to go through eleven different stages in order to reach its owner. Through its journey, several potential risks are linked to it which can eventually lead to baggage mishandling (Ahmed T et al., 2015). The focus of this research is on one logistics flow operation i.e. baggage management.

Airport baggage management is a very momentous part of the air travel industry (Ahmed & Pederson, 2015). An efficient baggage handling system ensures customer satisfaction and increases the overall revenue. However, due to several reasons, every year there have been increased instances of lost, mishandled or delayed baggage which not only costs the airport extra money but also creates frustration and inconvenience for the passengers (Ahmed & Pederson,

2015). The major baggage mishandling are: left behind at the origin airport, missed connecting flights, bag loss, wrong bag destination etc. According to the SITA Baggage Report 2014, 21.8 million bags were among those affected by baggage mismanagement in 2013-2014, resulting in a loss of $2.09 billion USD to the airline sector (Tanvir, 2015). Similarly, according to a report by SITA, the global mishandled baggage rate has increased by 24% to 4.35 bags per thousand passengers in 2021 (SITA Baggage IT Insights 2022). To remedy these issues, airports are now using RFID based baggage handling systems (Rajapaksha, 2020).

Over the years many airports across the world have implemented RFID based baggage management systems while many are still on the planning stages as shown in Figure 1.1 (Atkins el al., 2011). The RFID is primarily used in baggage management in order to track the value flows throughout the supply chain from point of origin to final stop (Wyld, 2015). The use of RFID not only enhances the automation of baggage handling but it also significantly decreases the cases of mishandled bags (Atkins el al., 2011). The acute link in customer's minds amid seeing the baggage on baggage carousel upon arrival and the opinion of passengers of an airport's service offering is empirically proven (Wyld et al., 2005).In an RFID baggage management, the rfid tag is attached to a bag which then passing through a number of checkpoints where RFID readers are deployed. The reader reads the tag information stored in tag and communicates over a wireless link to a network database. In the backend, the data is stored and evaluated for further processing. The deployment of RFID in baggage management system has been a transforming initiative for many airports as on-time baggage delivery qualifies an airport for core competency.

By using RFID, airports are enhancing their infrastructure intelligence. RFID system has many security flaws that can be exploited to damage and disrupt the operations at airports (Lykou et al., 2018). By using RFID to track the flow at multiple points in movement can have risks associated with it. These risks and attacks can be physical or cyber. According to the literature, the deployment of RFID technology is anticipated to pose a number of security and privacy problems (Rouchdi, Y., El Yassini, 2018). These risks are associated with the different layers of RFID where several kinds of cyber-attacks are possible. A cyber-attack is any attempt to gain unauthorized access to a computer, computing system or computer network with the intent to cause damage (K Huang, 2018). The risks of cyber-attacks is always prevalent in systems where internet of things is used. According to a research conducted by the European Aviation Security Agency (EASA),

1,000 airport cyber-attacks occur on a monthly basis. The Cathay Pacific hack was one of the largest in 2018, resulting in a data breach of more than 9.4 million records. Cyber risks will continue to expand in conjunction with technology advancements, while the link between aviation safety, security, and performance will become increasingly integrated (Georgia et al., 2018).

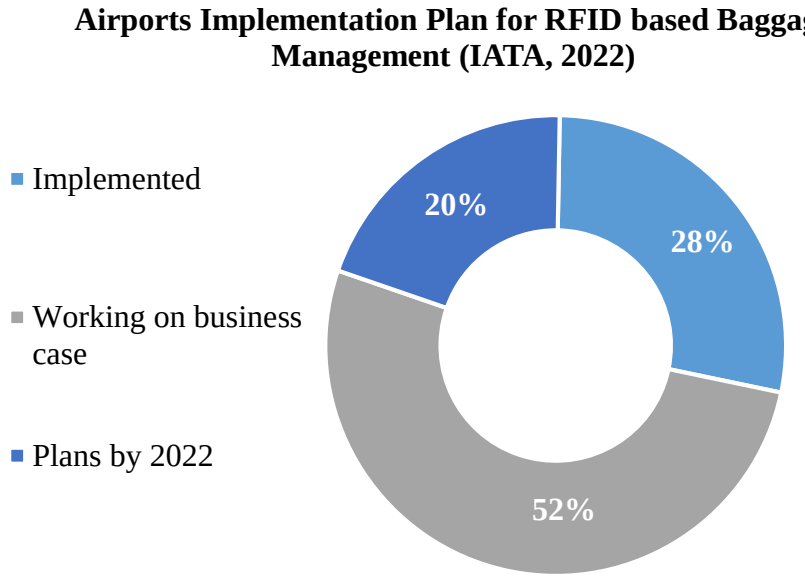

Figure 1.1 Airports adopting RFID based baggage management systems (IATA)

1.2 Problem Description

Due to overwhelming competition among the businesses for excellence, businesses are adopting various technologies to make their processes efficient and smart. For the purpose, various industries are using RFID system in their operations. In the same way, the aviation industry is at forefront in adopting digital tags (or RFID tags) for real time monitoring of its one of the most time valued and time sensitive logistics flow i.e. baggage management. But with the adoption of RFID technology, industries are adding complexities to their systems. These complexities open many vectors of attacks. With the incorporation of industrial IoT (Internet of Things) in airport services there are many risks that can take place. Research is available on the potential risks of RFID that may occur in time, but these risks have not been studied with reference to a particular

industry-in this case the airport industry- neither any comprehensive risk model or risk assessment framework is available. However, with the large-scale adoption of RFID demands a large investment with a substantial risk which thus requires a vigilant planning and risk assessment (Kulwiec, 2005).

An RFID system has many constraints related to its system – such as capacity, memory and communication- as a result of which there are many security and privacy risks that are resulted (Kumar et al., 2021). There are threats with its usage which mostly fall into three categories of availability, integrity and confidentiality (Kumar et al., 2021). In each of these categories there are a set of attacks on RFID system that can act as risks. For this reason, RFID is termed as one of the most invasive surveillance technology (Mishra, 2012). RFID-based systems can provide us with a view to human activity that is unprecedented in detail and breadth (Gillenson et al., 2019). Still the RFID technology is not completely secure and suffers from multiple threats. Now, all these issues and shortcomings related to an RFID system make it possible for various attacks to take place. Such an RFID based baggage management system at airports is also susceptible to such attacks which can hinder operational flow and customer service.

Airport business operations and models have developed substantially in recent decades to accommodate the global aviation industry's tremendous development. Administrative shifts in the modern generation of air travel led in massive gains in traffic, variation, and choice for passengers traveling. As airlines optimize their operational models to match expansion with efficiency, airports advance in tandem to build huge networks of hubs and sophisticated technologies that, when combined, form an efficient air transportation ecosystem (Lykou et al., 2015). By shifting to from conventional baggage management to an RFID based baggage management system, along with the benefits there are risks aspects involved which should be assessed to save airport from disruption in operations and ensuring customer service.

Hence, this research aims to address this gap and provide a theoretical, methodological and practical contribution to the literature. This research proposes a novel integrated risk assessment model for effective risk management and mitigation. The model combines a fuzzy based hybrid multi-criteria decision making method and optimization modelling for recognizing the risk prioritization, and minimizing the risks respectively. This framework is a qualitative-quantitative

risk assessment framework that effectively recognizes and mitigates risks. The pictorial representation of the problem description for this research thesis is given in Figure 1.2.

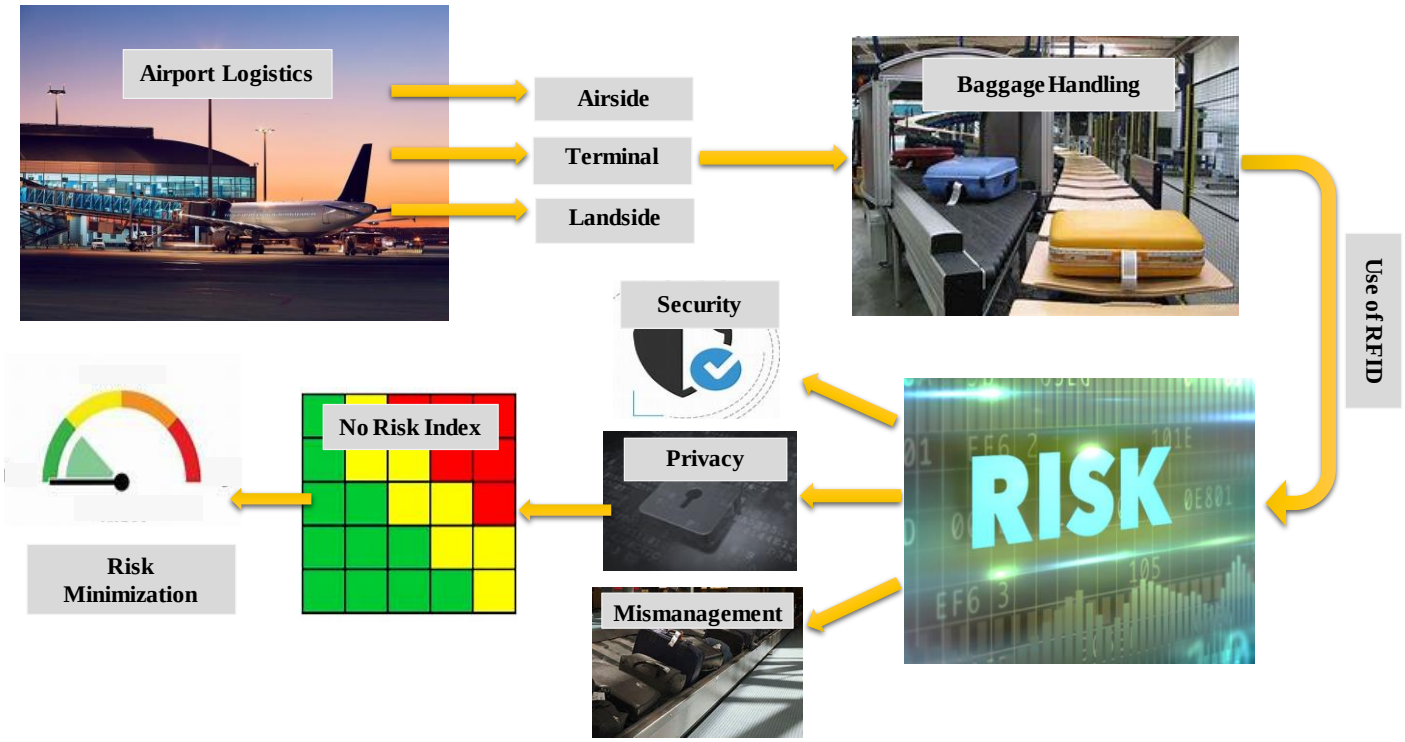

Figure 1.2 Problem description for using RFID in airport logistics operation of baggage management

The research problem shown in Figure 1.2 shows that in an airport there are three major areas where logistics activities take place. Those areas are airside, terminal and landside. So the logistics activities there are called as airside logistics, terminal logistics and landside logistics respectively. In the terminal area, baggage management is the most time sensitive and value adding activity. Timely and accurate delivery of baggage to passengers adds to the customer service quality of the airport. However, there have been many repeated incidents of lost, mishandled and delayed bags. In order to control these issues and improve the performance, airports are using RFID based baggage management systems. In an RFID baggage management, an RFID tag is attached to the baggage which stores information. That bag over the logistics flow is read by the RFID readers. By using RFID opens it up to several attacks which can compromise on security,

privacy and management. However, there is no such comprehensive risk index available in literature that can be used to identify risks ranks and minimize them.

1.3 Research Questions

This research is carried out to answer a few questions related to RFID usage in airport logistics operation of baggage management. The research will answer the following main questions as listed below:

1. What are the various risks associated with the use of RFID technology in airport logistics operations, particularly in baggage handling?
2. Which of the risks are high impact risks and low impact risks?
3. What are the various mitigation measures that can be used to eliminate risk?
4. How can the risks associated with RFID use in airport logistics be minimized effectively?

1.4 Research Goals

The major research goal of this research study is to develop a comprehensive risk assessment framework that can be used to carry out detailed risk assessment. Moreover, this study targets to study the risks involved in using an RFID based baggage management systems at smart airports using the proposed risk assessment framework. The risks of using RFID in airports basically emerges from the unsafe aspects of RFID which emerge owing to a number of factors. As RFID infrastructure is consisting of several layers, for each layer there are a number of vulnerabilities which make it susceptible to security and privacy risks. Hence, this study would identify and study those risks of RFID that can cause disruption and vulnerabilities in smooth operations of airport baggage management. This study is not limited to risk identification, but it also explores the way to effectively minimize and mitigate the identified set of risks that also satisfy a number of organizational constraints.

The risk is minimized by maximizing the risk reduction that is performed by implementing a mitigation strategy which targets more than one risk at a single time. For this, it includes the development of a risk mitigation matrix that is used to calculate the risk reduced after using a particular mitigation strategy. Afterwards, it optimizes the risk by maximizing the risk reduction obtained from the risk mitigation matrix. Hence, the overall goal of this research study is to effectively identify and mitigate the risks which emerge from using RFID tag based baggage

management system at smart airports. This would provide the managers and decision makers with a cost-risk analysis of using RFID based baggage management system and will provide them with a comprehensive index to help identify, target and focus on the high-risk threats.

1.5 Research Objectives

The objective of this research is to study the below mentioned research problems and gaps as found in the literature.

- To develop a comprehensive and integrated risk assessment framework to study and analyze the risks.
- To identify the risks of using RFID technology in airport logistics operation of baggage management that can act as disruption and security concerns.
- To obtain a comprehensive risk index based on priority level associated with the risks by assessing them against certain parameters.
- To select the best grouping of mitigation strategies to control and manage the red-zone risks.
- To minimize and mitigate the risks of using RFID in baggage management by effectively maximizing the risk reduction that is done after using best grouping of mitigation strategies.

1.6 Research Methodology

The objectives and goals of this research are achieved by using a risk assessment framework that is proposed in this research. On the basis of this framework, the analysis is built. The framework is based on four steps of risk assessment. In the step, risks are identifies by reviewing literature available of risks associated with an RFID system. Next, those risks are studies in context of RFID based baggage management system. After this, the ranks and scores of risks are identified by using a suitable multi-criteria decision making technique. Once, the scores of risks are obtained, next a clustering of risks is performed on the basis of risk score. The clustering divides risks into three zones- red, green and yellow- on basis of the severity and assessment of risks against different parameters. Afterwards, these red-zone risks are then used in risk mitigation matrix. In the risk mitigation stage, the appropriate risk mitigation strategies are identified and a

taxonomy is created. Using the risks and mitigation strategies from the prior stages, these risks are then minimized and mitigated by developing a mathematical model.

The mathematical model consists of two single objective functions and one single multi-objective function. First, using the single objective functions under certain constraints the results for risk reduction and cost minimization functions are obtained. Next, a single multi-objective function is formulated. The multi-objective function has only one variable which is the selection of mitigation strategy. The selection variable is binary in nature which is one if a mitigation strategy is selected and zero if the mitigation strategy is not selected. The mathematical models are solved in computer software using weighted goal programming technique. The solution of the weighted goal programming for risk minimization is analyzed by carrying out a sensitivity or numerical analysis. The numerical analysis is conducted by considering four cases in which the risk reduction goal and cost goal values are changed. Under four cases, the results are examined and results are obtained which are then further analyzed. The research methodology used in this research is shown in Figure 1.3.

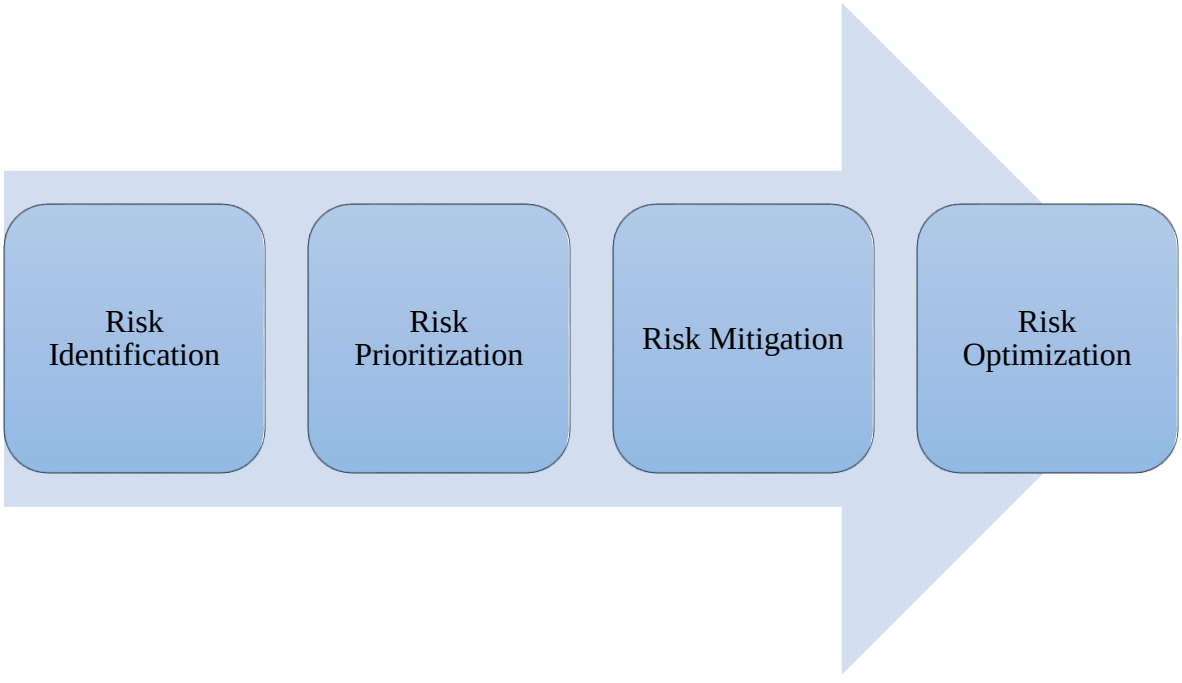

Figure 1.3 Flow for methodological implementation for research study

1.7 Research Contribution

RFID is an industrial internet of things technology that is used to detect items, objects, luggage and cargo across the supply chain from point of origin to point of delivery. RFID, although has immense benefits, yet research shows that RFID devices can be targeted easily and are thus exposed to security and privacy risks (Kumar et al., 2021). This research aims to target the risks involved in using an RFID based baggage management at airports. So, the contribution of this research study is mainly two-folds: methodological and practical. Initially, the research studies the RFID system flaws and vulnerabilities in the baggage system. Then, methodologically, this research proposes an integrated fuzzy based risk assessment and mitigation framework to study the risks associated with RFID use in airport logistics operations-primarily baggage handling. The risk assessment framework can be used to conduct the risk analysis in any supply chain or logistics flow. The proposed model uses a four stage risk assessment framework where it uses a hybrid multi-criteria decision making technique- Fuzzy Analytical Hierarchy Process (FAHP) – Fuzzy Technique for Order Preference by Similarity to Ideal Solution (FTOPSIS) for risk prioritization. Then it performs optimization modelling for minimization of risk under budgetary and risk reduction constraints. The research proposes a Risk Mitigation Matrix (RMM) which combined with optimization is used to select the best combination of mitigation strategies under goal programming approach.

Practically, the contribution of this research is that it provides a cost-risk analysis of the implementation of RFID based baggage management system. It provides the airports managers with a risk assessment where there are the most important risks identified. For those important risks, risk mitigation and minimization is carried out. In short, this study provides a complete risk assessment for the RFID tagged baggage management system at airports. Moreover, this thesis lays down the important aspects of the risk analysis which are often missed during large scale investment at the airport. With the implementation of RFID technology at large scale in airports, a variety of security and privacy risks must to be addressed equally by organizations and individuals ((Rouchdi et al., 2018). However, there are no such comprehensive threat models existing for the RFID systems which make it difficult for system operators at airports to manage risks when there is no risk assessment available. Hence, this research makes a practical

contribution by providing a comprehensive risk assessment framework for RFID based baggage management at the smart airports.

1.8 Research Structure

This research thesis is divided into seven chapters which includes introduction and conclusion sections as well. The Chapter 1 lists the introduction of the research and background of the research problem. It lays down the motivation and goal of research that come after describing the research problem and gap. The research problem is described both theoretically and pictorially for better understanding. Next, the Chapter 1 lists the research questions and research objectives which are the starting point of this thesis. The research objective is mainly to perform risk assessment of using RFID in baggage management systems in airport. Next in line is the research methodology which is briefly described to obtain a crux of the framework used in the research. Lastly, it provides a holistic overview of the contribution this research makes to the literature followed by the research structure used in this thesis.

Chapter 2 provides an orderly stepwise literature review of the study in focus in this thesis. The literature review is performed in order to have a foundation and concrete facts from previous researches that act as a stepping stone for the research in focus. The chapter of literature review is systematically divided into various sections. This division helps to effectively study different areas under focus from different perspectives. The literature review covers RFID as a whole system, applications of RFID in various industries, use of RFID in airport, use of RFID in baggage management, challenges with use of RFID etc. Each section in the literature review deeply reviews the important articles from literature on that particular area of study in focus. The detailed review sets as a stepping stone for the research in that area that has to be done by this thesis. Hence, this chapter describes each and every section in very detail.

Chapter 3 of the research thesis provides the methodology that is followed for the research purpose. It proposes and lays down an integrated risk assessment model that is based on both qualitative and quantitative analysis. The risk assessment framework is based on four stages. In the first stage the risks of RFID in baggage management are identified. After identification, the risks are prioritized in the next stage by assessing them against several parameters. Through this step, clusters of risks are obtained and different zones of risks are identified based on the severity.

In the proceeding step, the mitigation strategies for the red zone risks are identified and a risk mitigation taxonomy is developed by considering positive correlation. Next, a risk mitigation matrix is developed. Lastly, using the RMM and a multi-objective mathematical model developed, the risk is minimized. The risk minimization is carried out by optimizing the risk reduction as obtained from using mitigation strategies under some defined set of constraints. The major constraints are two: risk reduction and cost minimization constraints.

Chapter 4 of this dissertation provides the results obtained from the implementation of research methodology described in Chapter 3. This chapter provides step by step results for the four stages of risk assessment framework. It first gives results for the risk identification stage. Followed by the scores of risks obtained by using a hybrid multi-criteria decision making technique called as the Fuzzy Analytical Hierarchy Process (FAHP) - Fuzzy Technique for Order Preference by Similarity to Ideal Solution (FTOPSIS). This MCDM technique identifies the top risks of using RFID in baggage management. Followed by this, is the mitigation stage. Here it provides the suitable mitigation strategies that can mitigate risks effectively. Following the algorithm for Risk Mitigation Matrix (RMM) as described in Chapter 3 is used here to fill in the RMM. The RMM shows the risk level before implementing mitigation strategies, risk after implementing mitigation strategies and the risk reduction by subtracting later from former value. Lastly, it shows the best combination of strategies that can be selected by an airport. The results are also explained through graphical representation for better understanding.

Chapter 5 of this thesis focuses on the discussion and analysis portion of the research. The chapter discusses the results systematically. First, it presents a scenario analysis of the top risks identified from the risk assessment. In the scenario analysis, the chapter discusses the top ranked risks from baggage management context. It discusses the cascading effects and impact evaluation of the RFID risks that pose major threat to airport services. It also studies the relevant attacks that have already in past disrupted and compromised the airport operations. Furthermore, Chapter 5 discusses in detail the sensitivity and numerical analysis that has been performed for the risk minimization / risk reduction optimization part in Chapter 4. The graphs explain how changing the different goals from the multi objective optimization function can affect the selection of mitigation strategies and corresponding risk reduction. Finally, it discusses the mitigation strategies that can be selected under given budget and risk reduction goal.

Chapter 6 of this thesis presents the concluding remarks from the above conducted analysis in previous chapters. This chapter discusses the conclusion, managerial implications and future recommendations that can be adopted to extend the research. The managerial insights are provided to help the airports managers and policy-makers to evaluate not only the benefit but risk analysis to better understand the risks that come with the implementation of the RFID based baggage management system at airport.

Chapter 2. Literature Review

This chapter of the research presents a thorough description of the literature covering many areas under discussion in this study. The focus of this chapter is on the review of articles on baggage management operation at airport, the Radio Frequency Identification Technology (RFID), the risks related to RFID, applications of RFID, and risks of using it in the digital tagged baggage management. The literature review related to each section is thoroughly examined, and a brief synopsis of the research contribution is highlighted in this chapter. The literature review of each section is comprehensively evaluated which is then linked to the study under discussion.

2.1 Baggage Management at Airport

Radio Frequency Identification Detection (RFID) is a rapidly growing technology that is used in practically every industry. It is regarded as a crucial technology for increasing operational efficiency and enhancing supply chain management. RFID has been studied from a variety of aspects as a result of its fast adoption. Amini et al. (2007) sought to create a simulation model for investigating the collateral applications and exposition of RFID technology. Delen et al. (2007) investigated the use of RFID for improved supply chain management through information visibility. Keskilammi et al. (2003) proposed passive RFID systems for automated production and logistics control, as well as the impact of antenna settings on operating distance. Prater and Frazier (2005) investigated the effects of RFID on e-supply chains in the supermarket retailing industry. Saygin (2007) investigated adaptive inventory management through the use of RFID data. Whitaker et al. (2007) investigated RFID implementation and expected return rates. Zhou et al. (2007) investigated a remote monitoring system based on RFID for business internal production management. Xiao et al. (2007) envisioned different RFID technologies, numerous RFID applications, and current research concerns concerning RFID deployment, adoption, and usage.

While the Internet of Things (IoT) delivers many worthwhile benefits, it also exposes us to a wide range of security vulnerabilities in our daily lives (Hwang, Y. H, 2015). In the research available, there exists an asymmetry between benefits and risks of using RFID in various industries. Mishra 2012 studied the use of RFID in aviation industry and found that the technology is to both having enormous benefits for operations and also to be one of the most invasive surveillienace technology (Mishra, 2012). In airports, RFIDs are primarily used in passenger

baggage sorting, containers/ ULDs, passenger-baggage matching and cargo verification (Cerino, A., Walsh Research and application of RFID to enhance aviation security). Mishra 2021 also emphasized on the issues and risks associated with RFID use in aviation industry stating that security/privacy, reliability, system performance, automatic failover and contactless remote-controlled cards are some issues that are crucial. David 2013, critiqued the statement of a commercial director who stated that 'bags are being very well tracked right now' by saying that havoc is only created when one's own bag is lost.

Baggage mishandling is a significant problem owing to the nature of the baggage delivery being an 'all or nothing' event (Y.Rouchdi et al., 2013). In 2004, Delta Airlines conducted pilot tests of using RFID based baggage tracking and concluded following issues with the system: metal housing in ULDs impeded the radio signals raising concerns on the ability of tags to function under harsher environments; static electricity created along conveyor systems might harm tag antennas. (Collins, 2004). Zhang 2008 studied the optimality of using RFID in airport logistics flows. He emphasized that using a RFID based logistics management system in airports can reduce the baggage errors including mislaid baggage, lost bags and damaged bags by 10 percent. Contrary to it, Yassir Rouchdi studied that with the use of RFID in airport luggage tracking, a variety of security and privacy risks arise that need to be addressed. RFID tags are regarded as 'dumb' gadgets since they can only listen and reply. As a result, unprotected tags are open to eavesdropping, traffic analysis, spoofing, and denial of service attacks (Y.Rouchdi et al., 2013).

Airport is a region of high flow of logistics and personal (Tirthankar Datta, 2008). The volume of logistics generated every day at airport terminal adds to the complicacy of logistics management at airports. The aviation sector suffers substantial losses as a result of luggage mishandling. According to the Baggage Report 2014, 21.8 million bags were affected by baggage mishandling, resulting in a loss of $2.09 billion USD to the airline sector (Tanvir, 2015). Karygiannis 2006, in IEEE paper on RFID security presented a framework for organizing and analyzing the RFID issues. The paper did not compute the likelihood or possible effect of specific risks, nor did it examine the feasibility of building attacks to leverage these risks, nor did it give an evaluation of RFID system hazards. RFID technologies add complexity to an organization's IT infrastructure, which can result in more threat and attack vectors. Because some of the RFID system devices are not commonplace IT assets, the risks they entail may not be successfully

managed when they are first introduced (Karygiannis 2006). As a result, RFID installation must be preceded by thorough investigation (Gadysz, 2014). Kumar, A., Jain, A., and Dua, M. (2021) designed RFID security strategies and created a generic taxonomy of RFID threats. These risks have been hardly studied in context of the airport logistics operation of baggage management neither any risk assessment has been carried out. Moreover, in order to perform this risk assessment a novel risk assessment is proposed and would be used to perform risk assessment.

2.2 Radio Frequency Identification Detection (RFID)

Growing number of technologies are being integrated into business processes to gain competitive advantage. Since a last few years, RFID has emerged as one the most promising industrial technology (Mishra, 2012). There is extensive literature available on the benefits of the technology. However, as the RFID tagging has grown more common, the ethical concerns it presents have received little attention. Therefore, prior to implementation of RFID on a broad scale it is essential to keep in view both positive and negative aspects of the technology.

2.2.1 Description of RFID

RFID has been around for many years. However, it is only recently that the combination of reduced costs and boosted capabilities has prompted organizations to take a closer look at what RFID offers to them (R. Weinstein., 2005). RFID technology can be a tool to track time-stamped location of tagged entities through the processes they go; it can simply be considered as a data-collection platform where the user is "watching" as entities flow, without interfering with the flow (Can et al., 2010). RFID is analogous to barcoding in that data from a tag or label is sent and collected by a device and stored in a database. RFID, on the other hand, offers significant benefits over other technologies. The most noteworthy example is that the RFID tag data may be read from a distance without a line of sight, whereas an optical scanner must be used to align barcodes (Urso et al., 2020). Due to various benefits, the RFID technology is being increasingly used in many industries. However, there are many challenges linked to its adoption which must be investigated (Kumar et al., 2020).

2.2.2 Working of an RFID system

Radio Frequency Identification Detection (RFID) uses radio waves to automatically detect people or objects provided that an RFID tag has been placed upon them (Gaukler, 2011). RFID

systems work on the basic principle of labelling goods with tags. Most RFID tags contain some kind of identifying number, such as a customer number or a code. A reader collects and acts on data about the ID number from a directory. RFID readers situated in various locations. This data can track the movement of the detected object and make it accessible to any reader (R. Weinstein., 2005). The Figure 2.1 shows a general way an RFID system operates. It shows that in an RFID system two-way communication takes place where the tag transmits the data which is read by the reader which then sends it to the host system. The host then sends it to reader and then to tag (Wyld et al., 2005).

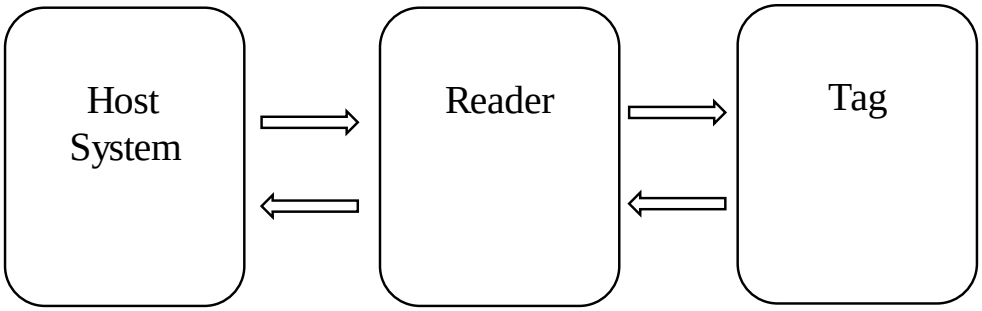

Figure 2.1 Working of an RFID system

2.2.3 Construction of an RFID System

An RFID system is typically consisting of three components: a tag, a reader and a host system or database (Achraf Haibi, 2011). These components interact with one another to operate. The communication among these components take place in radio frequency domain. The three components and their sub-parts are individually explained below:

a. RFID Tag

An RFID tag is a data carrying component of the RFID system that is affixed to things that must be uniquely recognized (Achraf Haibi, 2011). An RFID system's fundamental unit is the tag, and every tag has its own unique identification number system that enables it to be identified individually. These unique identification codes are stored in the internal memory of the tags and cannot be modified (read-only). Tags, on the other hand, can incorporate read-only or rewriteable extra memory. RFID readers generate magnetic fields via antennas in order to receive responses

from tags (Garfinkel & Rosenberg, 2005). The microchip is a small silicon chip with embedded circuit (Garfinkel & Rosenberg, 2005). Depending on the characteristics and its function inside an RFID system, this microchip may have read-only or writeable features. These properties are determined by the microchip circuitry that is formed and configured during tag fabrication. (Meiller & Bureau, 2009). Various forms of RFID tags exist and can be used depending on usage requirement.

b. RFID Reader

The RFID readers are actually devices that are powered externally that create and receive radio signals in RFID systems (GAO, 2005). A single reader can operate on many frequencies, which are determined by the manufacturer (Frank et al., 2006). The RFID reader is a device that sends and receives information through radio waves via the antennas linked to it (Achraf Haibi, 2011). Inside an RFID reader are components such as transmitting circuit, receiving circuit, frequency synthesize, circulator etc. (Ying, 2008). The reader is the heart of the RFID system, communicating with tags and computer programs. It provides tag information to a computer software after scanning each tag's unique ID (Sandip, 2005). The reader may connect to the computer through a connected or wireless connection. There are mainly two kinds of RFID readers: handheld and fixed readers. These readers can be used depending on the requirements of the organization implementing it. The readers are generally placed in locations along the supply chains where they can perform their task of efficient transponder interrogation (Preradovic, 2006).

c. Reader Protocol

RFID system deployments need RFID reader configuration, monitoring, and information management (C. Floerkemeier et al., 2008). RFID readers' capabilities include command, sensor, observation, alert, transport, host, and trigger (Glover, 2006). EPCglobal is the most frequently used and respected protocol. EPCglobal provides three levels of communication: information, transport, and reader (Zeisel & Sabella, 2006). Readers use two types of communication: synchronous and asynchronous (Shepard, 2005). In synchronous reader-host communication, the server requests an update from the reader (Garfinkel & Rosenberg, 2005). As an outcome, the reader sends the list of modifications to the host. In the case of asynchronous communication, the

reader tells the host of its observation. These reader protocols can be selected on the basis of the criteria of business implementing RFID system.

d. Antennas

RFID antenna is the middle-ware technology or component, it work between reader and tag and provide energy to tags in some cases (passive tags). It performs tags data collection. Its shape can be altered depend on the application and feasibility of use but shapes varies the range of antenna (Intermer, 2009). Antennas used in RFID differ on basis of their properties such as polarities and direction of signals. Antennas are used both for transmitting and receiving signals. Some examples of antennas include: Stick antennas, gate antennas, patch antennas, circular polarized, di-pole or multi-pole antennas, linear polarized, beam-forming or phased-array element antennas, Omni directional antennas and adaptive antennas (Zeisel et al., 2006). The major points to consider in choosing an antenna are: the type of antenna; its impedance; RF performance when applied to the object; and RF performance (P.R. Foster et al, 1999). There are two antennas in an RFID system:

i. Tag Antenna

A tag antenna is the one that accumulates energy and passages it to chip installed in tag which turns it on. The tag antenna's area is directly proportional to the ability of tag to collect data and read range of tag. The tag antenna must not only broadcast the wave containing the information contained in the tag, but it must also receive the wave from the reader in order to provide energy for tag operation (C. Floerkemeier et al., 2008). Tag antennas should be compact in size, inexpensive in cost, and simple to manufacture for mass manufacturing. The tag antenna should, in most situations, offer omnidirectional dispersion or hemispherical coverage (Achraf Haibi, 2011). The Figure 2.2 shows the circuitry used inside an RFID tag. This chip circuit is made up of silicon which is a powerful semiconductor.

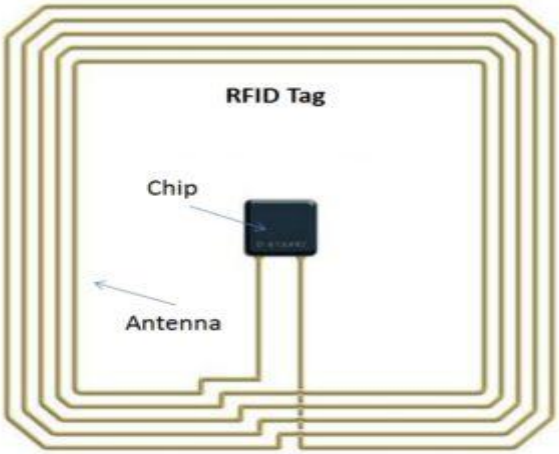

Figure 2.2 RFID tag circuitry used in an RFID based system

ii. Reader Antenna

Fixed readers are favored over portable readers because handheld readers require human operators and are thus vulnerable to human mistake (Parthiban, 2019). Electrical current is turned into electromagnetic waves by reader antennas, which are then projected into space and picked up by a tag antenna before being converted back to electrical current. In UHF RFID systems, reader antennas are crucial, as opposed to LF and HF RFID, which employ an inductor coil for transmission and receiving. Near-zone RF fields are generated by inductor coils. UHF RFID reader antennas could function as far-field or near-field emitters. Polarization, bandwidth, gain, voltage standing wave ratio (VSWR), beam width, and front-to-back ratio are important antenna properties that have a direct influence on tag detection performance (Parthiban, 2019). The RFID reader antenna uses different modulation schemes such as double sideband amplitude-shift keying (DSB-ASK), single-sideband amplitude-shift keying (SSB-ASK) or phase-reversal amplitude-shift keying (PR-ASK) modulation types (Parthiban, 2019).

e. Host

A middleware or host is a crucial component of an RFID system. RFID middleware is critical in integrating business management modules with data from RFID tags in large-scale or complicated RFID solutions (Oufaska et al., 2021). The RFID tag data gathered by RFID readers

is subsequently sent to a software system or middleware for data processing (Achraf Haibi, 2011). RFID data flows are frequently continuous, large volume, and redundant. To provide favorable conditions for RFID data processing and transmission, the system must have a middleware layer that controls both readers and a huge number of RFID events in real time (Rouchdi et al., 2018). Because the middleware serves as an interface between the readers and the information system, it is critical in handling the combined data flows from RFID readers. An RFID middleware's primary functions are as follows: it conceals the complete hardware component from backend programs; it applies filtering to redundant, nonsensical, or worthless information; it is in charge of raw data processing before delivering it to the appropriate applications and it provides the option of managing the readers (Achraf Haibi, 2011).

2.2.4 Frequency Ranges

RFID tags' capabilities and operating feasibility vary depending on their frequency and range. Tag pricing and use vary in response to a tag's frequency and range (Achraf Haibi, 2011). In Figure 2.3, different frequency ranges for different RFID systems have been given.

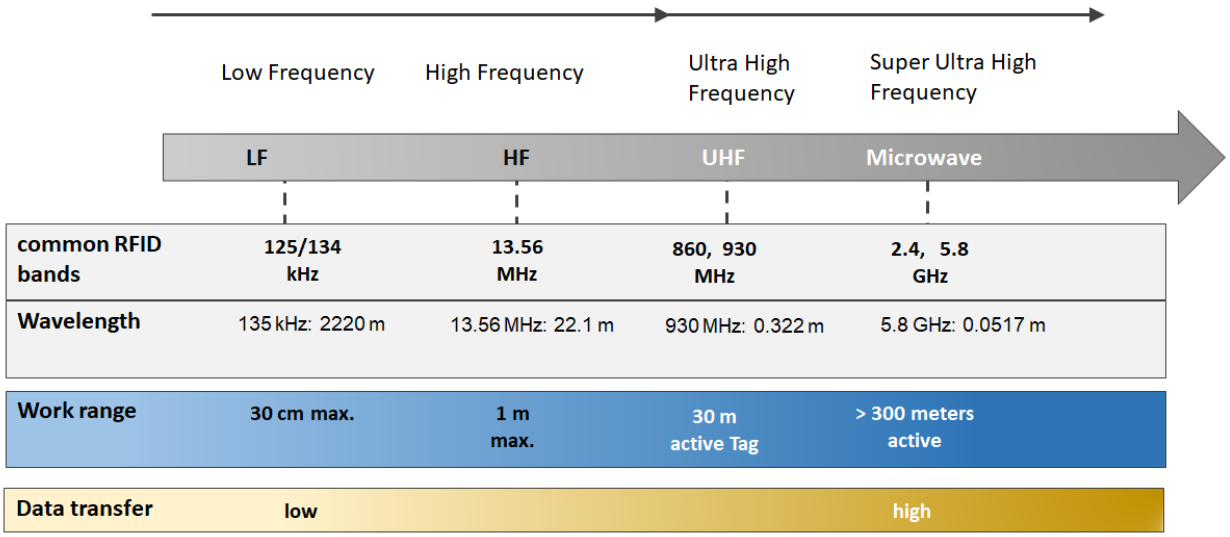

Figure 2.3 Frequencies and ranges of RFID (Source: Zeisel, 2006)

It is frequency of the RFID that determines the performance, range and interference of tag operation. Low frequency (LF) cannot be effectively used for metal or wet surfaces. If used, the operational efficiency will decrease. It work mostly in 125 KHz range and is expensive. Whereas, the high frequency works up to one meter and works at 13.56 MHz frequency. High frequency

(HF) RFID is also less expensive to implement (CAENRFID, 2008). However, Ultra High Frequency (UHF) has a much better range and read rate. It works between a ranges of 860-930 MHz (Srivastava, 2005). Lastly, the microwave works on 2.45 GHz and has the best reader rate. UHF has a one meter of tag read range (Kamran Ahsan, 2010). The UHF RFID is advantageous over the LF and HF RFID systems because they have a greater tag detection range, faster data transfer rate, multiple tag detection (around 200 tags or more at a time) and lower tag costs (Parthiban, 2019).

2.3 Application of RFID Technology

RFID is not only a viable, unique, and cost-effective option for everyday object identification; it is also regarded as an important instrument for providing traceable accessibility. (Zhang et al., 2008). Due to this reason, RFID systems have various applications, some of which are toll road applications, livestock monitoring, patrolling log applications, security and control, baggage monitoring, health care, construction, hospitality, traffic-control systems, warehousing, fleet management, supply chain management and retailing etc. (Nambiar, 2009). In recent years, radio frequency identification technology has risen from the shadows to help speed the processing of manufactured objects and commodities. (Kaur et al., 2011). RFID-based tracking features have already been integrated into the services of several logistics companies and postal agencies. Likewise, several retailers, including Best Buy, Metro, Target, Tesco, and Wal-Mart, are pioneering RFID use. These merchants are now focusing on enhancing efficiency of the supply chain and guaranteeing that goods is available when customers desire to purchase it (Kaur et al., 2011).

One of the major application area of these digital tags is in the baggage management systems at the airport. Using RFID tags for baggage handling has been solving problems of lost, missing and mishandled baggage as it provides real-time tracking and visibility of the luggage as it moves across the world. In the coming years, the adoption of this IoT technology in the aviation sector is going to boost. The market size by technology for RFID will increase over the years while there will be a decrease observed for barcode based baggage tracking at airports (Inkwood research, 2018). This is shown in Figure 2.4.

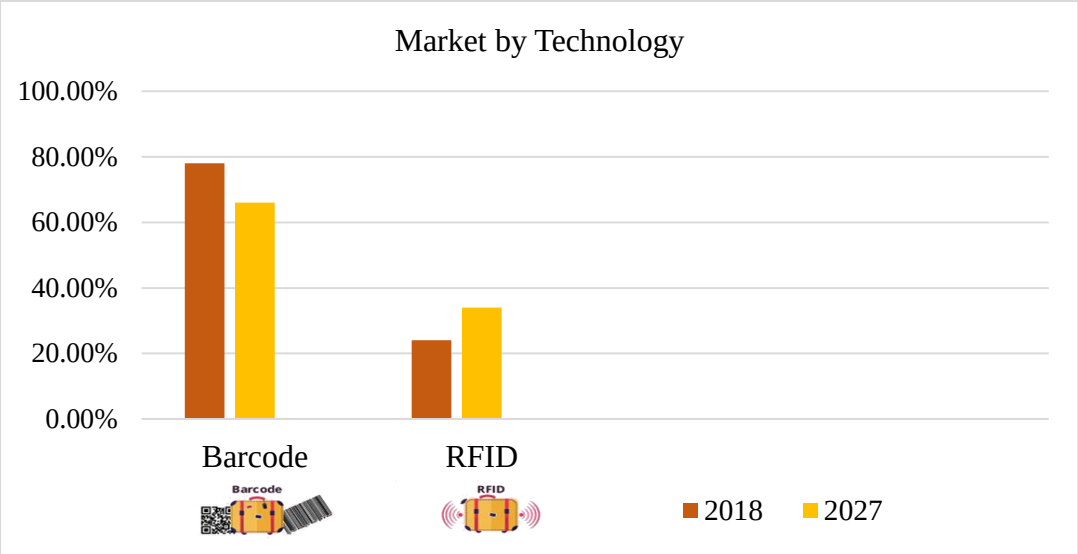

Figure 2.4 Market by technology of barcode and RFID in baggage management at airport

2.4 Application of RFID in Airport Logistics Operations

An airport is a region of high flow of logistics and personal (Tirthankar, 2012). Every year billions of luggage and personnel move across airports. Moreover, the demand of air cargo is expected to grow in years to come. According to a report published on air cargo traffic, the global volume of air freight increased rapidly in recent years with freight volumes reaching 66.2 million metric tons in 2021 (E. Mazareanu, 2021). This increasing transportation of baggage and cargo across airports have required use of a technology that is fast, increases visibility and accurate to provide better customer service (Mishra et al, 2012). RFID has begun to be implemented in baggage handling and customer support sectors at major airports and airlines in the aviation industry. RFID technology offers huge economic benefits to both businesses and consumers while also having the potential to be one of the most intrusive monitoring tools endangering consumer privacies (Kelly, RFID tags: business applications vs. privacy protection). In airports, RFID technology is being used primarily in areas of baggage sorting, baggage identification, containers/ULDs, passenger-baggage matching, cargo, verification and dispatching (Mishra et al., 2012). The application areas of RFID in airport is shown in Figure 2.5. The two major application areas are described below:

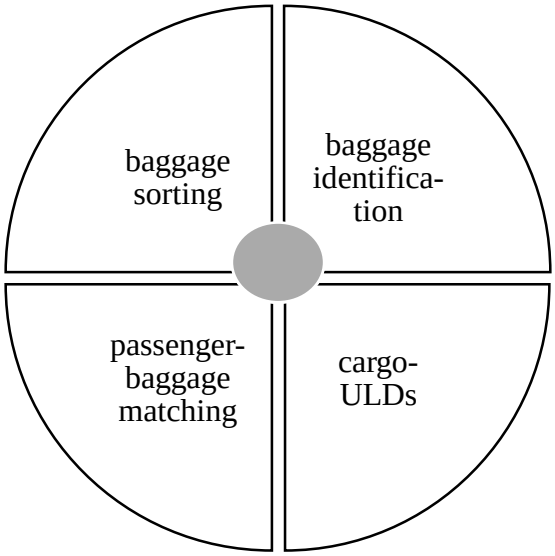

Figure 2.5 Application of RFID in Airport Logistics

a. Baggage Management

Airports are becoming larger and more comfortable on a daily basis, and time has become a key performance metric for both passengers and operators. The time issue has become a motivator, particularly for transit passengers at changeover locations. The effectiveness of the systems, which we might refer to as the airport's veins, began to gain prominence. Airport baggage handling systems (BHS) are among the most complicated systems (Mercan, 2022). It is a unique construction that incorporates both mechanical and electro-mechanical engineering principles into the system. The baggage handling system is in charge of ensuring that the baggage of incoming passengers is securely delivered to baggage trolleys or containers following check-in, as well as checking the baggage for security, security screening, sorting, and storage. This system is made up of conveyors that are linked together to build a larger system (Mercan, 2022). The baggage handling system is the most essential service network of airports in terms of operational efficiency, safety, and customer pleasure (Mishra, 2012). Moreover, the baggage management system is a key indicator of airport’s service quality as inefficient baggage service contributes towards passenger dissatisfaction (Mercan, 2022).

Baggage management is a substantial part of the aviation industry (Calders et al., 2015). RFID is being used in baggage management operation at airports. The number of passengers and luggage moving through an airport in exponentially increasing over the years. With this increased flow, the number of delayed, lost and mishandled baggage has been on the rise. Breakdowns at several airports during busy hours not only reduce passenger happiness, but also cause aircraft delays and significant expenditures. These systems must be efficient and reliable, especially at airports with a high volume of transit passengers. There may be instances where the person is unable to board the following aircraft and the luggage is unable to be loaded. As a result, incidents of passenger satisfaction and luggage loss should be considered as an inverse association. As technology associated to these airport systems evolve, unique tracking systems are integrated, and passenger happiness improves. The global mishandled baggage rate has increased by 24% in 2021, according to the SITA Baggage IT Insights 2022 report. According to the Baggage Report 2014, 21.8 million bags were affected by baggage mishandling, resulting in a loss of $2.09 billion USD to the airline sector (Tanvir, 2015).

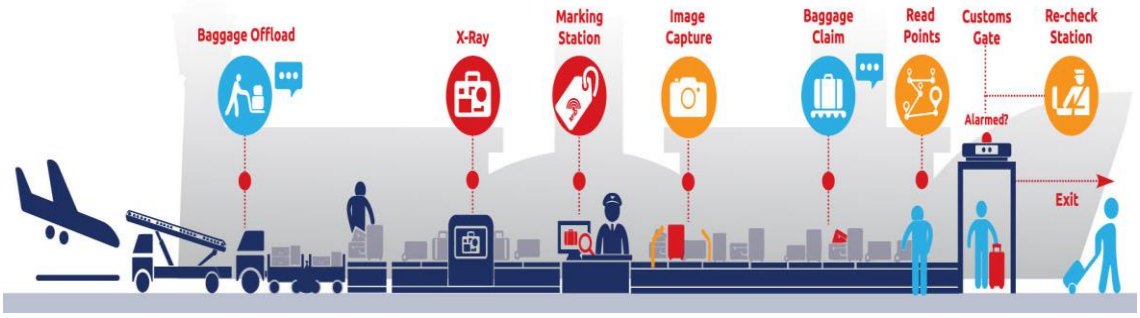

Figure 2.6 A general RFID based tracking system (source: trackit)

Improving baggage handling management is critical for increasing customer satisfaction and decreasing aircraft cycle time. The adoption of technology solutions at airports seeks to not only keep up with the rising number of passengers, but also to improve the passenger experience (S. Bouyakoub et al., 2017). Major airports have been considering the adoption of RFID technology for baggage handling process since 1999. Tests have been done at numerous airports/airlines in the world including Las Vegas, Jacksonville, Seattle, Los Angeles, San Francisco, Heathrow, Boston, New York, Gimpo-Seoul, Paris, Amsterdam, Rome and etc. In the US tests, it was turned out that RFID tags were far more accurate than bar code system when

applied to baggage handling operation. With the advancement of Internet technology and devices such as sensors, actuators, and tags, the physical world is being linked to cyberspace via smart gadgets, transforming the Internet into the "Internet of Things" (Bouyakoub, 2017).

The use of RFID technology helps for a more specific follow-up through all different stages of the baggage tracking process at an airport, particularly regarding registration of luggage, check and scan luggage, storage of luggage, sorting of luggage, withdrawal of luggage, loading and unloading from planes, and transfer of baggage between terminals (Achraf Haibi, 2011). A general RFID based tracking luggage system is shown in Figure 2.6. Figure 2.7 shows that according to SITA Baggage IT Insight (2022), out of 4.27 billion bags 24.8 million baggage were mishandled. In the mishandled baggage, the percentage of delayed baggage was 71%, the percentage e of damaged bags were 23% while 6 % bags were lost. Hence, to remedy it, real time access of baggage through transition is required. Also, a logical flow of baggage in airports is shown in Figure 2 .8.

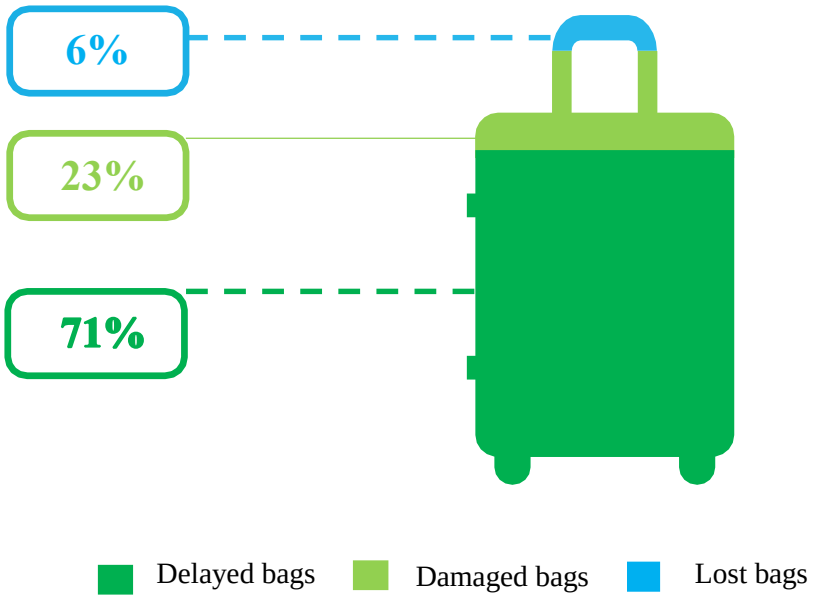

Figure 2.7 Baggage mishandling at airport in year 2021-2022 (SITA, 2022)

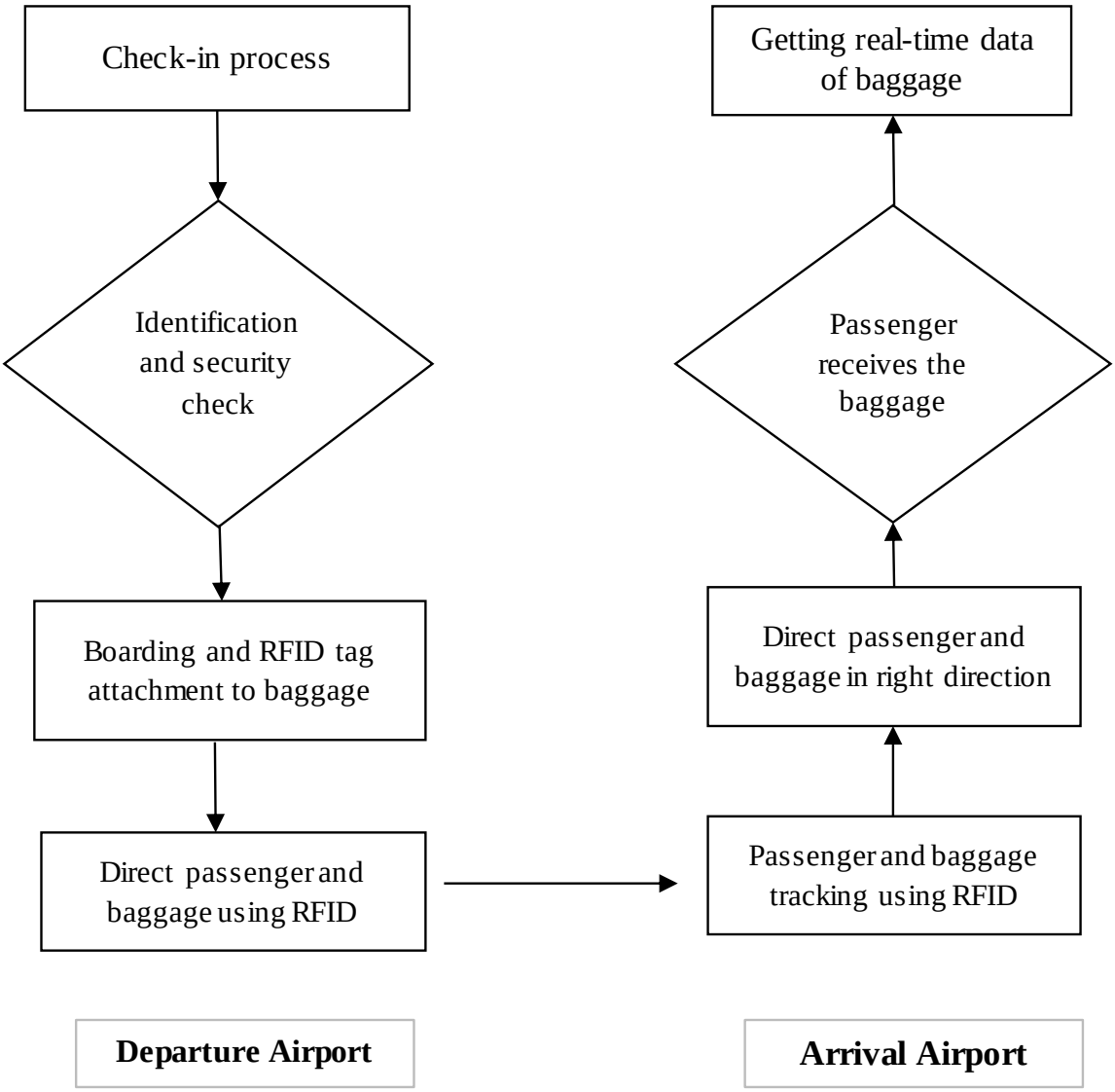

Figure 2.8 A logical flow of baggage using RFID

During air travel, baggage has to move across multiple paths and its movement is tracked at various points where RFID readers are attached (Md. Monzur Morshed et al., 2010). The areas for the baggage handling can be classified into following major zones.

i. Check-in area
ii. Conveyor
iii. Distribution area
iv. Trolley

There are a number of RFID readers placed across these zones where the baggage is tracked in real time.

b. Cargo Management

Air freight is also known as air cargo. It is the conveyance or transportation of products by an airline. When it comes to transferring express shipments throughout the world, air transport services are the most valuable, and they include air mail, air freight, and air express. The air cargo volume has been exponentially increasing over the years as shown in Figure 2.9 adapted from B. Feng et al. (2015). Large cargo airlines such as Lufthansa and Air France lose 5–6 percent of their Unit Load Device (ULD) inventory each year, equivalent to hundreds of millions of euros in losses, owing to malfunctions in the supply chain and its ULD tracking capabilities (Chang et al., 2010). RFID in air cargo management is primarily used in areas of tagging, loading, shipping, receiving and unloading. ULD management has further three areas of monitoring and control: ULD process, movement management and asset management. Normally the time ULDs enter the terminal until the time they are loaded onto an aircraft, it typically takes 4-24 hours (emergency cargo: 1.5 hours). All luggage at the truck dock should be loaded 4 hours before departure; animal and perishable goods should be entered terminal before 2.5 hours; and risky cargo should be stored in terminal 24 hours. During this time, an RFID tag linked to ULD records its whereabouts (Chang et al., 2010).

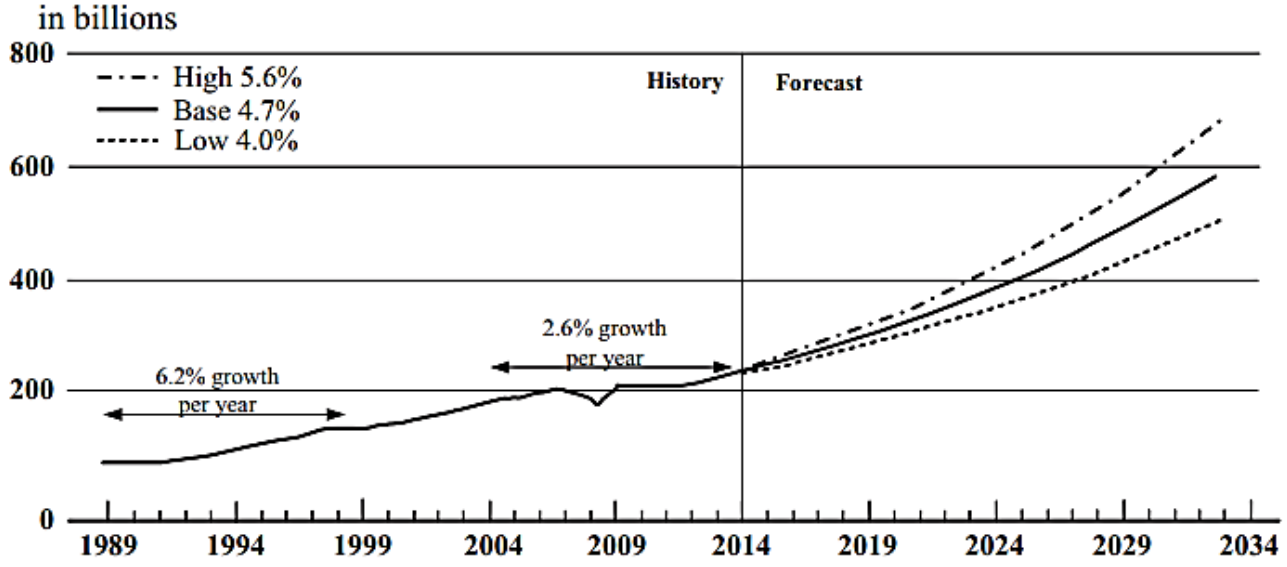

Figure 2.9 Volume of air cargo travelled across the world using airports

Air-cargo terminal is seen as one of the harshest environments for applying an RFID system for various electromagnetic noise sources and its operational setting. Five major zones are considered for ULD movement (Chang et al., 2010):

i. Truck dock
ii. Export zone
iii. Transit zone
iv. Import zone
v. Airside zone

2.5 Challenges of using RFID in Airport Logistics Operations

There are certain issues with the use of RFID at airport logistics operations. RFID technology is considered as one of the most disruptive technology over the years (Urso et al., 2020). Due to a variety of factors, there may be illegible tags in the reader's examination zone, causing its regular operation to be disturbed implies reading rates less than 100%, which is paradoxical to RFID's "complete visibility" premise (Can et al., 2010). The number of RFID readers and locations, their power levels, the speed of the baggage-handling conveyors, tag orientation, overlap with other tags, environmental noise, absorption, reflection, shadowing, interference, and the effects caused by the presence of metallic material attacks on RFID system. Inability to recognize a bag on a baggage conveyor can significantly increase the burden on a manual recovery conveyor, resulting in longer handling time and higher costs and lead to misplaced luggage (about 40 million bags per year) or misplaced luggage (about 50,000 per year) (Zhang et al., 2008). As a result, reliable and rapid luggage identification is essential and critical to attaining the main operational goal of airport. Such risks can lead to read-rate, security and privacy problems which can affect the RFID-based identification process and security of passengers. As a result of which, the overall effectiveness of RFID based baggage system decreases (Can et al., 2010). This way the timely delivery of checked baggage to gates is compromised.

2.6 Risks of using RFID Technology

Apart from the multifarious benefits that RFID offers, it also has negative effects that need attention. RFID by its development infrastructure has been vulnerabilities that result into security and privacy concerns (Kumar et al., 2021). So if the RFID is used in any system be it a part of any industry it poses some threats. Similar is the case when RFID is used in airports for baggage management. The risks of using RFID in airport logistics operations can compromise information and security in three major areas: availability, integrity and confidentiality. A compromise in these areas would mean that the service quality and passenger trust is compromised. A brief description of risk areas have been given below for your better understanding (Braganza et al., 2017).

1. Availability Related Risks

In an RFID system, availability refers to the fact that the original user's entree to resources or data at identified locations is provided. In terms of airport logistics operations, availability refers to the fact that genuine RFID tag can be accessible to the RFID genuine readers at various nodes. However, there are various threats to availability in RFID systems such as jamming, disabling tag, denial of service (DoS), and desynchronization attack (Kumar et al., 2021).

2. Integrity Related Risks

Integrity in RFID system ensures reliability and credibility of data while transmission over communication channels (Kumar et al., 2021). It refers to the fact that the information stored on the RFID tag shall not be subjected to any target of impersonation of piracy. There are various threats to the integrity of RFID systems such as tag cloning, spoofing attack, replay attack and relay attack.

3. Confidentiality Related Risks

In an RFID network system, secrecy is described as just an authorized user having access to sensitive information and protected data. In confidentiality, privacy of information is the main reason of concern for the organization and the user. Threats to secrecy of information and confidentiality include side-channeling, tracking, eavesdropping, key compromise, and privacy violations.

The following are the sub category risks that are in the domain of availability related risks. A brief description of these risks is also given below.

1. Jamming: The attacker jams communication between a valid tag and the reader, preventing the tag node from interacting with the reader. The attack generates a signal comparable to the reader, rendering the tag incomprehensible to the reader (Braganza et al., 2017).
2. Denial of Service (DoS): RFID devices have a limited amount of storage as well as a low-power battery. As a result, the attacker exploits of this and sends a large number of packets to the communication channel. As a result, the communication channel's bandwidth will grow. The Tag's power is put to good use in receiving these massive payloads. The RFID tag will be withdrawn from the RFID system due to power limits. (Braganza et al., 2017).
3. Desynchronization: In this attack, the synchronization can break between the tag and the reader. This will either make the reader unable to identify the tag or even detect the existence of the tag even though it is in range (Braganza et al., 2017)..
4. Covert Channel Attacks: In these sorts of cyber-attacks, the attacker builds unauthorized communication means to discreetly send data. The attacker covertly transmits the information by utilizing the unused memory space of several RFID tags, making it difficult to identify (Braganza et al., 2017).

The following are the sub category barriers that are in the domain of integrity related risks. (Braganza et al., 2017).

1. Tag Cloning: In cloning attack, a duplicate tag node similar to the existing tag node exists. Thus, the reader is not able to validate the cloned tag node, and the attack then results into unauthorized access to the reader (Braganza et al., 2017).
2. Spoofing: This attack is an impersonation type of attack in which a genuine tag is duplicated and all the information can be accessed (Braganza et al., 2017).
3. Replay: Replay attacks occur when an attacker listens in on a specific RFID system, captures the information going to and from the reader and sender, and then mimics the data getting transferred to act either as the originating readers or the tag. (Braganza et al., 2017).
4. Malicious Code Injection (MCI): As the name implies, the transmission of hostile code affects RFID network elements such as readers, communication networks, or devices, among others.

RFID tags' accessible memory is exploited to spread and store malicious programs or viruses in the back-end system (Braganza et al., 2017).

5. Relay Attack: In this technique, an attacker intercepts the communication between an RFID tag and a reader and then passes it to another device without examining or modifying it.

The following are the sub category barriers that are in the domain of confidentiality related risks. (Braganza et al., 2017).

1. Tracking: In the tracking attack, the attacker is able to guess the correct tag ID. This attack targets the confidentiality of the data.
2. Eavesdropping: The Eavesdropping attack is a passive attack. The tag comes in a range of the reader. Then, the communication takes place between tag and reader. During the exchange of information, the attacker steals information or message packets communicating between tags and the reader.
3. Disclosure: In a disclosure attack, the attacker would be able to guess secret information like shared key, ID, and other secret information from the RFID system.
4. Impersonation: This type of attack targets the security measure used for authentication of the RFID reader.
5. Side-Channel attack: In this type of attack, the stored information from the RFID system can be extracted by unauthorized authority by exploiting electromagnetic fields.

Occurrence of any of these risks associated with RFID can hamper the smooth logistics flow at an airport. A delay or inaccuracy at the airport may result in unmet consumer demand and additional costs. Previous study has quantified the benefits of employing RFID, however risk quantification has not been done in the literature. This research therefore aims to address this gap and come up with a quantitative risk index with reference to RFID implementation in airport logistics. Furthermore, this research will use a simulation based approach to model the risks of RFID in baggage and cargo handling. In addition to that, this research will develop risk mitigation strategies and minimization modelling of RFID risks in airport logistics flows. The risks of RFID in literature are found to be as shown in Figure 2.10.

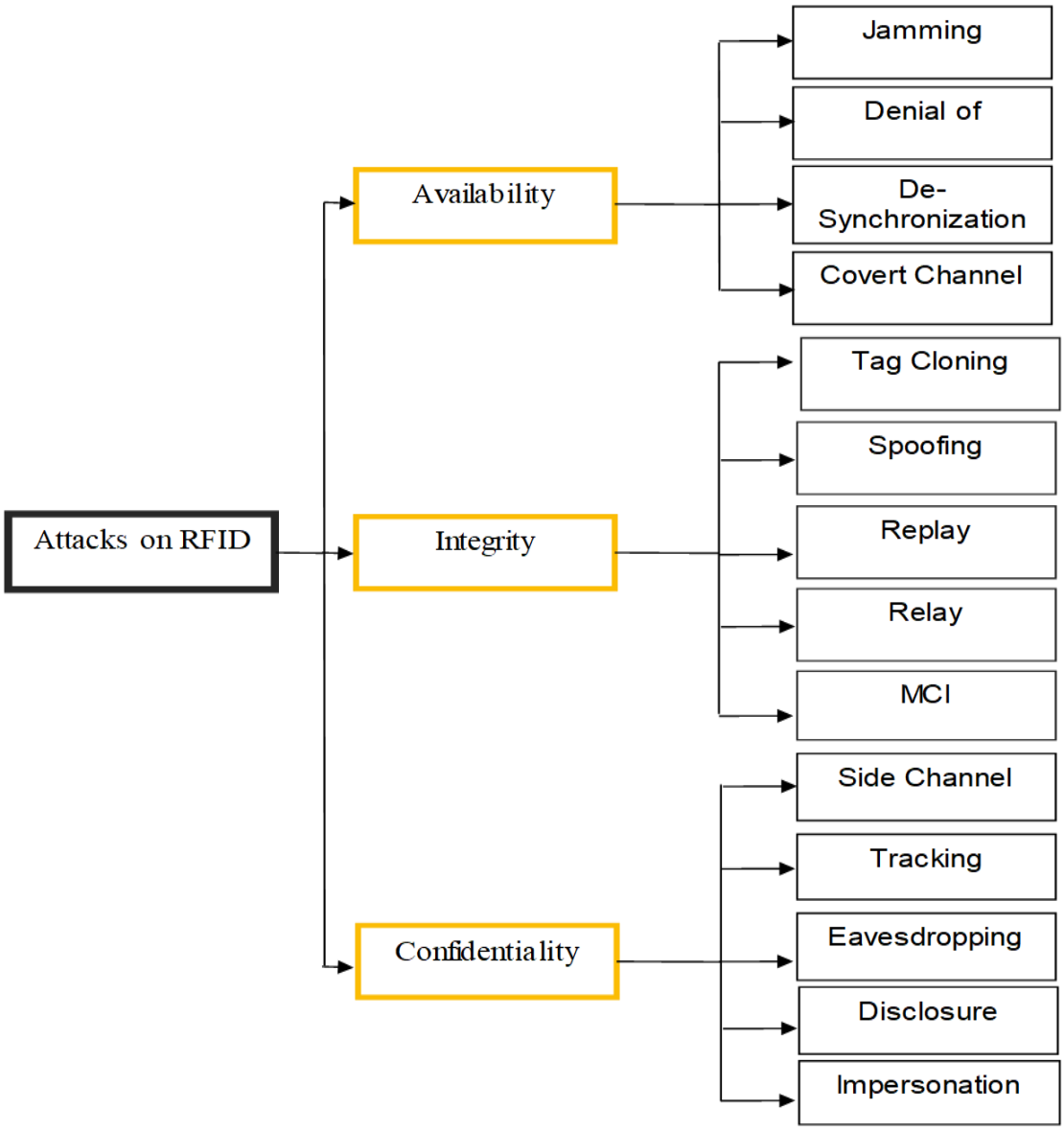

Figure 2.10 Attacks and risks on RFID system

Chapter 3. Research Methodology

This chapter of the dissertation presents and establishes the methodology that is to be used in this research study. The methodology is a framework which is novel in its approach as it is a qualitative-quantitative method of analyzing risks. This chapter develops the four stage risk assessment framework which uses a hybrid multi-criteria decision making technique and formulates a multi-objective optimization model for risk minimization. The algorithms used to complete each stage is also provided with step by step description. Moreover, this chapter introduces a novel concept of risk mitigation in which a risk mitigation matrix. Using the risk mitigation matrix, risk is then minimized by optimizing the risk reduction using goal programming.

3.1 Risk Assessment Framework

Risk assessment is significant for making long-term strategic decisions in an organization. Risk management is performed by undertaking a few crucial steps. These steps comprise of risk identification, risk assessment and risk mitigation. Averting any risk requires an organization to perform this hierarchy (Chan, 2012). There are many risk management frameworks are present in the literature. However, the research proposes a risk assessment framework methodology which is a novel integrated approach based on both qualitative and quantitative assessment. Different sectors have different standard risk assessment models. Most commonly used risk assessment frameworks include the Supply Chain Risk Assessment (SCAR), SCOR model, Failure Mode and Effect Analysis (FMEA), EVITA, HEAVENS, CEA, MITIGATE, NIST and House of Risk (HOR). Using these frameworks, a number of researches have conducted risk assessments for various risks and threats.

The above mentioned studies do not take in to account the risk mitigation part from a strategic point of view. In addition, these risk assessments do not provide a cost-risk analysis for problem solving. The proposed framework in this research study however is a more holistic and practical approach towards finding and mitigating risks. The framework is based on four stages of risk assessment as are shown in Figure 3.1. The result obtained from one stage is then used in the next stage for further calculations. This risk assessment framework is the foundation of the research. Each stage of the framework is based on a number of sub steps which are performed to complete the risk analysis. Each stage is further explained in more detail below.

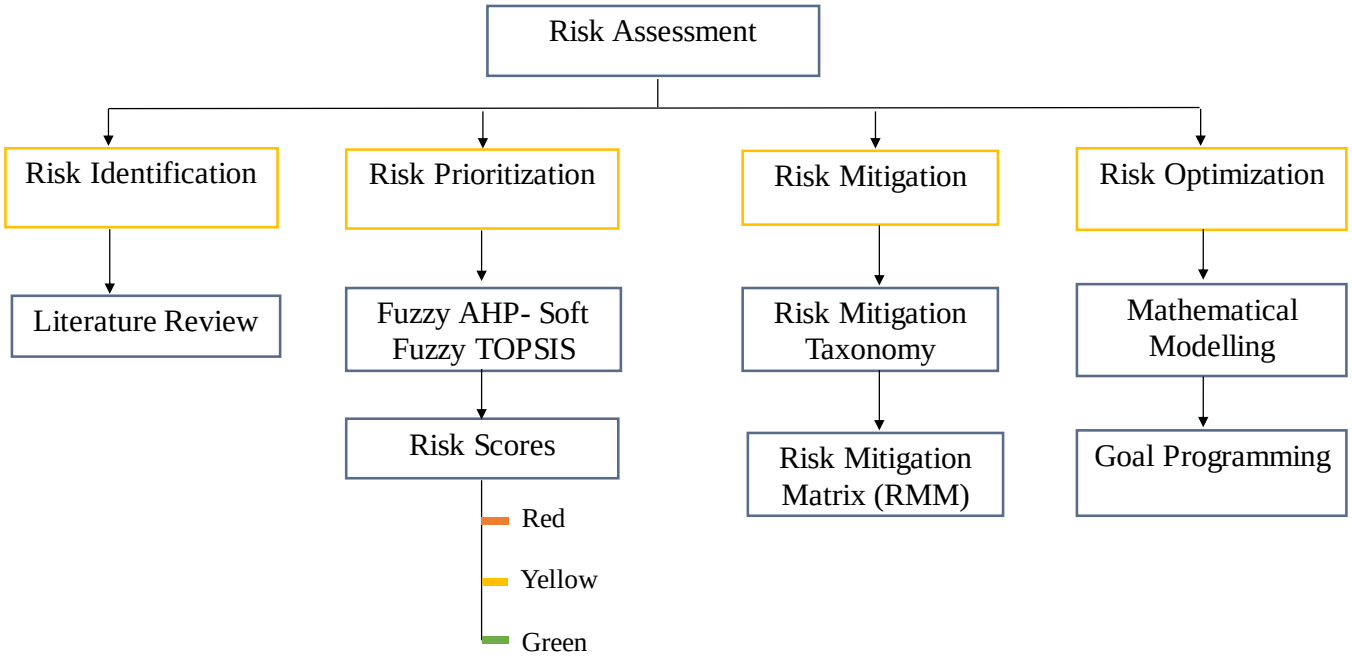

Figure 3.1 Proposed Risk Assessment Framework

3.1.1 Part 1: Risk Identification

The risk assessment procedure is divided into four parts. The first phase is of risk identification, which aims to provide a comprehensive list of events and their potential repercussions (Amirshenava et al., 2018). The risks can be identified by reviewing the literature or by taking expert input. The identified risks can then be used to make a risk hierarchy that would be used in the next step. In this research, the risks identification is carried out extensively by reviewing the literature. Once the risks are identified only then further computation can be performed. So the risk identification stage sets the foundation of this research framework for risk assessment.

3.1.2 Part 2: Fuzzy Analytical Hierarchy Process (FAHP) - Fuzzy Technique for Order Preference by Similarity to Ideal Solution (FTOPSIS)

After identification of the risks, risks are to be ranked in an order. Ranking of risks has been adopted in some of the prominent methods of risk assessment, one such is Failure Mode and

Effect Analysis (FMEA) which ranks risks on basis of the risk priority number (RPN). Several multi-criteria decision making techniques have been used in literature to rank risks. The FAHP-FTOPSIS is a hybrid multi-criteria decision making technique used for ranking different factors against multiple criteria. Both qualitative and quantitative methodologies are used in hybrid models. Because supply chain risks are unknown and there is a lack of risk data, hybrid modelling approaches are helpful for risk analysis, evaluation, and devising appropriate mitigation measures (F. Aqlan et al., 2015).

For risk assessment of using RFID technology in logistics of airport, this research uses a hybrid multi criteria decision making (MCDM) technique-Fuzzy Analytical Hierarchy Process (FAHP) – Fuzzy Technique for Order Preference by Similarity to Ideal Solution (FTOPSIS). The MCDM technique will be used for quantifying the risks of using RFID in logistics operations of airport and determine a risk index. The risk index will indicate the high and low ranked risks. FAHP-FTOPSIS has been excessively used in literature where risk assessment is involved (Chan 2012). AHP has also been used to rank criteria, however, subjectivity is involved in assigning weights via AHP. Therefore, an extended approach of AHP known as Fuzzy AHP will be used for the purpose of assigning weights to different alternatives. Felix T.S. Chan (2012) used FAHP-FTOPSIS for quantifying risks in a supply chain. Specifically, this research will deliver a risk quantification framework and strengthen the inquiry of risk management for the logistics flow at airports.

The risk priorities that will be determined by this research would allow for the application of systematic risk mitigation techniques and the deployment of essential resources to maximize the efficiency of airport logistics management. The first stage is to create a detailed hierarchy of all the risks of RFID that could affect the airport logistics operation of baggage management. This is accomplished by extensively researching under consideration and identifying any flaws. The next stage in the process is to give weights to the criteria based on their relevance. Fuzzy AHP is employed for this, and expert opinions are used as input. The third phase is calculating the scores of various risks by examining them through various criteria. In the second phase of this research, the FAHP-FTOPSIS is used for risk ranking. It would be performed in two steps as discussed below.

1. Fuzzy Analytical Hierarchy Process (FAHP)

Analytic Hierarchy Process (AHP) is a widely used multi-criteria decision-making process that uses pairwise comparison to determine the weights of criteria and the priority of alternatives in an organized manner. Because subjective judgments during comparison may be erroneous, fuzzy sets and AHP have been merged (Liu et al., 2020). This is known as fuzzy AHP or FAHP. The FAHP multi-criteria decision making technique is first used to identify the weights of different risk factors by conducting pairwise comparison of all the risks. Pairwise comparison would be done by experts via filling questionnaires designed for collecting responses. The method used for calculation of fuzzy weights is the fuzzy geometric mean method as used by (Buckley, 1998). However, after the calculations performed in fuzzy numbers, the final weights are converted into crisp weights for being used in Fuzzy TOPSIS.

By integrating Saaty's AHP with fuzzy set theory, the fuzzy AHP technique expands Saaty's AHP. Fuzzy ratio scales are used in fuzzy AHP to reflect the relative strength of the factors in the related criterion. As a result, a fuzzy judgment matrix may be created. The steps for creating a fuzzy AHP model are as follows: creating the comparison matrix, aggregating many judgments, assessing consistency, and defuzzifying the fuzzy weights (Liu et al., 2020). The best option is determined by sorting the fuzzy numbers using specific algebraic operations. These fuzzy numbers are obtained through triangular membership functions. A fuzzy judgment vector is then created for each risk by using fuzzy integers to represent the relative relevance of one risk category over another. These judgment vectors form part of the fuzzy pairwise comparison matrix (Buckley, 1998).

For the purpose of pairwise comparison through FAHP, a questionnaire is prepared. The target sample size for experts in the researches through literature review is between 5 and 15. So, for this research a sample size of eight has been taken. Next, the experts through questionnaires provide their opinions in the form of the linguistic terms, which are subsequently transformed and examined to determine the weights. The linguistic terms are against the different levels. These levels are also then converted into fuzzy triangular membership function values. The methodology steps are as given below.

Step 1: Create a pair-wise comparison matrix with the help of scale of relative importance as proposed by Saaty (1980). Using the pairwise comparison matrix, a decision matrix is obtained. The scale of relative importance used for the creation of pairwise comparison is shown in Table 3.1.

Table 3.1 Scale of relative importance

Scale	Meaning	Fuzzy Values
1.0	Equally Important	1,1,3
3.0	Moderately Important	1,3,5
5.0	Strongly Important	3,5,7
7.0	Very Strongly Important	5,7,9
9.0	Extremely Important	7,9,9

Step 2: Next, the crisp numbers from the scale are replaced with fuzzy triangular membership function values. A fuzzy triangular number has three points: left, middle and right to cover the area under the triangle. Equation 3.1 shows hoe the three points represent one fuzzy number.

$$\mu\Delta(x) = \Delta = (n, m, o) \tag{3.1}$$

Also, calculation of inverse fuzzy number is performed where needed for intermediate values and a final fuzzified pairwise matrix is obtained. The inverse calculation is done by equation 3.2.

$$A^{-1} = (n, m, o)^{-1} = \left(\frac{1}{o}, \frac{1}{m}, \frac{1}{n} \right) \tag{3.2}$$

Step 3: Create a fuzzified pairwise comparison matrix for each decision maker.

Step 4: Calculate Fuzzy geometric mean values using the formula given in equation 3.3 and 3.4. Here eq. 3.3 and eq. 3.4 show how two fuzzy numbers are multiplied. ri gives the product of two numbers.

$$A_1 \otimes A_2 = (n_1, m_1, o_1) \otimes (n_2, m_2, o_2) \tag{3.3}$$

$$r_i = (n_1 * n_2, m_1 * m_2, o_1 * o_2) \tag{3.4}$$

Step 5: Calculate the fuzzy weights of alternatives. The fuzzy weights are obtained by first adding all the geometric mean values and then taking an inverse. Next, the inversed sum of the geometric mean values is multiplied with the fuzzy geometric mean values obtained from step 4.

$$w_i = r_i \otimes (r_1 \oplus r_2 \oplus \ldots \oplus r_n)^{-1} \tag{3.5}$$

Where w_i is the fuzzy weight and i is *1, 2…n*. While $r_i$is the geometric mean value. The addition for two fuzzy numbers is shown in eq. 3.6.

$$A_1 \oplus A_2 = (n_1, m_1, o_1) \oplus (n_2, m_2, o_2) \tag{3.6}$$

Step 6: De-fuzzification by center of area method to obtain crisp weights. The de-fuzzification will give the final value in crisp number.

$$COA = wi = \left(\frac{n + m + o}{3}\right) \tag{3.7}$$

Fuzzy AHP is used to only calculate weights of the risks and not to rank them. The weights calculated from this method will be incorporated in Fuzzy TOPSIS to finally rank the risks. The weights obtained from eq. 3.7 for one risk w.r.t all eight experts is then averaged to obtain a single weight for a particular type of risk.

2. Fuzzy Technique for Order Preference by Similarity to Ideal Solution (FTOPSIS)

Hwang and Yoon (1992) introduced the Approach for Order Performance by Similarity to Ideal Solution (TOPSIS), which is the most well-known technique for tackling MCDM issues. This strategy is based on the idea that the chosen option should be the closest to the Positive Ideal Solution (PIS) - the solution that minimizes the cost criteria while maximizing the benefit criteria- and the furthest away from the Negative Ideal Solution (NIS) (Nădăban et al., 2016). In this step, a fuzzy pairwise comparison of risks is performed against five different parameters or criteria.

These parameters are risk type, probability of occurrence, impact of risk, ease of mitigation, and cost of activity increase. Next, the fuzzy decision matrix is normalized. After normalization of matrix, defuzzification is done by using center of area (COA) method. Now, this de-fuzzified matrix is multiplied with weights obtained from FAHP to get scores for different risks. These scores will give the prioritized risk index dividing risks into three categories: red, yellow and green (moving from more risky to less risky).

TOPSIS has been widely used in various cases because of its simplicity, computing efficiency, and broad mathematical notion. The fuzzy TOPSIS approach, which extends the conventional TOPSIS method with reference to fuzzy logic, has also been effectively deployed in a variety of application areas (Palczewski, 2019). A review study of Fuzzy TOPSIS by Palczewski (2019) shows that fuzzy TOPSIS was applied in many real-world use cases, starting from selecting a proper supplier for manufacturing, through assessment of services quality, selection of weapon for defense industry and ending at selection and ranking of the renewable energy sources, proving that is broadly employed in a range of practical problems. There have been many variants of TOPSIS used in literature and the most number of times used one is FTOPSIS which accounts for 19 out of 25 implementations (Palczewski, 2019).

Step 1: Develop a decision matrix using linguistic terms for comparison of alternatives against different parameters. Here the risks are compared against different parameters to assess their importance.

Step 2: Formulate a group decision matrix. For group decision making where opinion is collected from experts, linguistic scale is converted to fuzzy numbers; we get a fuzzified matrix.

Step 3: Combine group decision matrix is made by using the formulas in eq. 3.8 and eq. 3.9 as used by (Nădăban et al., 2016).

$$X_{ij} = \left(a_{ij}, b_{ij}, c_{ij}\right) \tag{3.8}$$

$$a_{ij} = min\left[a_{ij}^{k}\right], b_{ij} = \frac{1}{k}\sum_{k=1}^{K} b_{ij}^{k}\ , c_{ij} = max\left[c_{ij}^{k}\right] \tag{3.9}$$

Here *i* represents the number of alternatives (risks), *j* represents the number of parameters or criteria. The value of *k* varies as the number of decision makers k= 1, 2…n. In eq. 3.9,

the a_{ij} is the minimum value of all the first numbers of a fuzzy vale, c_{ij} is the maximum of the last numbers while b_{ij} is the average of all the middle numbers in the fuzzy values.

Step 4: Compute normalized fuzzy decision matrix. This is done using the formula below in eq.3.10.

$$r_{ij} = (r_{aij,} r_{bij,} r_{cij}) = \left(\frac{c_j^+ - c_{ij}}{c_j^+ - a_j^-}, \frac{c_j^+ - b_{ij}}{c_j^+ - a_j^-}, \frac{c_j^+ - a_{ij}}{c_j^+ - a_j^-}\right) \quad (3.10)$$

Where $c_j^+ = max_i c_{ij}$ and $a_j^- = min_i a_{ij}$.

Step 5: De-fuzzification of the normalized fuzzy decision matrix by center of area (COA) method. The defuzzification is carried out to obtain a crisp value that can be used to obtain a weighted decision matrix.

$$r_{ij}'' = \left(\frac{r_{aij+} r_{bij+} r_{cij}}{3}\right) \quad (3.11)$$

Step 6: Compute a weighted normalized decision matrix:

$$v_{ij} = w_i * r_{ij}'' \quad (3.12)$$

Here w_i is the weight of respective risks calculated from Fuzzy-AHP from eq. 3.7 after average is taken since there are a total of eight experts.

Step 7: Compare above values to positive and negative ideal solutions by using following formulas'.

$$A^* = \{(\max v_{ij} \mid j \in J), (\min v_{ij} \mid j \in J') \mid i = 1,2, \dots, m\} \quad (3.13)$$

$$A^- = \{(\min v_{ij} \mid j \in J), (\max v_{ij} \mid j \in J') \mid i = 1,2, \dots, m\} \quad (3.14)$$

Step 8: Compute distance of each value from positive and negative ideal solution. These are the Euclidean distances.

$$d_i^* = \sqrt{\sum_{i=1}^{n} (v_{ij} - A^*)^2} \quad (3.15)$$

$$d_i^- = \sqrt{\sum_{i=1}^{n} (v_{ij} - A^-)^2} \quad (3.16)$$

Step 9: Compute closeness co-efficient for each alternative to the negative ideal solution. Computing closeness to negative ideal solution gives rank of risks in descending order of importance. And finally rank according to the closeness coefficient index (CCI) as calculated. The higher value is given the higher rank.

$$CCI = \frac{d_i^-}{d_i^* + d_i^-} \tag{3.17}$$

The flow of MCDM methodology is shown as in Figure 3.2.

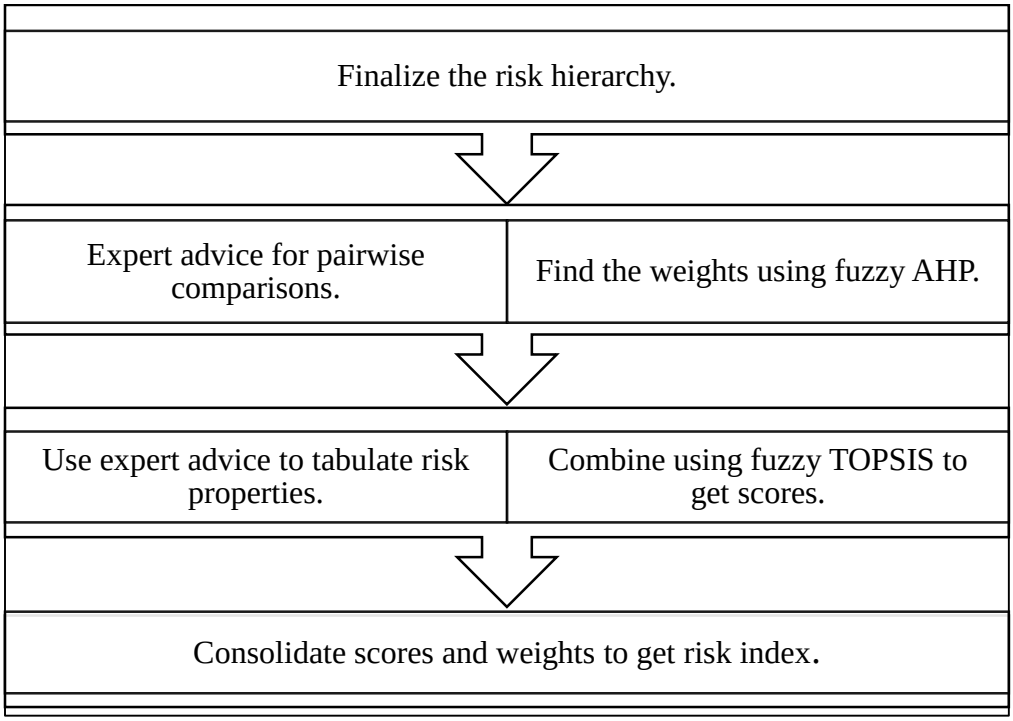

Figure 3.2 Flow of FAHP-FTOPSIS

The risks obtained from the FAHP-FTOPSIS are then categorized into three risk areas that are marked by colors; red, yellow and green. The red zone risks are the one that are of highest importance and can cause more disruption. The yellow zone risks are of moderate significance while green zone risks are safe zone risks. Now, this categorization is done on the basis of CCI values obtained from FTOPSIS for each risks. Next, ranges are determined and risks falling in range determined for red zones are taken to next step. The categorization of these risks is done by using a data mining approach of K-Mean clustering. This methodology takes the CCI values as the

data set and divides it into *k* number of clusters. Then, it assigns centroid values to each cluster and determines the Euclidean distance of each data point from the respective centroid. This method is repeated until the sampling condition is satisfied.

3.1.3 Part 3: Risk Mitigation

According to Chopra and Sodhi (2004), there is no one-size-fits-all technique for protecting organizational supply chains against risks, and managers must select the appropriate risk-mitigation strategy for each risk. Mitigation methods are classified into four categories (Zsidisin and Ritchie).2009): (1) remove the risk, (2) minimize the frequency and severity of the risk, and (3) shift the risk through insurance and risk sharing, and (4) risk acceptance. Managers often select appropriate mitigation techniques depending on a number of factors such as the type of the risk, the source of the risk, the company's resources, and so on. Other techniques for mitigation include the following: risk avoidance and risk exploitation (F. Aqlan et al., 2015).

To control and mitigate the risks, effective mitigation strategies must be identified and developed (F. Aqlan et al., 2015). There are two kinds of mitigation strategies: proactive and reactive. Proactive risk reduction solutions focus on risk prevention. Reactive risk mitigation techniques, on the other hand, plan for the occurrence of a risk event in order to mitigate its economic impact (Panjehfouladgaran & Lim, 2020). Once the prioritized list of risks is obtained, then next task will be to effectively manage and control these risks. It is important to effectively mitigate the risks after their identification to achieve organizational efficiency. Thus, this research proposes a comprehensive Risk Mitigation Matrix (RMM) that shows the risk reduction by each mitigation strategy. This phase is further divided into three steps as are described below:

1. Identification of Mitigation Strategies

Risk mitigation is a significant part while doing risk assessment. Risk control strategies can either be identified from literature, expert opinion or be developed. In this research, the mitigation strategies are identified by reviewing the literature. Extensive review of literature is done by exploring the recent papers since such papers have strategies that are nor obsolete and are still in use. For the proposed risk assessment, such mitigation strategies for red zone risks are identified that can mitigate more than one risk at a time. This way implementing that strategy not

only cut downs on the resources used for implementation but also time which is important for large-scale organizations.

2. Development of Risk-Mitigation Taxonomy

When the risks are of serious nature and multiple, it is pertinent to develop a taxonomy of risks that is based on inter-correlation between them. Mitigation techniques should be proactive and very effective in preventing any form of service disruption incident (Panjehfouladgaran & Lim, 2020). For example, one mitigation strategy can mitigate one or more than one risks. For selection of appropriate mitigation strategies that result into risk minimization by increasing the risk reduction, a RMM is proposed in this research. The risk mitigation matrix will show risk interconnections with risk reduction by each mitigation strategy. The experts mark the risk reduction on basis of two major factors: probability of occurrence of risk and impact. The RMM will also include the cost of mitigation strategies. On the basis of this RMM, the mitigation strategies are to be selected for risk minimization.

The RMM is shown in Table 3.2. The Table 3.2 can be filled by using approach in Figure 3.3. The first column in Table 3.2 shows the mitigation strategies while the next five columns show the red zone risks. After that, second last column shows the risk reduction score.

Table 3.2 Risk Mitigation Matrix

Mitigation/Risk	Risk 1	Risk 2	Risk 3	Risk 4	Risk 5	Mitigation Score	Mitigation Cost
Strategy 1	?	?	?	?	?	?	?
Strategy 2	?	?	?	?	?	?	?
Strategy 3	?	?	?	?	?	?	?
Strategy 4	?	?	?	?	?	?	?
Strategy 5	?	?	?	?	?	?	?
Strategy 6	?	?	?	?	?	?	?
Current Risk Score	?	?	?	?	?	?	?

3. Algorithm for filling Risk Mitigation Matrix (RMM)

Using the risk-mitigation taxonomy developed from the aforementioned discussion, next a RMM is constructed. RMM is novel method of maximizing the risk minimization or risk reduction. It is a table made of series of rows and columns representing mitigation strategies and risks respectively. Only those risks are considered here that were obtained from Section 3.1.2 falling in the red zone using K-Mean clustering algorithm. Considering those risks, before and after using mitigation strategy values of risks are put in the RMM to obtain the final risk reduction value. Moreover, the RMM also considers the cost of implementing the mitigation strategies. This is the cost that should remain under the budget constraint in order to satisfy the optimization in next Section 3.1.4. For filling of the Risk Mitigation Matrix (RMM), a three phase algorithm is proposed.

In the first stage, two calculations are simultaneously performed. First, data is collected from a set of 8 experts on probability and impact of risks using a linguistics scale. This data collection is done from two set of experts; before and after implementation of mitigation strategies. Next, these crisp values are converted into fuzzy numbers using triangular fuzzy numbers equivalent. Next, two fuzzy numbers in the form of probability and impact are multiplied using fuzzy multiplication by QKB method (Qudaimi et al, 2021) named after the authors of that research. Following this step, defuzzification is done using the Center of Area (COA) method. As a result, the value of R1 is obtained which is the value of risk before any mitigation strategy is used. On the other side, the value of R2 is calculated which is the value of risk after a mitigation strategy is implemented by following the same steps as for R1. Next is the phase 2 in which the risk reduction R' value is calculated by subtracting R2 from R1. In the third and last phase, the R' risk reduction value is normalized and risk reduction by mitigation strategy score is calculated. The algorithm is shown in Figure 3.3.

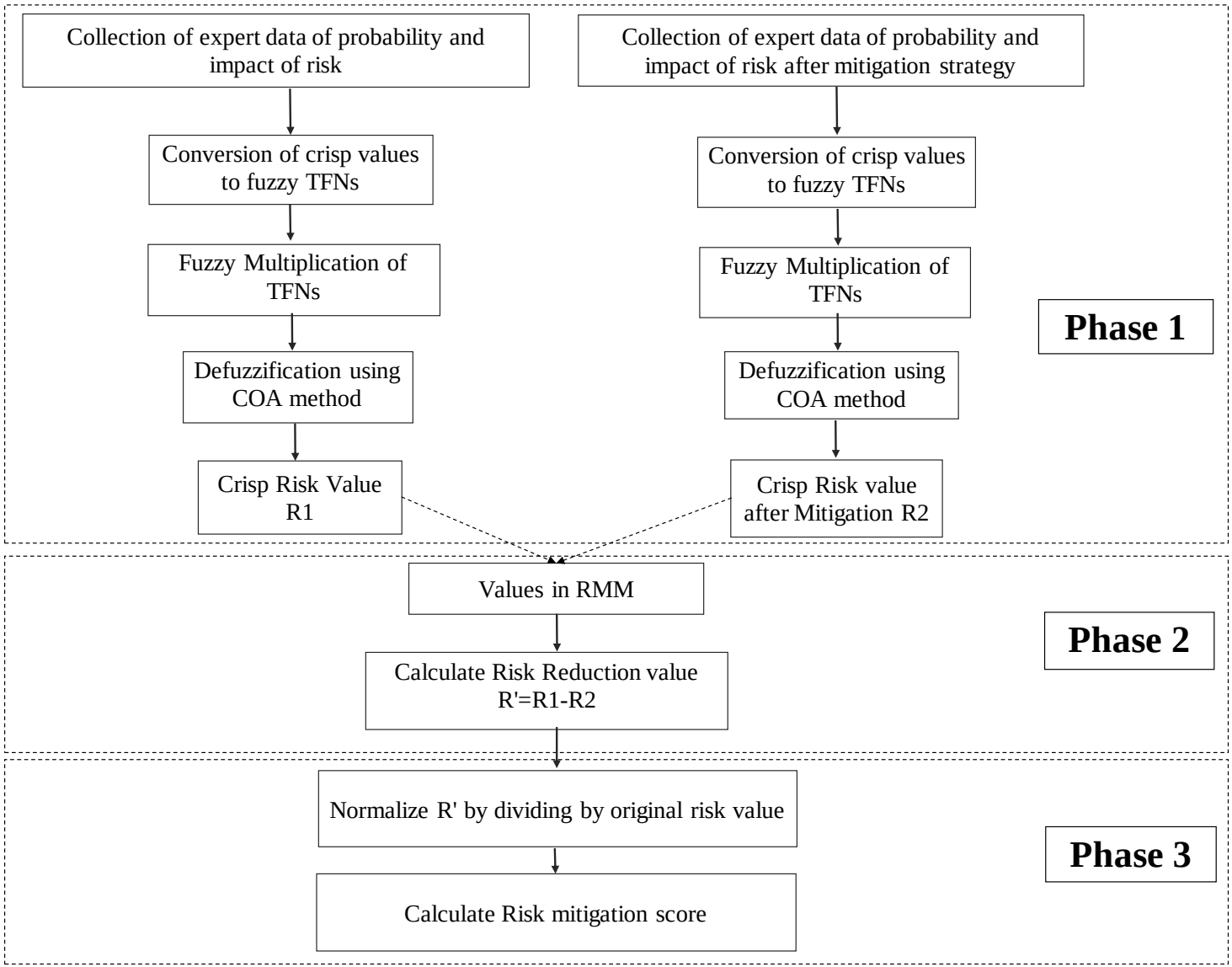

Figure 3.3 Algorithm for Risk Mitigation Matrix

3.1.4 Part 4: Risk Reduction Optimization

Once the RMM is obtained, then an optimization problem is formulated. A risk reduction based approach is adopted to minimize the risks. The risk reduction optimization is used for selecting those set of mitigation strategies that would reduce risks more. Hence, as a result of this the risk would be minimized by using the most apt set of mitigation strategies. The optimization is performed for selection of best combination of mitigation strategies that satisfy two constraints: risk reduction and cost minimization. First, two single objective functions are formulated and used to get results. Since there are two major objectives when using a mitigation strategy to mitigate risk: risk reduction and cost (F. Aqlan et al., 2015). Thus, two single objective models were formulated. Below is given the Table 3.3 showing list of parameters and variables.

Table 3.3 Sets, paramerters and variables

M	Set of risks (index *i*)
N	Impact of risk (index *j*)
R_i	Current level of risk *i* before implementing mitigation strategy *j*
R'_{ij}	Amount of reduction in risk *i* after implementing mitigation strategy *j*
C_j	Cost of implementing mitigation strategy *k*
B	Dedicated budget for risk mitigation
x_j	1 if mitigation strategy *j* is selected 0, otherwise

Using the two single objective functions, a single multi-objective function is formulated by using linear integer weighted goal programming approach. This model is constructed in a way that different preference weights are assigned to the two goals under consideration. These goals are then varied to conduct sensitivity analysis and study the optimal conditions under which the risk reduction and cost goal is achieved. Moreover, different cases are constructed in which both goals are varied one by one and the corresponding effect is observed.

1a. Risk Reduction Objective

The first single objective is to minimize the risk by maximizing the risk reduction. Risk reduction is the level by which a risk is reduced after using a mitigation strategy. The risk reduction maximization as objective function is formulated below in eq. 3.18. Here, R'_{ij} is the risk reduced after using a mitigation technique. For the under consideration objective, this value for a risk is divided by R_i which is the value of original risk to normalize the values and obtain it between 0 and 1. Next, the values are summed for all the mitigation strategies to obtain the result.

$$\min Z_1 = \sum_{i=1}^{M} \sum_{j=1}^{N} \left(\frac{R_{ij}^{'} * x_j}{R_i} \right) \tag{3.18}$$

1b. Constraints of the model

The constraints of this model are the budget constraints and the positive risk reduction value constraints.

i. Budget constraint

The budget constraints limits the costs of implementing mitigation strategies to a value that is either less than the allocated budget value or equal. This budget limit acts as an above cap that cannot be crossed. The budget constraint is given in eq. 3.19.

$$\sum_{j=1}^{N} (x_j * C_j) \leq B \tag{3.19}$$

ii. Positive reduction value

The positive risk reduction constraint is to make sure that a certain level of risk reduction has occurred. It aims to eliminate the possibility that the risk reduction after implementation of mitigation strategies is equal to zero which means none. The constraint is shown in the eq. 3.20.

$$\sum_{j=1}^{N}(R_{ij}^{'} * x_j) \geq 0 \qquad \forall i \in M \tag{3.20}$$

$$x \in [0,1], binary \tag{3.21}$$

In a nutshell, the objective function as shown above maximizes the risk reduction after using mitigation strategies. The constraint 3.19 ensures that the sum of cost of mitigation strategies will be within the budget. The constraint 3.20 ensures that risk reduction should be positive meaning thereby that a certain risk reduction after implementing a mitigation strategy must exist.

2a. Objective of Cost Minimization

The second single objective model is for cost minimization as shown below in eq. 3.22. This constraint controls the cost values of implementing mitigation strategies and assures that the budget value is not crossed.

$$\min Z_2 = \sum_{j=1}^{N}(x_j * C_j) \tag{3.22}$$

2b. Constraints of the model

The constraints of the cost minimization are shown as in eq. 3.23 and eq. 3.24.

i. Positive reduction value

The positive risk reduction constraint requires that a specific degree of risk reduction take place. It seeks to eliminate the chance that the risk reduction following mitigation strategy implementation is equal to zero, i.e. none. The constraint is expressed in the equation 3.23.

$$\sum_{j=1}^{N}(R_{ij}^{'} * x_j) \geq 0 \qquad \forall i \in M \tag{3.23}$$

$$x \in [0,1], binary \tag{3.24}$$

3a. Multi-Objective Function

By combining both these objective, one single- multi objective model can be formulated. This multi-objective model function can then be solved by using a multi-objective optimization technique. In this research a weighted goal programming is used to solve the model. The combined model is as shown below in eq.3.25. Here w_1 and w_2 are the weights assigned to both the goal 1 i.e. of risk reduction and goal 2 i.e. of mitigation cost respectively. And d_1^- and d_2^+ are the negative and positive deviations related to goal 1 and 2 respectively.

$$\min Z_3 = w_1 d_1^- + w_2 d_2^+ \tag{3.25}$$

3b. Constraints of the model

There are two major goal constraints of the multi-objective model are risk reduction and cost minimization.

i. Risk Reduction Maximization Constraint

The first constraint for goal programming model is of risk reduction. Here in eq. 3.26, b1 represents the risk reduction goal. This equation shows that risk reduction should achieve the goal set for risk reduction where positive deviations are possible but negative deviations are to be reduced.

$$\sum_{i=1}^{M}\sum_{j=1}^{N}\left(\frac{R_{ij}^{'} * x_j}{R_i}\right) + d_1^- - d_1^+ = b_1 \tag{3.26}$$

ii. Cost Minimization Constraint

The second goal constraint is of cost. The constraint given in eq. 3.27 shows that the sum of all the costs of mitigation strategies should be kept below the total value of allocated budget. Here, b2 represents the cost goal.

$$\sum_{j=1}^{N}(x_j * C_j) + d_2^- - d_2^+ = b_2 \tag{3.27}$$

iii. Positive Reduction Value

The positive risk reduction constraint requires that a specific degree of risk reduction take place. It seeks to eliminate the chance that the risk reduction following mitigation strategy implementation is equal to zero, i.e. none. The constraint is expressed in the equation 3.28.

$$\sum_{j=1}^{N}(R_{ij}^{'} * x_j) \geq 0 \qquad \forall i \in M \tag{3.28}$$

iv. Additional constraints

$$x \in [0,1], binary \tag{3.29}$$

$$d_1^-, d_1^+, d_2^-, d_2^+ \geq 0 \tag{3.30}$$

Using the risk optimization modelling, the objective is to select intelligently those set of mitigation strategies that ensure maximum risk reduction by not violating the cost constraint. For risk reduction optimization, the risk reduction after using mitigation score is aimed to be maximized. The risk reduction score is the one obtained from RMM which is an accumulating sum of the risk reduction value obtained by one mitigation strategy for multiple risks. In this way, intelligent resource allocation can be performed.

Chapter 4. Results

This chapter of the research thesis presents the results obtained after using the novel integrated risk assessment framework presented in Chapter 3. Stage wise results obtained from the risk assessment have been shown in this chapter along with a description of the results. The risk identified for use of RFID in baggage management are fourteen in number. These risks fall into three different categories where disruption and impact can occur. From those risks the most important risks are identified. This is done by using a MCDM technique. To control the red zone risks, proper mitigation strategies are identified which are -for this study- six in number. Numerical analysis is conducted on the RMM and the optimal conditions for risk minimization are studied.

4.1 Risk Identification

For risk assessment of using the RFID technology in airport logistics operation of baggage management, first the risks were identified. The risk identification was done by extensively reviewing the literature. A total of fourteen risks were identified which make an RFID system susceptible to security, privacy and management risks. Following risks were identified from the literature as shown in Table 4.1. These risks are then identified from reviewing research papers, review papers, conference papers, reports and IEEE. Risks or threats that are linked with RFID have been studied excessively from perspective of industries other than aviation. Thus, by this study the research gap is bridged and those risks have been studied in this research. The risks of RFID fall into three major categories that are identified in literature: confidentiality, integrity and availability (Kumar et al., 2021). A detailed explanation of these risks is given in Chapter 2.

Kumar et al (2021) refers to the problem and explains that as RFID devices have become essential part of our computing, various threats paradigms are open. Kumar (2021) puts stress on the importance of identifying and finding solutions for these risks of RFID. He identifies a set of risks that are linked to the different layers of RFID. Wyld (2015) examines the adoption of RFID in commercial aviation industry and its role in baggage management. While stressing upon the benefits the author also makes a point to study the risks that come with the adoption of this Internet of Things (IoT) technology that can prove to be disruptive in cases. Mishra (2012) in an exploratory study potentially is an invasive technology to consumer security and privacy. RFID’s

are dumb devices that can listen and response irrespective of from where the request come says Rouchdi (2018) and lists down a number of risks associated with it.

The risks of using RFID in baggage management are identified into three categories which then have further sub-categories. The risks are shown in Figure 4.1.

1. Availability: Jamming, denial of service, desynchronization and covert channel attack.
2. Integrity: Tag cloning, spoofing, replay, malicious code injection and relay attack.
3. Confidentiality: Tracking, eavesdropping, disclosure, impersonation and side channel attack.

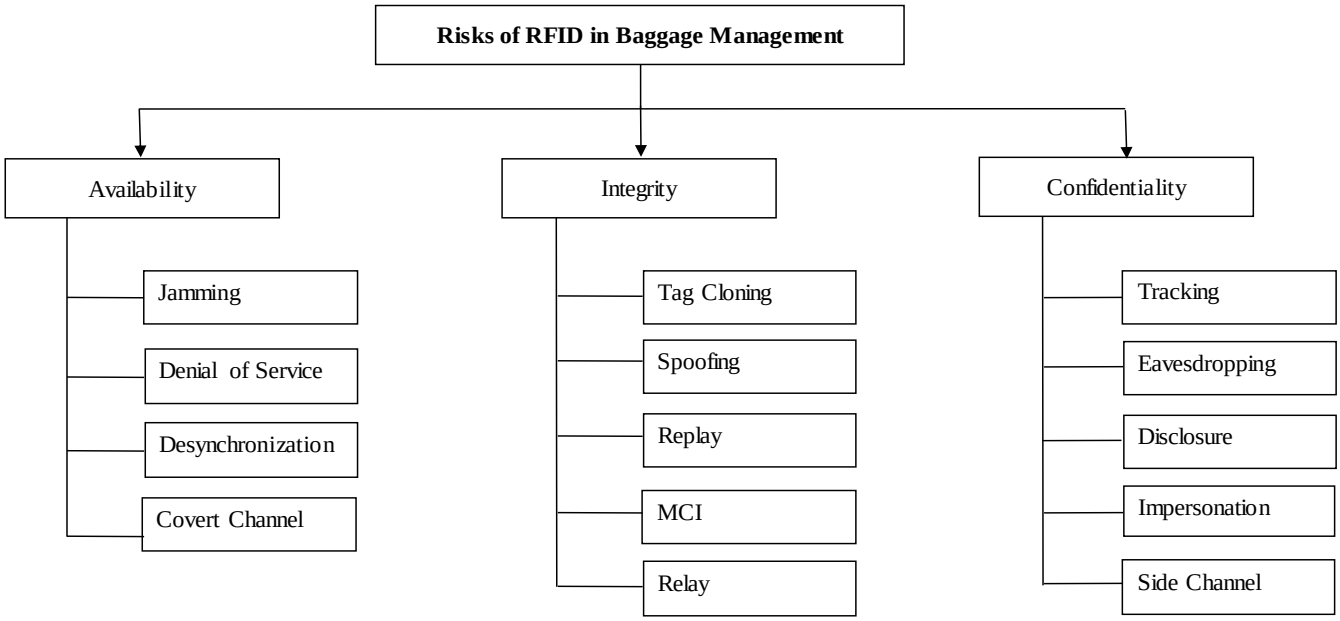

Figure 4.1 Risks of using an RFID system in baggage management

4.2 Fuzzy Analytical Hierarchy Process (FAHP) – Fuzzy Technique for Order Preference by Similarity to Ideal Solution (FTOPSIS)

After the risk identification, a questionnaire was prepared for taking input from the experts for pairwise comparison of risks and to perform the selected MCDM technique for this study i.e. FAHP- FTOPSIS. The questionnaire was distributed among 16 experts out of which eight experts responded. The sample size for FAHP-FTOPSIS was thus taken as 8. The experts were from industry and academia. The experts were the ones who were working in the RFID based airports, faculty with PHD and main research work in RFID, operations managers and owners of RFID based companies.

The scale used for pairwise comparison was a linguistic scale as proposed by Saaty (1980) in his study (Samvedi et al., 2012). The questionnaire had a set of questions targeting each category and sub-categories of risk. In the first step, pairwise comparison of risk areas is performed e.g. availability is compared to integrity on a 5 point linguistic scale. The step is completed for all the categories by the experts using the questionnaire. In the next step, all the risk factors are compared to all risk factors on the same 5 point linguistic scale as shown in Table 3.1. These crisp values are then converted in to triangular fuzzy numbers and by using triangular fuzzy arithmetic, their weights are calculated. These weights are in the end normalized to obtain the values between zero and one range. In this way, the weights of risks are calculated.

Similarly, next for FTOPSIS the first step used pairwise assessments of risks against a set of parameters or criteria. These were also computed through linguistic using the Table 4.18 to Table 4.23. These crisp numeric values obtained from the pairwise comparison are then converted into triangular fuzzy numerical values. The pairwise comparison matrix is formulated by the help of expert input. The fuzzy TOPSIS is performed next to obtain risk scores. Since single expert can give inaccurate advice hence data is collected from eight experts and group decision matrix is made. The weights of all other risk types, at each level of the hierarchy are calculated in the same method. The fuzzy weights are then averaged over the number of experts use to obtain a value. The FAHP-FTOPSIS was performed in Excel software through which results were obtained. The results for FAHP-FTOPSIS are shown in Tables 4.1-4.32.

4.2.1 Fuzzy Analytical Hierarchy Process (FAHP)

There are two levels of pairwise comparisons. First is the one in which comparison between main categories take place. Next, in level two there are three sub levels. First sub level is for the availability related risks where risks falling under this category are studied. Below given Table 4.1 and Table 4.2 show the pairwise comparison performed by expert 1. The pairwise comparison is performed by using a linguistic scale.

Table 4.1 Pairwise comparison of different risks for expert 1

Expert 1				
Availability	Jamming	Denial of service	Desynchronization	Covert channels
Jamming	1.00	5.00	5.00	5.00
Denial of service	0.20	1.00	5.00	5.00
Desynchronization	0.20	0.20	1.00	0.20
Covert channels	0.20	0.20	5.00	1.00

Using triangular fuzzy numbers, next these crisp numbers are converted into corresponding fuzzy numbers. It is to be noted here that fuzzy arithmetic have been performed by using fuzzy geometric mean analysis. The end weight is normalized to obtain values between zero and one. Moreover, a complete mathematical formulation has been given in Section 3.1.2.

Table 4.2 Fuzzified pairwise comparison matrix with fuzzy arithmetic for expert 1

Expert 1							
Availability	Jamming	Denial of service	Desynchronization	Covert channels	FGM Value	Fuzzy Weight	Weight
Jamming	1,1,3	3,5,7	3,5,7	3,5,7	2.28,3.34,5.66	1.27,0.58,1.1	0.97
Denial of service	1/7,1/5,1/3	1,1,3	3,5,7	3,5,7	1.07,1.49,2.65	0.13,0.94,0.5	0.52
Desynchronization	1/7,1/5,1/3	1/7,1/5,1/3	1,1,3	1/7,1/5,1/3	0.23,0.3,0.58	0.03,0.1,0.11	0.08
Covert channels	1/7,1/5,1/3	1/7,1/5,1/3	3,5,7	1,1,3	0.48,0.67,1.24	0.1,0.12,0.23	0.15

Similarly, the Table 4.3 and Table 4.4 are for expert 2. Expert 2 compares the risks of category one by using a linguistic scale. The pairwise comparison is to observe from an expert point of view which risk has a higher degree of preference as compared to other risks belonging to the same category. Thus, it is a way of seeing the standing of different risks which is then used for overall weight calculation.

Table 4.3 Pairwise comparison of different risks for expert 2

Expert 2				
Availability	Jamming	Denial of service	Desynchronization	Covert channels
Jamming	1.00	3.00	3.00	5.00
Denial of service	0.33	1.00	5.00	0.33
Desynchronization	0.33	0.20	1.00	0.20
Covert channels	0.20	3.00	5.00	1.00

Similarly here for the second expert all the crisp numeric values are converted into fuzzy domain. The fuzzy analysis is used to lessen the subjectivity and impreciseness from the expert opinions. In Table 4.4, fuzzy mathematics can be observed which has performed fuzzy geometric mean calculation. Final column shows the crisp weights obtained after de-fuzzifying the fuzzy weights which are then subjected to normalization.

Table 4.4 Fuzzified pairwise comparison matrix with fuzzy arithmetic for expert 2

Expert 2									
Availability	Jamming	Denial of service	Desynchronization	Covert channels	FGM Value	Fuzzy Weight			W
Jamming	1,1,3	1,3,5	1,3,5	3,5,7	1.32,2.59,4.8	0.13	0.59	1.6	0.759
Denial of service	1/5,1/3,1/1	1,1,3	3,5,7	1/5,1/3,1/1	0.59,0.86,2.1	0.06	0.17	0.7	0.319
Desynchronization	1/5,1/3,1/1	1/7,1/5,1/3	1,1,3	1/7,1/5,1/3	0.25,0.34,0.8	0.03	0.07	0.3	0.125
Covert channels	1/7,1/5,1/3	1,3,5	3,5,7	1,1,3	0.81,1.32,2.4	0.01	0.26	0.8	0.39

Likewise, Tables 4.5 and 4.6 are for expert 3. Expert 3 uses a linguistic scale to draw comparisons the risks of category one. The purpose of the pairwise comparison is to determine which risk has a higher degree of preference in comparison to other risks in the same category, as determined by an expert. Thus, it is a method of determining the position of possible threats, which would be used to represent the estimated strength.

Table 4.5 Pairwise comparison of different risks for expert 3

Expert 3				
Availability	Jamming	Denial of service	Desynchronization	Covert channels
Jamming	1.00	0.33	5.00	0.14
Denial of service	3.00	1.00	0.14	5.00
Desynchronization	0.20	7.00	1.00	7.00
Covert channels	7.00	0.20	0.14	1.00

Similar manner, all of the crisp numeric values for the third expert are transitioned to fuzzy domain. Fuzzy analysis is used to lessen the personal biases and ambiguities of expert evaluations. Table 4.8 shows fuzzy mathematics that has performed a fuzzy geometric mean calculation. The last column exhibits the crisp weights obtained after de-fuzzing the fuzzy weights, which are then normalized.

Table 4.6 Fuzzified pairwise comparison matrix with fuzzy arithmetic for expert 3

Expert 3									
Availability	Jamming	Denial of service	Desynchronization	Covert channels	FGM Value	Fuzzy Weight			W
Jamming	1,1,3	1/5,1/3,1/1	3,5,7	1/9,1/7,1/5	0.51,0.69,1.4	0.7	0.16	0.4	0.23
Denial of service	1,3,5	1,1,3	1/9,1/7,1/5	3,5,7	0.76,1.21,2.1	0.1	0.28	0.6	0.35
Desynchronization	1/7,1/5,1/3	5,7,9	1,1,3	5,7,9	1.37,1.77,3.0	0.2	0.41	0.9	0.52
Covert channels	5,7,9	1/7,1/5,1/3	1/9,1/7,1/5	1,1,3	0.53,0.67,1.2	0.1	0.15	0.3	0.19

Next is the pairwise comparison for expert number 4. The same procedure is repeated as performed in the aforementioned tables. Here when jamming is compared to other risks such as denial of service, the expert 4 has given weight 9. This implies that jamming attack on RFID based baggage management system is extremely important as compared to the denial of service attack. While denial of service is 1/9 times less important than the jamming attack.

Table 4.7 Pairwise comparison of different risks for expert 4

Expert 4				
Availability	Jamming	Denial of service	Desynchronization	Covert channels
Jamming	1.00	9.00	0.14	7.00
Denial of service	0.11	1.00	7.00	7.00
Desynchronization	7.00	0.14	1.00	7.00
Covert channels	0.14	0.14	0.14	1.00

Next for expert 4, a shift is done into fuzzy domain. The conversion is done to perform FAHP multi-criteria decision making technique. The fuzzy geometric mean value once obtained is then used for calculating fuzzy weights. Afterwards, conversion into crisp values takes place which is then followed by normalization

Table 4.8 Fuzzified pairwise comparison matrix with fuzzy arithmetic for expert 4

Expert 4							
Availability	Jamming	Denial of service	Desynchronization	Covert channels	FGM Value	Fuzzy Weight	Weight
Jamming	1,1,3	7,9,9	1/9,1/7,1/5	5,7,9	1.40,1.73,2.64	0.168	0.346
Denial of service	1/9,1/9/,1/7	1,1,3	5,7,9	5,7,9	1.30,1.53,2.43	0.156	0.306
Desynchronization	5,7,9	1/9,1/7,1/5	1,1,3	5,7,9	1.30,1.63,2.64	0.156	0.326
Covert channels	1/9,1/7,1/5	1/9,1/7,1/5	1/9,1/7,1/5	1,1,3	0.19,0.23,0.40	0.0228	0.046

Following that is the pairwise analysis for expert number 5. The same procedure as in the preceding tables is followed. When comparing denial of service to the other risks such as jamming, expert 5 has assigned weight 3. This implies that a denial of service attack on an RFID-based baggage management system is far more important than a jamming. While jamming is 1/3 the severity of the denial of service attack.

Table 4.9 Pairwise comparison of different risks for expert 5

Expert 5				
Availability	Jamming	Denial of service	Desynchronization	Covert channels
Jamming	1.00	0.33	5.00	0.14
Denial of service	3.00	1.00	0.14	7.00
Desynchronization	0.20	7.00	1.00	7.00
Covert channels	7.00	0.14	0.14	1.00

These crisp numbers are then translated into equivalent fuzzy numbers using triangular fuzzy values. It should be emphasized that fuzzy arithmetic was executed utilizing fuzzy geometric mean analysis. The final weight is adjusted to produce values ranging from zero to one. Section 3.1 also has a comprehensive mathematical formulation.

Table 4.10 Fuzzified pairwise comparison matrix with fuzzy arithmetic for expert 5

Expert 5							
Availability	Jamming	Denial of service	Desynchronization	Covert channels	FGM Value	Fuzzy Weight	Weight
Jamming	1,1,3	1/5,1/3,1/1	3,5,7	1/9,1/7,1/5	0.51,0.70,1.43	0.0663	0.161
Denial of service	1,3,5	1,1,3	1/9,1/7,1/5	5,7,9	0.86,1.32,2.28	0.1118	0.3036
Desynchronization	1/7,1/5,1/3	5,7,9	1,1,3	5,7,9	1.37,1.77,3.00	0.1781	0.4071
Covert channels	5,7,9	1/9,1/7,1/5	1/9,1/7,1/5	1,1,3	0.50,0.61,1.02	0.065	0.1403

Furthermore, Tables 4.11 and 4.12 are for expert 6. Expert 6 uses a linguistic scale to compare the risk under category one. The same procedure is followed by filling a questionnaire to understand whether a risk has a higher degree of predilection in contrast to other risks in the same category, as determined by an expert. Thus, it is a technique for determining the ranking of various hazards.

Table 4.11 Pairwise comparison of different risks for expert 6

Expert 6				
Availability	Jamming	Denial of service	Desynchronization	Covert channels
Jamming	1.00	1.00	1.00	0.33
Denial of service	1.00	1.00	1.00	1.00
Desynchronization	1.00	1.00	1.00	0.33
Covert channels	3.00	1.00	3.00	1.00

Next fuzzy conversion is undertaken and fuzzy weights are obtained for expert 6 as well. The formulation is repeated for all experts in order to obtain ranks of the risks. In Table 4.12 it can be seen that covert channels has higher weight than other risks in the same category.

Table 4.12 Fuzzified pairwise comparison matrix with fuzzy arithmetic for expert 6

Expert 6							
Availability	Jamming	Denial of service	Desynchronization	Covert channels	FGM Value	Fuzzy Weight	Weight
Jamming	1,1,3	1,1,3	1,1,3	1/5,1/3,1/1	0.67,0.76,2.28	0.0737	0.1824
Denial of service	1/3,1,1	1,1,3	1,1,3	1,1,3	0.76,1.00,2.28	0.0836	0.24
Desynchronization	1/3,1,1	1/3,1,1	1,1,3	1/5,1/3,1/1	0.39,0.76,1.31	0.0429	0.1824
Covert channels	1,3,5	1/3,1,1	1,3,5	1,1,3	0.76,1.73,2.94	0.0836	0.4152

Following that is the pairwise analysis for expert number 5. The same procedure as in the preceding tables is followed. When comparing jamming to the other risks such as desynchronization, expert 7 has assigned weight 3. This implies that a jamming attack on an RFID-based baggage management system is far more important than a desynchronization attack. While desynchronization is 1/3 the severity of the jamming attack.

Table 4.13 Pairwise comparison of different risks for expert 7

Expert 7				
Availability	Jamming	Denial of service	Desynchronization	Covert channels
Jamming	1.00	0.20	3.00	0.33
Denial of service	5.00	1.00	3.00	0.33
Desynchronization	0.33	0.33	1.00	0.33
Covert channels	3.00	3.00	3.00	1.00

Applying triangular fuzzy values, these crisp numbers are converted into fuzzy output numbers. It should also be noticed that the fuzzy arithmetic was accomplished out using fuzzy geometric mean assessment. The final weight is changed to create values ranging from zero and one.

Table 4.14 Fuzzified pairwise comparison matrix with fuzzy arithmetic for expert 7

Expert 7							
Availability	Jamming	Denial of service	Desynchronization	Covert channels	FGM Value	Fuzzy Weight	Weight
Jamming	1,1,3	1/7,1/5,1/3	1,3,5	1/5,1/3,1/1	0.41,0.67,1.50	0.041	0.134
Denial of service	3,5,7	1,1,3	1,3,5	1/5,1/3,1/1	0.88,1.50,3.20	0.088	0.384
Desynchronization	1/5,1/3,1/1	1/5,1/3,1/1	1,1,3	1/5,1/3,1/1	0.30,0.44,1.32	0.036	0.088
Covert channels	1,3,5	1,3,5	1,3,5	1,1,3	1.00,2.28,4.40	0.103	0.456

Lastly, for expert number 8, pairwise comparison is performed. The results obtained from the questionnaire are then analyzed in excel by mathematical computation of FAHP. All the pairwise comparison performed for all the eight experts are then consolidated by averaging the final weights. It is worth noticing here that FAHP is used in this study to obtain only the weights of the risks and not the ranks. The ranks would be obtained by using these weights from using FTOPSIS.

Table 4.15 Pairwise comparison of different risks for expert 8

Expert 8				
Availability	Jamming	Denial of service	Desynchronization	Covert channels
Jamming	1.00	3.00	5.00	5.00
Denial of service	0.33	1.00	5.00	5.00
Desynchronization	0.20	0.20	1.00	3.00
Covert channels	0.20	5.00	0.33	1.00

Table 4.16 Fuzzified pairwise comparison matrix with fuzzy arithmetic for expert 8

Expert 8							
Availability	Jamming	Denial of service	Desynchronization	Covert channels	FGM Value	Fuzzy Weight	Weight
Jamming	1,1,3	1,3,5	3,5,7	3,5,7	1.73,2.94,5.21	0.1903	0.4998
Denial of service	1/5,1/3,1/1	1,1,3	3,5,7	3,5,7	1.16,1.70,3.48	0.1276	0.289
Desynchronization	1/7,1/5,1/3	1/7,1/5,1/3	1,1,3	1,3,5	0.38,0.59,1.14	0.0418	0.1003
Covert channels	1/7,1/5,1/3	3,5,7	1/5,1/3,1/1	1,1,3	0.54,0.76,1.62	0.0594	0.1292

This is the evaluation for one level that is for availability. Similar computation is done for risks falling under integrity and confidentiality for all the eight experts. Table 4.17 shows the final weights of risks obtained from using FAHP. The pictorial representation of these weights is given in Figure 4.2.

Table 4.17 Weights of risks obtained from using RFID in baggage management

Jamming	Denial of service	Desynchronization	Covert Channel	-
0.10	0.09	0.06	0.06	-
Tag Cloning	Spoofing	Replay	MCI	Relay
0.10	0.10	0.07	0.09	0.08
Tracking	Eavesdropping	Disclosure	Impersonation	Side Channel
0.07	0.04	0.04	0.05	0.04

The weights as shown from Figure 4.2 show that the risks of using RFID in baggage handling have a range of weights among the other risks.

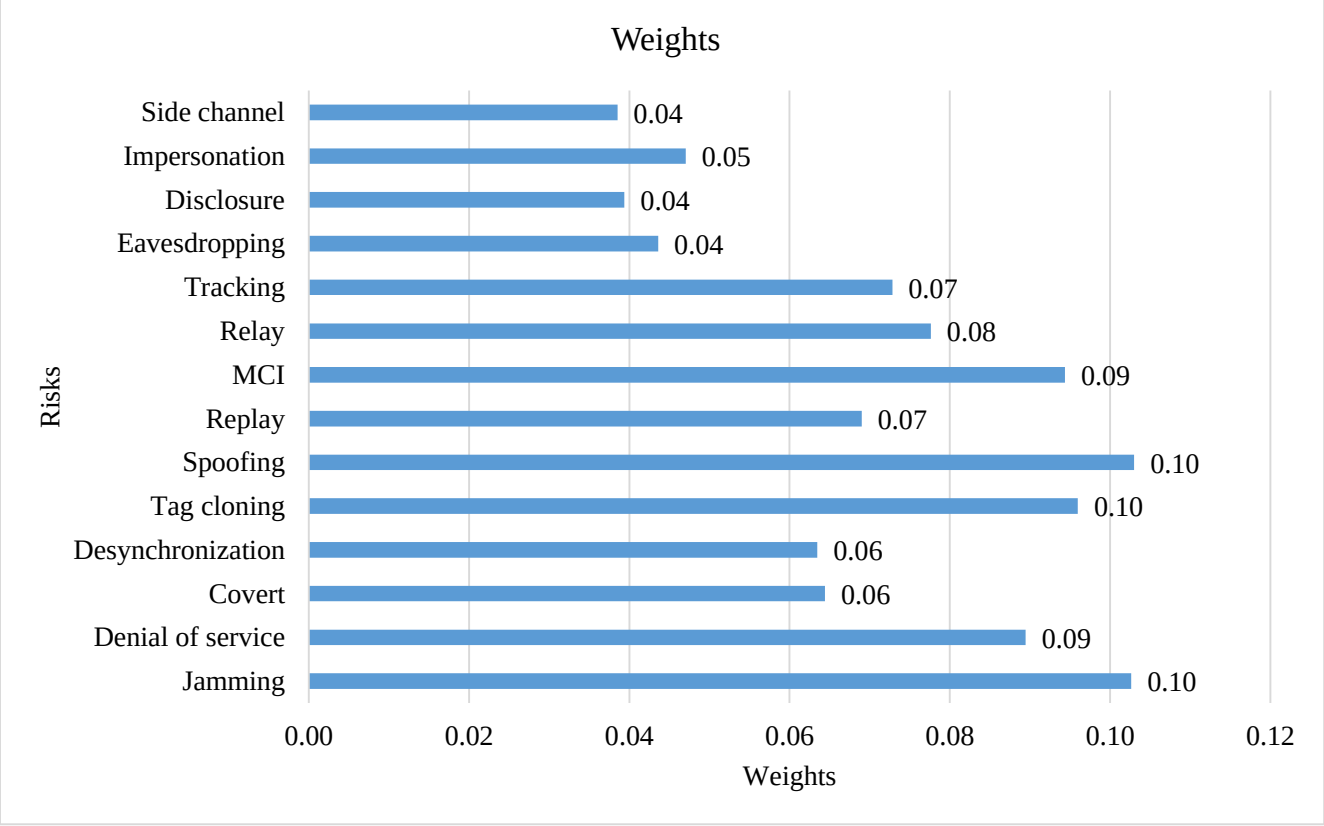

Figure 4.2 Weights associated with various risks

4.2.2 Fuzzy TOPSIS

After obtaining the weights from FAHP, all the risk factors are then compared against a set of parameters to get scores using FTOPSIS. The second step of the method assigns scores to all the risks identified from stage one of the risk assessment framework. In this step, each risk is measured against six parameters, namely type of risk, probability of occurrence, impact of risk, ease of mitigation, increase in activity duration and increase in cost. These values are obtained from the same experts that filled questionnaire for FAHP. Eight experts responded to the questionnaire in the form of linguistic expressions as shown in the tables below. Similar to the last step, a group decision matrix was made and results were averaged into a single value. The linguistic expressions used are as shown below. These linguistics scales have been used in literature for carrying out risk assessment. (Samvedi et al., 2012 & Ball et al., 2009).

Linguistic Scales of Parameters

a. Type of Risk

The type of risk parameter is divided into five different linguistic variables namely strategic, mid-strategic tactical, tactical, mid-tactical operational and operational. The strategic nature of a risk is the one that poses least vulnerability to an organization whereas the operational nature of it is the most disruptive one (F. Aqlan et al., 2015).

Table 4.18 Type of risks

Strategic	S
Mid-strategic tactical	ST
Tactical	T
Mid-technical operational	TO
Operational	O

b. Probability of Occurrence

The probability is measured mostly in terms of low, medium, high, very high and extreme levels. The higher the probability of a risk event to occur, greater would be its contribution in the weight of the risk. The linguistic scale for this is given in Table 4.19.

Table 4.19 Probability of risk

Low	L
Medium	M
High	H
Very high	VH
Extreme	E

c. Impact on Operations

The impact of a risk event is a measure of the consequences it leaves on the target. It is also termed as influence it produces after its occurrence (F. Aqlan et al., 2015). The impact of risk is also measures on levels that are used for probability i.e. low, medium, high, very high and extreme (F. Aqlan et al., 2015).

Table 4.20 Impact of risk

Low	L
Medium	M
High	H
Very high	VH
Extreme	E

d. Mitigation ease

The risk mitigation ease is the affluence with which the risk can be controlled. It is measured against linguistic variables of very easy, easy, medium, difficult and very difficult (F. Aqlan et al., 2015).

Table 4.21 Mitigation ease of risk

Very easy	VE
Easy	E
Medium	M
Difficult	D
Very Difficult	VD

e. Increase in Activity Time

Once a risk event has occurred, due to the disruption caused the usual time for performance of an operations is delayed. To measure how the occurrence of a risk event effects the time period of an activity, following levels are used which are namely: no influence, low influence, medium influence, high influence and very high influence.

Table 4.22 Increase in activity time

No influence	N
Low influence	L
Medium influence	M
High influence	H
Very high influence	VH

f. Increase in Cost

The last parameter against which the risk is measured is the 'increase in cost'. This parameter refers to the fact that when a disruptive event occurs there is an increase in cost that is incurred as a result of implementing corrective measures. Table 4.23 shows the linguistic scale used for this purpose (Aqlan et al., 2015).

Table 4.23 Increase in cost

No influence	N
Low influence	L
Medium influence	M
High influence	H
Very high influence	VH

1. Decision Matrix for FTOPSIS

The Table 4.24 shows different linguistic variables with their abbreviations marked for all the fourteen risks.

Table 4.24 A decision matrix on comparing the risks against decision parameters

No.	Risks	Type of risk	Probability	Impact	Mitigation ease	Increase in activity duration	Increase in cost
1	Jamming	O,T,MT,MS,O,O,MT,O	L,H,VH,H,H,L,VH,L	L,VH,VH,H,M,M,E,H	E,M,M,E,E,E,M,VD	M,L,M,M,H,L,VH,H	M,M,M,M,VH,L,L,H
2	Denial of service	T,MS,O,T,MS,MS,MT,T	M,M,M,M,M,M,E,L	M,H,H,VH,H,H,VH,M	E,M,M,D,M,E,VD,M	M,M,M,H,M,L,H,H	L,M,M,M,M,L,H,H
3	Desynchronization	T,T,MT,MT,T,MT,O,T	L,M,H,M,M,L,E,L	L,VH,M,H,M,L,E,L	E,E,D,M,M,VD,VE,M	L,VH,H,H,M,N,H,M	L,L,M,M,M,N,VH,M
4	Covert channels	MT,S,T,MS,T,MS,MS,S	L,L,L,L,M,M,L,L	L,L,L,L,M,M,L,L	E,E,M,E,M,M,E,VE	N,M,M,H,L,VL,M,L	N,M,M,H,L,VL,M,L
5	Tag cloning	O,S,T,O,MT,O,T,S	L,H,H,M,M,M,VH,L	L,H,VH,H,H,M,H,L	M,E,M,M,M,E,D,M	M,L,M,M,M,L,H,N	M,M,M,M,M,L,L,L
6	Spoofing	MS,T,MT,MT,T,T,MT,T	H,H,E,VH,H,M,VH,L	M,H,H,H,H,M,E,L	M,M,D,M,M,E,VD,VE	M,VH,L,M,M,L,M,N	M,M,H,M,M,L,H,N
7	Replay	MT,S,T,T,T,MS,O,S	L,L,H,H,H,M,VH,L	L,VH,M,H,H,H,VH,L	M,VE,M,M,M,D,E,VE	L,N,L,M,M,M,H,N	L,VH,M,M,M,H,VH,N
8	MCI	T,T,T,T,MS,T,O,S	L,H,H,H,M,H,E,L	L,VH,M,H,M,L,H,VH,L	E,VD,M,M,M,D,D,VE	L,VH,M,M,M,M,VH,N	L,VH,M,M,M,M,VH,N
9	Relay	MT,O,O,T,T,O,MT,S	L,L,H,H,M,L,VH,L	M,L,M,H,M,L,E,L	M,VE,M,M,M,VE,E,VE	L,M,M,M,M,N,VH,N	L,L,M,M,N,N,VH,N
10	Tracking	T,O,O,O,T,MS,T,S	H,E,H,H,H,VH,E,L	M,M,M,H,H,H,E,L	E,E,M,M,M,M,M,VE	L,L,M,H,M,M,H,L	L,H,M,H,M,M,H,L
11	Eavesdropping	T,O,T,T,T,O,MT,S	M,H,H,H,H,L,E,L	H,M,H,M,H,L,VH,L	M,VE,M,D,D,VE,VD,VE	L,M,M,H,H,N,M,N	L,N,M,M,H,N,VH,N
12	Disclosure	T,T,MT,MT,MS,MS,O,S	H,M,H,M,M,M,VH,L	H,L,M,M,M,M,VH,L	M,M,M,M,M,M,VD,VE	M,H,M,M,M,M,VH,N	L,M,M,M,M,M,VH,N
13	Impersonation	T,MT,MT,MS,T,S,O,S	H,VH,M,M,H,L,M,L	H,E,H,H,H,H,VH,L	E,VD,M,M,M,M,D,E	L,M,M,M,M,M,L,N	M,M,M,M,M,M,H,N
14	Side channel	T,S,MS,MS,MT,O,MT,S	M,M,H,H,H,M,E,L	M,M,H,H,H,M,E,L	M,M,M,M,D,D,VE	L,N,M,L,H,L,VH,N	L,VH,M,M,H,L,VH,

2. Fuzzy Group Decision Matrix

Once a group decision matrix has been obtained the subsequent step is that of obtaining a fuzzified group decision matrix. The fuzzy group decision matrix is obtained by using a fuzzy linguistic scale that is obtained against the crisp linguistic variables. The values that can be seen in the Table 4.25 are the triangular membership equivalent values for fuzzy numbers against linguistic variables. For all the five parameters the fuzzy domain values are obtained. Since the further calculations are to be carried out in fuzzy domain, the conversion from crisp decision matrix to fuzzy decision matrix is important.

Table 4.25 A fuzzy group decision matrix on comparing the risks against decision parameters

No.	Type of risk	Probability	Impact	Mitigation ease	Increase in activity duration	Increase in cost
R1	1,7.25,9	1,4,9	1,5,9	1,4.5,9	1,5.5,9	1,5.25,9
R2	1,5,9	1,3.5,9	1,5,9	1,4.75,9	1,5.5,9	1,5,9
R3	3,6,9	1,3.25,9	1,3.75,9	1,4.75,9	1,5.5,9	1,4.5,9
R4	1,3.75,9	1,1.5,5	1,1.5,5	1,3.5,7	1,3.75,9	1,3.75,9
R5	1,5.75,9	1,3.5,9	1,4,9	1,5,9	1,4.25,9	1,4.25,7
R6	1,5.5,9	1,5.25,9	1,4.5,9	1,4.75,9	1,4.5,9	1,4.75,9
R7	1,4.5,9	1,3.5,9	1,4.25,9	1,4,9	1,3.75,9	1,5.5,9
R8	1,4.75,9	1,4.25,9	1,4,9	1,5.25,9	1,5.25,9	1,5.25,9
R9	1,6.5,9	1,3,9	1,3.25,9	1,3.25,7	1,4.25,9	1,3.5,9
R10	1,5.75,9	1,6,9	1,4.25,9	1,4,7	1,4.75,9	1,5.25,9
R11	1,5.75,9	1,4.25,9	1,3.75,9	1,4.25,9	1,4.25,9	1,4,9
R12	1,5,9	1,3.75,9	1,3.25,9	1,4.75,9	1,5.25,9	1,4.75,9
R13	1,4.75,9	1,3.5,9	1,5.25,9	1,5.25,9	1,4,7	1,4.75,9
R14	1,4.5,9	1,4.25,9	1,4.25,9	1,5.25,9	1,4,9	1,6,9

3. Normalized Decision Matrix

After obtaining the group decision matrix, the next step is of normalization. The normalized group decision matrix is obtained by using the mathematical formulae shown in Section 3.2.1. The objective of carrying out normalization is to obtain values of all the risks against criteria between zero and one. The results of the carried out normalization are as shown in Table 4.26.

Table 4.26 A normalized decision matrix on comparing the risks against decision parameters

No.	Type of risk	Probability	Impact	Mitigation of risk	Increase in activity duration	Increase in cost
R1	0,0.22,1	0,0.63,1	0,0.50,1	0,0.56,1	0,0.44,1	0,0.47,1
R2	0,0.50,1	0,0.69,1	0,0.50,1	0,0.53,1	0,0.44,1	0,0.50,1
R3	0,0.38,0.75	0,0.72,1	0,0.66,1	0,0.53,1	0,0.44,1	0,0.56,1
R4	0,0.66,1	0.5,0.94,1	0.5,0.94,1	0.25,0.69,1	0,0.66,1	0,0.66,1
R5	0,0.41,1	0,0.69,1	0,0.63,1	0,0.50,1	0,0.59,1	0.25,0.59,1
R6	0,0.44,1	0,0.47,1	0,0.56,1	0,0.53,1	0,0.56,1	0,0.53,1
R7	0,0.56,1	0,0.69,1	0,0.59,1	0,0.63,1	0,0.66,1	0,0.44,1
R8	0,0.53,1	0,0.59,1	0,0.63,1	0,0.47,1	0,0.47,1	0,0.47,1
R9	0,0.31,1	0,0.75,1	0,0.72,1	0.25,0.72,1	0,0.59,1	0,0.69,1
R10	0,0.41,1	0,0.38,1	0,0.59,1	0.25,0.63,1	0,0.53,1	0,0.47,1
R11	0,0.41,1	0,0.59,1	0,0.66.1	0,0.59,1	0,0.50,1	0,0.63,1
R12	0,0.50,1	0,0.66,1	0,0.72,1	0,0.53,1	0,0.47,1	0,0.53,1
R13	0,0.53,1	0,0.69,1	0,0.47,1	0,0.47,1	0.25,0.63,1	0,0.53,1
R14	0,0.56,1	0,0.47,1	0,0.59,1	0,0.47,1	0,0.63,1	0,0.38,1

4. De-Fuzzified Decision Matrix

The normalized group decision matrix obtained from previous step is then de-fuzzified to get de-fuzzified decision matrix. It is worth noting here that the defuzzification is carried out since crisp non fuzzy numbers are required for multiplying it with weight obtained from FAHP. Then this defuzzified matrix and the weights obtained from FAHP are used to obtain a weighted group decision matrix. Next, for each risk FTOPSIS is performed to calculate final scores. Table 4.27 shows the results for defuzzified decision matrix.

Table 4.27 A defuzzified decision matrix on comparing the risks against decision parameters

No.	Type of risk	Probability	Impact	Mitigation	Increase in activity duration	Increase in cost
R1	0.41	0.54	0.50	0.52	0.48	0.49
R2	0.50	0.56	0.50	0.51	0.48	0.50
R3	0.38	0.57	0.55	0.51	0.48	0.52
R4	0.55	0.81	0.81	0.65	0.55	0.55
R5	0.47	0.56	0.54	0.50	0.53	0.61
R6	0.48	0.49	0.52	0.51	0.52	0.51
R7	0.52	0.56	0.53	0.54	0.55	0.48
R8	0.51	0.53	0.54	0.49	0.49	0.49
R9	0.44	0.58	0.57	0.66	0.53	0.56
R10	0.47	0.46	0.53	0.63	0.51	0.49
R11	0.47	0.53	0.55	0.53	0.50	0.54
R12	0.50	0.55	0.57	0.51	0.49	0.51
R13	0.51	0.56	0.49	0.49	0.63	0.51
R14	0.52	0.49	0.53	0.49	0.54	0.46

5. Weighted Group Decision Matrix

As a defuzzified decision matrix is obtained, the subsequent operations is of obtaining a weighted normalized decision matrix. This is the step where FAHP and FTOPSIS are integrated. Here, the weight obtained from FAHP is used with FTOPSIS to get a weighted decision matrix. This resultant matrix is then used for further FTOPSIS calculations. Table 4.28 shows the result for this matrix.

Table 4.28 A weighted normalized decision matrix on comparing the risks against decision parameters

No.	Type of risk	Probability	Impact	Mitigation	Increase in activity duration	Increase in cost
R1	0.04	0.06	0.05	0.05	0.05	0.05
R2	0.04	0.05	0.04	0.05	0.04	0.04
R3	0.02	0.04	0.04	0.03	0.03	0.03
R4	0.04	0.05	0.05	0.04	0.04	0.04
R5	0.05	0.05	0.05	0.05	0.05	0.06
R6	0.05	0.05	0.05	0.05	0.05	0.05
R7	0.04	0.04	0.04	0.04	0.04	0.03
R8	0.05	0.05	0.05	0.05	0.05	0.05
R9	0.03	0.05	0.04	0.05	0.04	0.04
R10	0.03	0.03	0.04	0.05	0.04	0.04
R11	0.02	0.02	0.02	0.02	0.02	0.02
R12	0.02	0.02	0.02	0.02	0.02	0.02
R13	0.02	0.03	0.02	0.02	0.03	0.02
R14	0.02	0.02	0.02	0.02	0.02	0.02

6. Positive Ideal Solution and Negative Ideal Solution (PIS and NIS)

TOPSIS is based on the concept that a chosen alternative is at the closest to the positive ideal solution and farthest from the negative ideal solution (Hwang, 1981). So, in this step the positive and negative ideal values from the weighted matrix were found.

Table 4.29 Positive and negative ideal solution

A*	0.05	0.06	0.05	0.05	0.05	0.06
A-	0.02	0.02	0.02	0.02	0.02	0.02

7. Distance Calculation

In the next step, Euclidean distances of each alternative from the positive and negative ideal solutions were calculated. The Table 4.30 and Table 4.31 show the distances calculated for each alternative from PIS and NIS respectively.

Table 4.30 Calculation of distances from PIS

No.	Type of risk	Probability	Impact	Mitigation	Increase in activity duration	Increase in cost	d*
R1	0.00	0	5.05334E-06	0	1.84967E-05	7.3562E-05	0.00
R2	2.22159E-05	2.88097E-05	7.80397E-05	5.99722E-05	0.000112856	0.00019984	0.02
R3	0.000634105	0.000354641	0.000321148	0.000420953	0.000512795	0.000643663	0.06
R4	0.000205318	1.72042E-05	3.7947E-06	0.000152048	0.000340386	0.000564158	0.04
R5	1.87899E-05	2.87836E-06	2.00641E-06	2.89516E-05	7.2699E-06	0	0.08
R6	0	2.7987E-05	0	6.97237E-07	0	4.01021E-05	0.08
R7	0.000184066	0.000285524	0.000288922	0.000252255	0.000236781	0.000663074	0.11
R8	1.74183E-06	3.30953E-05	5.26616E-06	5.08745E-05	5.36964E-05	0.000159523	0.09
R9	0.000241777	0.000109911	8.20903E-05	5.74105E-06	0.000154364	0.000229193	0.09
R10	0.000231625	0.000495861	0.00022411	5.98344E-05	0.00026984	0.000537582	0.08
R11	0.00083823	0.001066427	0.000866649	0.000915744	0.001008991	0.001237452	0.12
R12	0.00088504	0.001153888	0.000959836	0.001107635	0.001174036	0.001503792	0.12
R13	0.000648402	0.000857087	0.00093177	0.000919894	0.000580707	0.001217091	0.11
R14	0.000864934	0.001360593	0.001098595	0.001189648	0.001064799	0.001692904	0.12

Table 4.31 Calculation of distances from NIS

No.	Type of risk	Probability	Impact	Mitigation	Increase in activity duration	Increase in cost	d-
R1	0.000485872	0.001360593	0.00095463	0.001189648	0.000897808	0.00106068	0.12
R2	0.000626814	0.000993432	0.000591027	0.000715408	0.000558889	0.000729456	0.11
R3	2.08683E-05	0.000325958	0.000231784	0.000195277	0.000135007	0.000248832	0.06
R4	0.000237798	0.001071805	0.000973256	0.000491088	0.000250104	0.000302513	0.10
R5	0.000645917	0.001238311	0.001006703	0.000847427	0.000996535	0.001692904	0.05
R6	0.00088504	0.000998304	0.001098595	0.001132744	0.001174036	0.001211896	0.05
R7	0.000261875	0.00039955	0.000260737	0.000346285	0.000356323	0.000236997	0.02
R8	0.000808256	0.000969287	0.000951737	0.000748495	0.000725571	0.000813086	0.04
R9	0.000201653	0.000697084	0.000580072	0.001030103	0.00047698	0.000676301	0.03
R10	0.000211132	0.000213694	0.000330322	0.000715884	0.000318173	0.00032253	0.05
R11	6.3587E-07	1.78931E-05	1.37355E-05	1.78931E-05	6.24796E-06	3.56108E-05	0.01
R12	0	8.51058E-06	4.68219E-06	1.46442E-06	0	5.59872E-06	0.00
R13	1.83689E-05	5.79148E-05	6.86516E-06	1.73182E-05	0.000103355	3.91637E-05	0.02
R14	0.00	0	0	0	2.66653E-06	0	0.00

8. Score of risks of RFID based baggage management system

In the final step, a closeness consistency index (CCI) value is calculated for all fourteen risks. The formula used for achieving the last step is given in Section 3.2.1. From the Table 4.32 shown, it can be observed that risks have been divided into different zones depending upon their CCI values- red, yellow and green zone.

Table 4.32 Scores from FTOPSIS

Risks	d*	d-	CCI	Rank
Jamming	0.00	0.12	0.89	1
Denial of service	0.02	0.11	0.74	3
Covert Channel	0.06	0.06	0.29	10
Desynchronization	0.04	0.10	0.73	4
Tag cloning	0.08	0.05	0.45	6
Spoofing	0.08	0.05	0.72	5
Replay	0.11	0.02	0.07	14
MCI	0.09	0.04	0.36	8
Relay	0.09	0.03	0.26	11
Tracking	0.08	0.05	0.84	2
Eavesdropping	0.12	0.01	0.19	9
Disclosure	0.12	0.00	0.09	13
Impersonation	0.11	0.02	0.30	7
Side channel	0.12	0.00	0.05	12

4.3 Risk Mitigation

Risk mitigation strategies for identified red zone risks were recognized by studying literature. Risk mitigation strategies are composed of both technical and organizational measures. After reviewing the mitigation strategies from literature, a risk mitigation taxonomy was created. Subsequently, a risk mitigation matrix was filled with the algorithm given in Section 3.2.3 in Chapter 3.

4.3.1 Risk Mitigation Strategies

The risk mitigation strategies identified are shown in the Table 4.33. These are those mitigation strategies that have been mostly cited in the literature for mitigation of under consideration risks.

Table 4.33 Mitigation Strategies

Risks	Impact(ed) Area	Mitigation
Jamming	Availability	MIMO based techniques, Frequency hopping spread spectrum, Antenna phase array, Intrusion detection, Data encryption, strong user authentication (Georgia et al., 2018), Wang et al. in [195] proposed an authentication scheme to cope with RFID replay attack. Avanco et al. in [196] proposed a low-power jamming detection mechanism in RFID networks, MIMO-based jamming mitigation, spectrum spreading, and frequency hopping.
Tracking	Confidentiality	Disabling tags by crushing or puncturing (Ying Lao et al., 2015), microwave for several seconds, blocker tags, cryptographic (Fritsch et al., 2009), adopt pseudo-random function (), HASH (Peris-Lopez et al., 2006)
Denial of Service	Availability	Linux Kernel, Virtual bridges, Linux virtual server, Trusted Authentication Device and Counter (Afify et al., 2014). Cryptographic, packet-by-packet encryption scheme, PCF-02 and M-hmac2 (Malekzadeh et al., 2011), Firewall, volumetric protection from the Internet Service Provider (ISP), (Georgia et al., 2018).
Desynchronization	Availability	Anti-desynchronization RFID authentication protocol (Z., &Wong, 2010), Ultraligtweright RFID authentication protocol (many), Hash Protocol, HASP, LCAP protocol
Spoofing	Integrity	Anti-spoofing facial authentication using COTS RFID (XU, Zheng at al., 2021), LCAP (Hoon lee et al., 2005), HASH chains (Paul, 2005),

4.3.2 Risk Mitigation Taxonomy

Using the information above, interconnections between the risks and the mitigation strategies are found. The purpose of identifying relations between different mitigation strategies and risks is that in this way resource allocation would be made smart. Thereby implying that cost and time of implementing mitigation strategy would be reduced. The correlation considered in this research

are positive correlation which imply that one mitigation strategy targets more than one risk. By considering those correlation, a risk mitigation taxonomy is developed. The taxonomy is shown in Table 4.34. The tick mark in the table denote that a particular mitigation strategy can mitigate more than one risks at a time. For example, HASH protocol can target tracking, desynchronization and spoofing at the same time.

Table 4.34 Taxonomy of Correlated Risks and Mitigation Strategies

Mitigation/ Risk	Jamming	Tracking	Denial of Service	Desynchronization	Spoofing
HASH Protocol		✓		✓	✓
Blocker tag	✓	✓			
Cryptography		✓	✓		✓
Firewall			✓	✓	✓
Ultra lightweight authentication (P)	✓		✓	✓	✓
Blockchain		✓	✓		✓

4.3.3 Risk Mitigation Matrix (RMM)

For the filling of RMM, a questionnaire was developed and experts' opinion was taken. The same sample size as for the FAHP-FTOPSIS part was taken i.e. eight experts. These experts were cyber security experts both from industry and academia. The questionnaire had questions which targeted each mitigation strategy for risk and asked for evaluations against a linguistic scale for probability and occurrence of risk. The Table 4.35 shows the first stage in RMM in which risk values before and after strategy implementation are placed. The last column shows the cost associated with the mitigation strategies.

Table 4.35 RMM with values of risk before and after mitigation

Mitigation/Risk	Jamming	Tracking	Denial of service	Desynchronization	Spoofing	Risk score	Cost $
HASH Protocol	-	-	18.73	9.35	9.83	37.91	150,000 (IEEE,2012)
Blocker tag	13.125	-	13.69	-	-	13.69	900,000 (Amzaon.com)
Cryptography	-	9.29	25.13	-	13.5	47.92	1,000,000
Firewall	-	-	-	18.75	13.88	32.63	175,000 (Cisco.com)
Ultra lightweight authentication (P)	17.98	13.13	-	9.67	13.17	35.97	100,000 (Safkhani et al., 2022)
Blockchain		9.4	18	-	9.98	37.38	302,114 (Panuparb, 2022)
SUM	34	31.4	33.17	35.83	35.21	34	

Next stage of RMM has calculation of risk reduction value. The value is calculated by subtracting the risk value after mitigation strategy from risk value before mitigation strategy.

Table 4.36 RMM with R' risk reduction values

Mitigation/Risk	Jamming	Tracking	Denial of service	Desynchronization	Spoofing	Risk score	Cost $
HASH Protocol	-		12.67	26.48	25.38	64.53	150,000 (IEEE,2012)
Blocker tag	20.875		17.71	-	-	38.585	900,000 (Amzaon.com)
Cryptography	-	23.88	6.27	-	21.71	51.86	1,000,000
Firewall	-	-	-	17.08	21.33	38.41	175,000 (Cisco.com)
Ultra lightweight authentication (P)	16.02	20.04	-	26.16	22.04	84.26	100,000 (Safkhani et al., 2022)
Blockchain		23.77	13.4	-	25.23	62.4	302,114 (Panuparb, 2022)

Next in the last step, the risk mitigation matrix is normalized. The normalization takes place by dividing the risk reduction values from Table 4.36 with the original risk value in order to obtain values between zero and one range. The Table 4.37 shows the RMM with normalized values.

Table 4.37 Risk reduction values in RMM normalized

Mitigation/Risk	Jamming	Tracking	Denial of service	Desynchronization	Spoofing	Risk score	Cost $
HASH Protocol	-	-	0.40	0.74	0.72	1.86	150,000 (IEEE,2012)
Blocker tag	0.61	-	0.56	-	-	1.18	900,000 (Amzaon.com)
Cryptography	-	0.72	0.20	-	0.62	1.54	1,000,000
Firewall	-	-	-	0.48	0.61	1.08	175,000 (Cisco.com)
Ultra lightweight authentication (P)	0.47	0.60	-	0.73	0.63	2.43	100,000 (Safkhani et al., 2022)
Blockchain	-	0.72	0.43	-	0.72	1.14	302,114 (Panuparb, 2022)

4.4 Risk Reduction Optimization

After risk mitigation, the next part of the research is on risk minimization optimization. The risk is minimized by maximizing the risk reduction results obtained from RMM in the last section. In this stage, a numerical analysis is conducted for studying the optimal risk reduction and cost values under certain constraints. So, for the numerical analysis four cases are studied as shown in Table 4.38-4.41.

A. Effect of changing b2 value on mitigation strategy selection and risk reduction (b1=1.08)

In the first case, the risk reduction goal b2 is varied while the cost goal b1 is kept constant. By varying b2 the effect on mitigation strategy selection and total risk reduction is observed. It is shown in Table 4.38.

Table 4.38 Effect of changing b2 value on mitigation strategy selection and risk reduction (b1=1.08)

b2 value ($)	Mitigation Matrix	Risk reduction value after mitigation
50,000	0 0 0 0 0 0	0.00 0.00 0.00 0.00 0.00
100,000	0 0 0 0 1 0	0.47 0.60 0.00 0.73 0.63
1,000,000	0 0 1 0 0 0	0.00 0.72 0.56 0.00 0.62
1,500,000	0 0 1 1 0 1	0.00 1.44 0.63 0.00 1.95
1,575,000	0 0 1 1 1 1	0.47 2.04 0.63 1.21 2.58
2,000,000	0 1 1 0 1 0	1.08 1.32 0.76 0.73 1.35
2,545,592	1 1 1 1 0 1	1.08 1.44 1.59 1.95 2.67

The Figure 4.3 shows the graph for Table 4.40. The graph represents the behavior of mitigation matrix under sensitivity analysis.

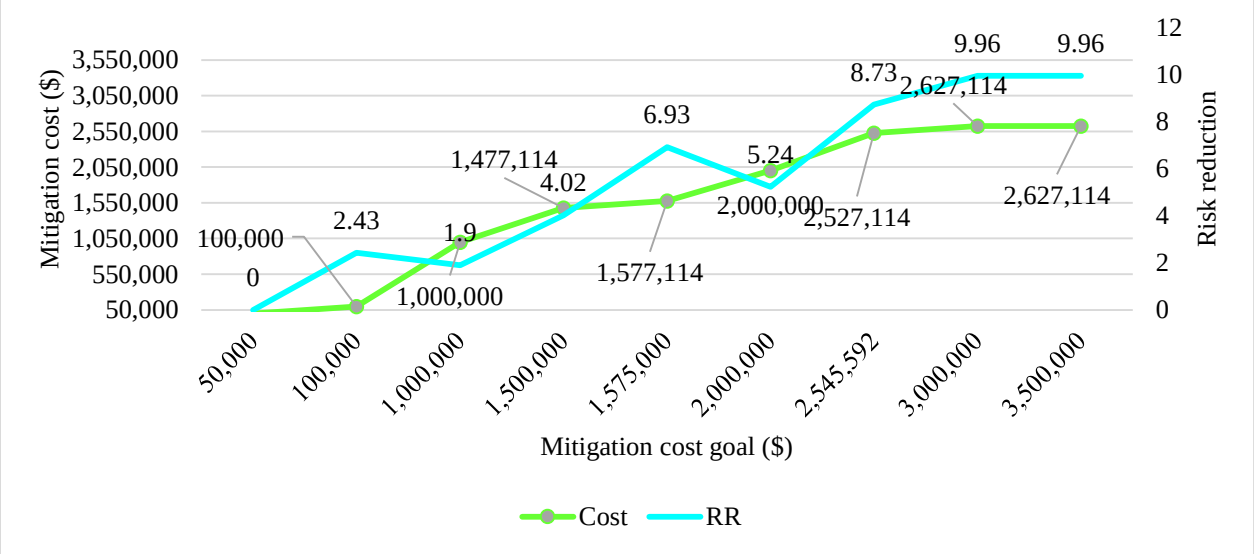

Figure 4.3 Graph of changing b2 value

B. Effect of changing b1 value on mitigation strategy selection and risk reduction (b2=$2.5 Million)

In the first case, the risk reduction goal b1 is varied while the cost goal b2 is kept constant. By varying b1 the effect on mitigation strategy selection and total risk reduction is observed. It is shown in Table 4.39.

Table 4.39 Effect of changing b1 value on mitigation strategy selection and risk reduction (b2=$ 2.5 Million)

b1 value	Mitigation Matrix	Risk reduction value after mitigation
0.0	0 0 0 0 0 0	0.00 0.00 0.00 0.00 0.00
1.0	0 0 0 1 0 0	0.00 0.00 0.00 0.48 0.61
2.0	1 0 0 1 0 0	0.47 0.60 0.40 1.47 1.35
3.0	1 1 1 0 1 1	1.08 1.32 1.59 1.47 2.69
4.0	1 0 0 1 0 1	0.00 0.72 0.83 1.22 2.05
5.0	1 0 0 1 1 1	0.47 1.32 0.83 1.95 2.68
6.0	1 1 1 0 1 1	1.08 2.04 1.59 1.47 2.09
7.0	1 0 0 1 1 1	0.47 1.32 0.83 1.95 2.68
8.0	1 0 1 1 1 1	0.47 2.04 1.03 1.95 3.30
9.0	1 0 1 1 1 1	0.47 2.04 1.03 1.95 3.30

The Figure 4.4 shows the graph for Table 4.39. The graph represents the effect on mitigation matrix and risk reduction level under sensitivity analysis.

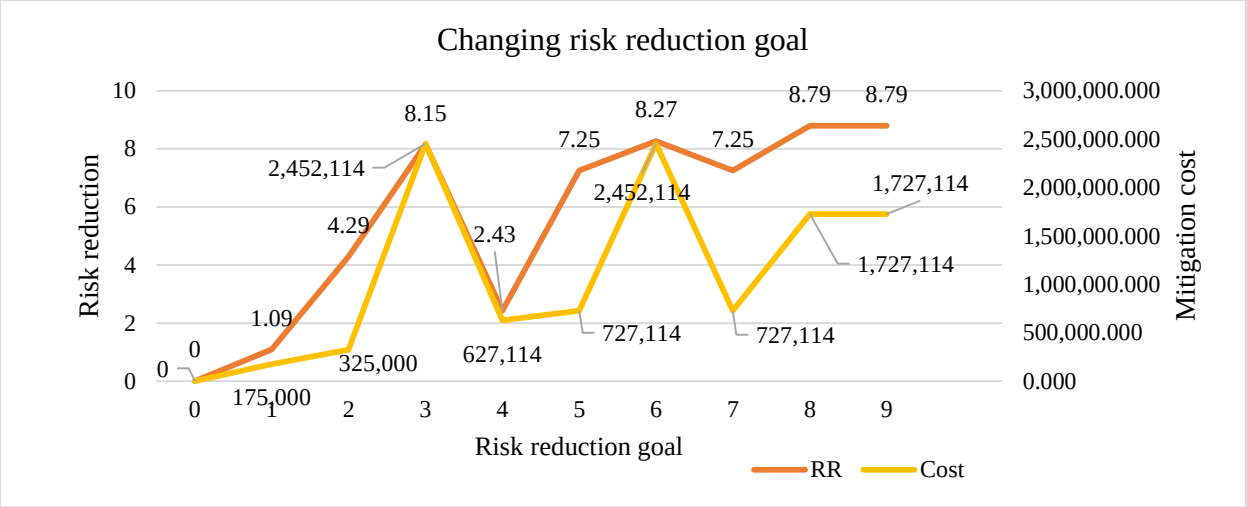

Figure 4.4 Graph of changing b1 goal value

C. Effect of increasing b1 and b2 value on mitigation strategy selection and risk reduction

In the third case of numerical analysis, both the goal values are varied in an increasing manner. The increase is stepwise for both b1 and b2 where for b1 it is one step and for b2 it is divided in to three levels. The sensitivity analysis for this case is showed in the Table 4.40.

Table 4.40 Effect of increasing b1 and b2 value on mitigation strategy selection and risk reduction

b1	b2 ($)	Mitigation Matrix	Risk reduction value after mitigation
1.0	50,000	0 0 0 0 0 0	0.00 0.00 0.00 0.00 0.00
2.0	100,000	1 0 0 0 0 0	0.00 0.00 0.40 0.74 0.72
3.0	1,000,000	0 0 1 0 0 0	0.00 0.72 0.20 0.00 0.62
4.0	1,500,000	0 1 1 0 0 0	0.61 0.72 0.76 0.00 0.62
5.0	1,575,000	0 1 1 0 0 0	0.61 0.72 0.76 0.00 0.62
6.0	2,000,000	0 1 1 0 1 0	1.08 1.32 0.76 0.73 1.38
7.0	2,545,592	0 1 1 1 1 1	1.08 2.04 1.19 1.21 2.58
8.0	3,000,000	1 1 1 1 1 1	1.08 2.04 1.59 1.95 3.30
9.0	3,500,000	1 1 1 1 1 1	1.08 2.04 1.59 1.95 3.30

The Figure 4.5 shows the graph for Table 4.40. The graph represents the effect on mitigation matrix and risk reduction level under sensitivity analysis.

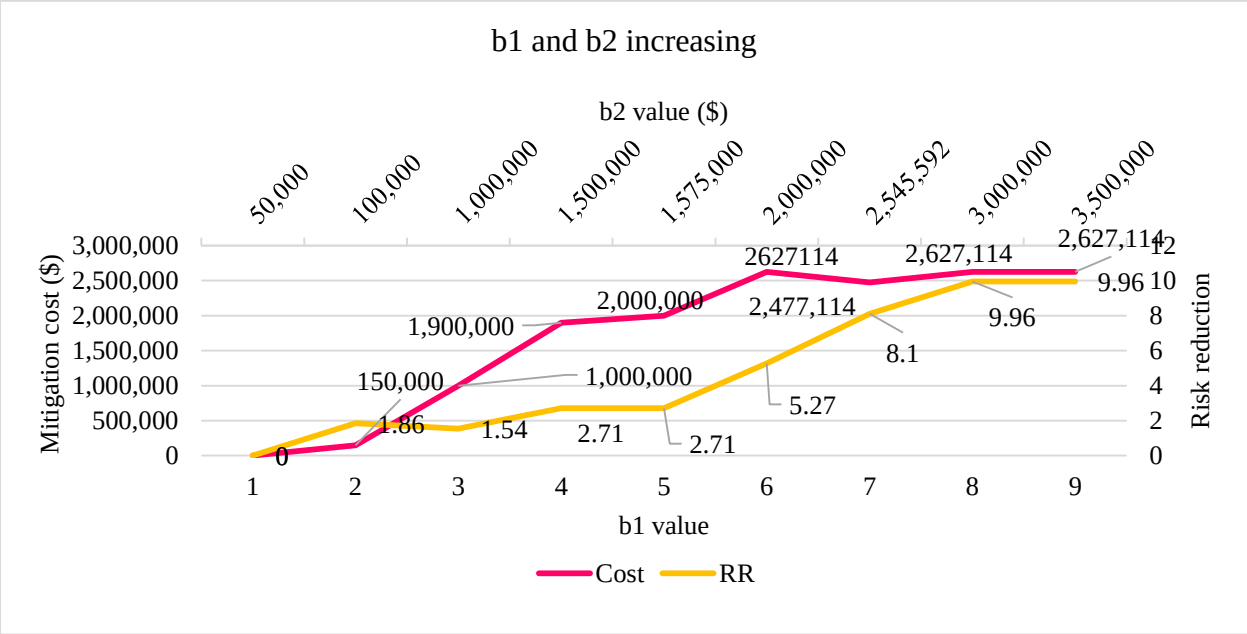

Figure 4.5 Graph of increasing b1 and b2

D. Effect of increasing b1 and decreasing b2 value on mitigation strategy selection and risk reduction

In the fourth and last case of numerical investigation, both the goal values are varied but in an alternate manner. The risk reduction goal b1 is increased while the cost goal is decreased. The sensitivity analysis for this case number four is showed in the Table 4.41. The b2 goal value is decreased in three stages to show the effect of sensitivity analysis. First stage is the one where b2 goal is well above the allocated budget, in the second stage the b2 value is equal or close to the budget value while in the last stage b2 value is well below the budget values.

The Figure 4.6 shows the graph for showing the sensitivity analysis for Table 4.41. The graph represents the effect on mitigation matrix and risk reduction level under numerical computation. The green graph line represents the risk reduction goal while the blue graph represents the cost goal.

Table 4.41 Effect of increasing b1 and decreasing b2 value on mitigation strategy selection and risk reduction

b1 value	b2 value ($)	Mitigation Matrix	Risk reduction value after mitigation
1.0	3,500,000	1 1 1 1 1 1	1.08 2.04 1.59 1.95 3.30
2.0	3,000,000	1 1 1 1 1 1	1.08 2.04 1.59 1.95 3.30
3.0	2,545,592	1 1 1 1 0 1	1.08 2.04 1.19 1.21 2.58
4.0	2,000,000	0 1 1 0 1 0	1.08 1.32 0.76 0.73 1.38
5.0	1,575,000	0 0 1 1 1 1	0.47 2.04 0.63 1.21 2.58
6.0	1,500,000	0 1 0 1 1 1	1.08 1.32 0.99 1.21 1.96
7.0	1,000,000	0 1 0 0 1 0	1.08 0.60 0.56 0.73 0.63
8.0	100,000	0 0 0 0 1 0	0.47 0.60 0.00 0.73 0.63

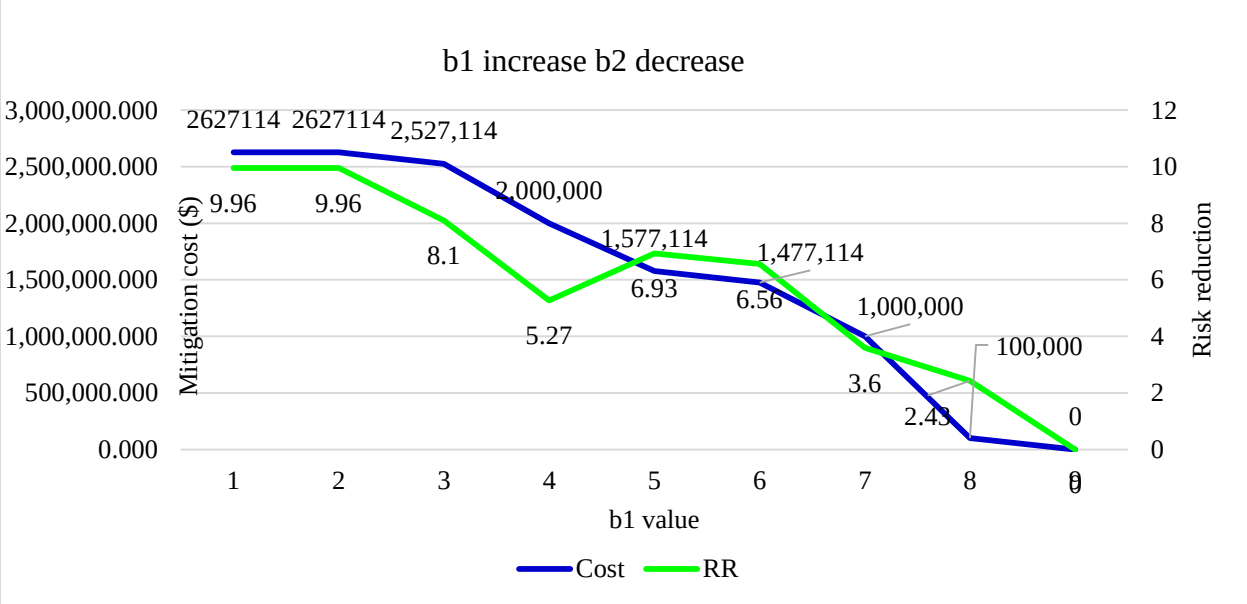

Figure 4.6 Graph of increasing b1 and decreasing b2

Chapter 5. Discussion

This chapter of the research study discusses the results obtained from chapter 4. The chapter step by step describes the results and performs a comprehensive analysis on it. The first part of the research was focused on obtaining ranks of risks associated with the use of RFID in airport logistics operation of baggage management. The risks obtained from the literature review were used in the novel risk assessment framework that has been proposed in this research. Using the framework, the top five risks are identified which are namely jamming, tracking, denial of service, desynchronization and spoofing. After obtaining these risks, risk mitigation strategies were identified and risk minimization was performed.

5.1 Scenario Analysis of Risks

The purpose of studying the risks of an RFID based baggage management is to analyze the areas which can be vulnerable as a result of introducing RFID system. This is understood by conducting a scenario analysis. Scenarios attend one of the two functions: one is risk management, where scenarios enable strategies and decisions to be tested against conceivable futures, while the other is originality and generating novel concepts (Lang, 2001). In this research, it is for the purpose of studying RFID adoption from a risk perspective.

1. Jamming
2. Tracking
3. Denial of Service
4. Desynchronization
5. Spoofing

These risks may occur as a result of several intentional / unintentional factors (Kumar et al., 2021). Each of these attacks may lead to security incidents with breach of confidentiality, integrity and availability and should be considered (Georgia et al., 2018) (Zeng et al., 2022). A detailed description of these red zone risks along with their disruptive and negative effect in terms of airport operation of baggage management is given below. It is explained in parts namely; risk, impact evaluation, cascading effect and mitigation.

1. Jamming

Jamming attack is an event in which the antagonist stops communication between a genuine tag and the reader, such that the tag node cannot interact with the reader. The adversary creates a signal alike to the reader that makes the tag undetectable with the reader (Kumar et al., 2021). IoT networks are always susceptible to attacks from malicious sources in which operators disrupt normal operation and gain access. Various kinds of wireless communication can be jammed such as wireless communications, air traffic management etc. These attacks can have impact on airport's system availability (Georgia et al., 2018) (Hamam, et al., 2009). Although wireless technologies have significantly advanced in the past decades, most wireless networks are still vulnerable to radio jamming attacks due to the openness nature of wireless channels (Zeng et al., 2022).

Zeng studied the jamming attacks that can take place where RFID systems are used. It results into passenger delays, cancelled flights, network outages which could have serious impact on smart airport, along with loss of confidence and potential financial damages (Georgia et al., 2018). To inhibit communication between reader and tag, a signal that mimics the load modulation of a tag must be transmitted, preventing the reader from receiving the tag's reflected signal. (Youssef et al., 2012). Wireless networks are more sensitive to radio jamming attacks when compared to other security risks such as eavesdropping and data falsification for the subsequent reasons: easy to launch, second jamming threats cannot be thwarted at network level. Zeng classifies jamming attacks on RFID to be constant, reactive or deceptive threats.

Impact Evaluation

1. There can be events of bulk jamming or selective jamming of RFID tags used on the baggage at airports.
2. As a result of jamming, the availability of tag to reader can be compromised. Which will result into baggage mishandling and lost baggage. Los Angeles Airport has experienced a number of cyber incidents in the past, related to malware that targeted networked baggage systems (Gopalakrishnan et al., 2013).
3. Moreover, it will also lead to missing data from the airport database.

Cascading Effects

1. Poor service availability to customers (Georgia et al., 2018).
2. Decrease operational efficiency.
3. Long passenger waiting queues (Georgia et al., 2018).
4. Longer boarding time.
5. Can impact integrity of information. For example facilitate the boarding of unknown passengers into the plane.
6. Point 5 can lead serious security risks concerning safety.
7. Terrorist facilitation for a possible attack.
8. Loss of confidence from the customers and stakeholders.

Mitigation

There are multiple strategies that can be used to mitigate the risk of jamming attack on an RFID system. Some of the most commonly used mitigation techniques that fall in security domain are intrusion detection, data encryption, strong user authentication (Georgia et al., 2018). Wang et al. in 2008 proposed an authentication scheme to cope with RFID jamming attack that is primarily a MIMO-based jamming mitigation. Other resilience measures can be spectrum spreading, and frequency hopping, to minimize equipment communication port, restrict usage of external media drives.

2. Tracking

The attacker is able to predict the proper tag ID in the tracking attack because he is already familiar with numerous tag IDs (Kumar et al., 2021). This hack aims to compromise data confidentiality (Phew, 2009). Most privacy activists are not particularly opposed to secret spying. The most difficult issue is customer tracking (Lockton et al., 2005). According to Ying Lao et al., 2015, the use of RFID technology to offer covert monitoring or surveillance of persons is a big privacy problem.

Tracking, or abuses of location privacy, is a concern strongly connected to privacy. This is feasible because tag responses are frequently predictable: in fact, tags almost always offer the same identification, allowing a third party to quickly establish a relationship between a particular tag

and its holder or owner. Even if tags strive not to divulge any important information that may be used to identify themselves or their bearer, there are several instances in which tracking is still feasible by employing a collection of tags (constellation) (Peris-Lopez et al., 2006).

Impact Evaluation

1. Tracking of passengers can create vulnerability for them and the airport.

Cascading Effects

1. Poor service availability to customers (Georgia et al., 2018).
2. Tracking the movement of high official for planning an attack.
3. Point 2 can lead to more serious security risks involving safety.
4. Terrorist facilitation.
5. Loss of confidence.
6. Knowing passengers movement and location.

Mitigation

There are multiple strategies that can be used to mitigate the risk of tracking attack on an RFID system. Some of the most commonly used mitigation techniques are disabling tags by crushing or puncturing (Ying Lao et al., 2015), microwave for several seconds, blocker tags, cryptographic (Fritsch et al., 2009), and adoption of pseudo-random function (). However, to ensure that the identity the passenger, their current location and other sensitive data, are not misused for tracking by a third party, the data safety should be guaranteed secrecy via a policy implementation.

3. Denial of Service Attack

Wireless networks are used in a variety of vital sectors, including health care facilities, hospitals, police agencies, and airports. Communication via networks is critical in these domains, and real-time connectivity as well as network availability are critical. However, denial-of-service attacks are one of the most significant risks to network availability (Malekzadeh et al., 2011).). DoS attack is an assault on the system's network, software, and hardware that renders the system

or network(s) incapable of performing the tasks intended, or renders system services inaccessible and prevents users from accessing the system. Attackers can use network flooding, redirection, code injection, and physical attack to achieve Dos success (Afify et al., 2014). Successful DoS attack can result in either access deny for the legitimate users or system's inability to distinguish legitimate users from fake ones (Georgia et al., 2018).

The enemy prevents the RFID tag in this assault. RFID devices have a limited storage capacity as well as a low-power battery. As a result, the attacker takes advantage of this and sends several packets to the communication channel. As a result, the communication channel's bandwidth will grow. These tags take a lot of electricity to receive these massive packets. The RFID tag will be withdrawn from the RFID system due to power limits (Kumar et al., 2021). (Afify et al., 2014) analyzed Denial of Service (DoS) assaults at airports, particularly in their automation systems, by detailing how attacks are launched and effective remedies. DoS problem has great impact on all devices in automation system in airports (Afify et al., 2014). Denial of Service attacks also enable attackers to disrupt information systems and networks, being able to impact on airport's system availability (Georgia et al., 2018).

Impact Evaluation

Launch of a DoS attack impacts the availability of smart airport's assets and services in the following ways:

1. This form of assault may result in actions such as aircraft cancellations, passenger delays, the inability to access cloud-based services, or even the failure of staff communication systems.
2. A similar assault occurred in June 2015 at Warsaw Chopin Airport, where about 1,400 passengers were grounded for five hours due to a DoS attack on a Polish airline. ("Hackers ground 1,400 passengers at Warsaw in attack on airline's computers", 2022).
3. The domains of safety and airport operations are prone to attacks as their operations are mainly established on the airport's network.

Cascading Effects

1. Poor service availability to customers (Georgia et al., 2018).

2. Decrease operational efficiency.
3. Long passenger waiting queues (Georgia et al., 2018).
4. Longer boarding time.
5. Can impact integrity of information. For example facilitate the boarding of unknown passengers into the plane.
6. Point 5 can lead to security risks connecting safety.
7. Terrorist facilitation.
8. Loss of confidence.

Mitigation

There are numerous approaches that can be used to mitigate the risk of denial of service attack on an RFID system. DoS attacks are one of the most harmful attacks on a cyber space system and cause the most devastation. To mitigate this attack some of the most commonly used mitigation techniques Linux Kernel, Virtual bridges, Linux virtual server, Trusted Authentication Device and Counter (Afify et al., 2014).The cyber security measure approaches include cryptography, packet-by-packet encryption scheme, PCF-02 and M-hmac2 (Malekzadeh et al., 2011), and firewall. (Georgia et al., 2018).

4. Desynchronization

The desynchronization can be caused by physical conditions like distance between tag and reader or by adversarial intervention (de Koning Gans & Garcia, 2010). This desynchronization has then impact on availability (de Koning Gans & Garcia, 2010). Garcia (2010) defines desynchronization as the case where synchronization between a tag and reader is no longer possible.

Impact Evaluation

1. The desynchronization in baggage management means passenger-baggage mismatching.
2. The correct operation of passenger management systems, such as kiosk devices or passenger check-in and boarding, may be one of the repercussions of such unavailability.

Cascading Effects

1. Decrease operational efficiency.
2. Long passenger waiting queues (Georgia et al., 2018).
3. Longer boarding time.
4. Loss of trust.
5. Loss of valuable items.

Mitigation

There are several strategies that can be used to mitigate the risk of desynchronization attack on an RFID system. Some of the most commonly used mitigation techniques Anti-desynchronization RFID authentication protocol (Z., &Wong, 2010), Ultra lightweight RFID authentication protocol, HASH protocol and firewall. The desynchronization between tag and reader can also result due to the distance between the both; for this case the mitigation strategy that can be used is to ensure that the read range is not interrupted and is suitable.

5. Spoofing

This is an impersonation attack in which the adversary inserts harmful devices into the communication channel. The attacker impersonates an authentic tag node and obtains all of the authentic tag node's rights and information. The attacker then saves these bits of information in the malicious node (Kumar et al., 2021). The key privacy problems are tag information leakage, person tracing, and tag impersonation (Hoon lee et al., 2005). Table 5.1 shows the overall scenario analysis combined for these risks.

Impact Evaluation:

1. Incorrect boarding.
2. Information can be leaked.

Cascading Effects:

1. Loss of trust.

2. Loss of valuable items and information.

Mitigation

There are multiple strategies that can be used to mitigate the risk of spoofing attack on an RFID system. Some of the most commonly used mitigation techniques include anti-spoofing authentication using COTS RFID (XU, Zheng at al., 2021), LCAP (Hoon lee et al., 2005), HASH chains (Paul, 2005), cryptography, firewall, and blockchain. These and many other cyber security related mitigation strategies can help prevent the occurrence of spoofing attacks where RFID systems are in use.

Table 5.1 An explanation of detail, launch and cascading effect of RFID risks at baggage management

Risk	Detail	Launch	Cascading effect
Jamming	• Jamming attack is an event when the adversary stops communication between a genuine tag and the reader • IoT networks are always susceptible to attacks from malicious sources in which operators disrupt normal operation and gain access. • Wireless networks are still vulnerable to radio jamming attacks due to the openness nature of wireless channels (Zeng et al., 2022).	• The adversary creates a signal equivalent to the reader that makes the tag non-communicable with the reader (Kumar et al., 2021). • In order to block the communication between reader and tag, there is a need to transmit a signal which mimics the load modulation of a tag, thus preventing the reader from receiving the tag's reflected signal (Youssef et al., 2012).	• These attacks can have impact on airport's system availability (Georgia et al., 2018) • It results into passenger delays, cancelled flights, which could have serious impact on smart airport, along with loss of confidence and potential financial damages (Georgia et al., 2018). • Poor service availability to customers (Georgia et al., 2018). • Long passenger waiting queues (Georgia et al., 2018). • Can impact integrity of information.
Tracking	• These are privacy attacks in which the attacker can trace tags through rogue readers (Burmester, 2015). • This hack aims to compromise data confidentiality (Phew, 2009).	• The use of RFID technology to offer covert monitoring or surveillance of persons is a big privacy problem (Ying Lao et al., 2015). • Tracking is a threat directed to an individual.	• Tracking of passengers can create vulnerability for them and the airport. • Poor service availability to customers (Georgia et al., 2018). • Tracking the movement of high official for planning an attack. • Terrorist facilitation. • Loss of confidence. • Knowing passengers movement and location.
Denial of service	• Unauthorized tag disabling (Malekzadeh et al., 2011); • Temporary or permanently incapacitated • Enables to disrupt information systems and networks, being able to	• RFID devices have a limited storage capacity as well as a low-power battery. As a result, the attacker takes advantage of this and sends several packets to the communication channel.	• Passenger delays • Inability to access cloud-based services • Poor service availability to customers (Georgia et al., 2018). • Decrease operational efficiency.

	impact on airport's system availability (Georgia et al., 2018).	• As a result, the communication channel's bandwidth will grow. These tags take a lot of electricity to receive these massive packets. The RFID tag will be withdrawn from the RFID system due to power limits (Kumar et al., 2021).	• Long passenger waiting queues (Georgia et al., 2018). • Can impact integrity of information. For example facilitate the boarding of unknown passengers into the plane.
Desynchronization	• The case where synchronization between a tag and reader is no longer possible. • Impact on availability (de Koning Gans & Garcia, 2010).	• The correct operation of passenger management systems, such as kiosk devices or passenger check-in and boarding, may be one of the repercussions of such unavailability.	• The desynchronization in baggage management means passenger-baggage mismatching. • Decrease in operational efficiency. • Long passenger waiting queues (Georgia et al., 2018). • Longer boarding time. • Loss of trust on part of customers. • Loss of valuable items.
Spoofing	• This is a kind of impersonation attack where harmful devices are introduced in the communication channel. • A masquerade by a forged tag as a valid tag.	• The attack impersonates the legitimate tag and obtains all authentic information to be used by other fake tags.	• Loss of trust by passengers. • Incorrect boarding. • Leakage of information (Hoon et al., 2005).

5.2 Optimization of Risk Reduction

Next part of the research includes the optimization of risk reduction. The optimization models for risk reduction are solved by using goal programming through computer software. A numerical analysis is performed for the multi-objective optimization model in which the multi-objective risk reduction optimization model is tested with four different cases to study the optimal risk reduction and mitigation cost under different cost and risk constraints. Table 4.38 shows how changing the b2 value by keeping b1 value constant will affect the selection of mitigation strategies and risk reduction. Similarly Table 4.39 shows how changing the b1 value while keeping the b2 value constant will affect selection of optimal mitigation strategies. In Table 4.40, both the goal values (b1 and b2) are changed simultaneously (increasing way) and the effect on selection of optimal strategies under risk reduction and cost constraints are observed. In Table 4.41, the b1 value is increased and b2 value is decreased and the effect on selection of optimal strategies under risk reduction and cost constraints are observed.

For this numerical analysis, a case study of McCarran International Airport, Las Vegas is taken. McCarran International Airport, Las Vegas is one of the first airport to start large-scale baggage tagging using RFID (Santonino et al., 2018). In Table 4.39, the b1 (risk reduction) value is changed with step size of 1 and the b2 value (cost) is kept constant. The b2 value here taken is the budget that the McCarran International Airport, Las Vegas has kept for implementing cyber security measures at its airport which is $2.5 million which is 12% of the IT budget which is 3.67% of its revenue (SITA Air Transport Security Insights, 2018) ("Financial Statements at Clark County Department of Aviation", 2018). It can be observed from the table that changing the b1 value changes the mitigation strategies that can be selected and hence the risk reduction value after mitigation varies. For example, in Table 4.39 row 4, using b1=4, the best combination of mitigation strategies satisfying the constraints are 1, 4 and 6 (HASH, LCAP/HCAP, and Blockchain). After using these mitigation strategies, all the five risks can be reduced to the corresponding values in third column.

Similarly, in Table 4.38, the b1 value is kept constant and the b2 value (cost/budget) is increased with covering three cases as was used by (Aqlan & Lam, 2015) in their research. The b1 value can be fixated at any desired value depending on the company's goal. In this research, b1 is kept 1.08 which is the smallest risk reduction gained after using a mitigation strategy. It can be

observed from the table that changing the b1 value changes the mitigation strategies that can be selected and hence the risk reduction value after mitigation varies. Further, in Table 4.40, the values of b1 and b2 are changed simultaneously in an increasing manner. Changing these value affects the selection of mitigation strategies and risk reductions. And lastly, in Table 4.41, the values of b1 is increased while the value of b2 is decreased and the effect of this is observed in the selection of mitigation strategies and risk reductions.

Next is the graphical representation of all these four cases. It can be seen from Figure 4.3 that when the mitigation cost objective is set lower than the feasible value, the overall mitigation cost equals the minimal feasible value. Furthermore, if the mitigation cost objective is set at a higher value than the available budget ($2.5 million), the overall mitigation cost will be very near to the budget allocation. In Figure 4.4, it can be observed that while the overall mitigation cost for all mentioned vales is almost equal to the goal mitigation cost, the total risk reduction is closer to the predetermined target.

What can be observed from the above analysis is that risk reduction and cost are two opposing objectives. The decision-maker or organization implementing the strategy has to decide what is more preferable to them. While taking the case for McCarran International Airport, Las Vegas, it can be seen that with a budget of $2.5M, all the mitigation strategies can be implemented for securing RFID baggage operations except strategy 5. Risk mitigation outcomes can be included into tactical, operational, and strategic planning by the airports implementing this IoT technology into its baggage management operation.

5.3 Comparative Analysis Study

5.3.1 FAHP-FTOPSIS vs. AHP-TOPSIS

Despite the vast number of MCDM approaches that are available, no one method is deemed best for all sorts of decision-making situations. This creates the dilemma that selecting an acceptable technique for a particular problem result in an MCDM problem (Mulliner et al., 2016). A variety of practical applications of comparison analyses of various MCDM approaches are presented in the literature (Mulliner et al., 2016). In this research, a hybrid MCDM method is used for ranking risks where Fuzzy Topsis is used in combination with the Fuzzy AHP method. The AHP-TOPSIS method has been used in the literature for assigning ranks to the alternatives prior to the discovery of fuzzy sets. Fuzzy domain is used in order to lessen the subjectivity and impreciseness attached to the opinions of decision makers. Howsoever, the argument remains that how fuzzy based MCDM technique performs better than the conventional method. The argument is justified by conducting a comparative analysis of the research study with both the fuzzy and non-fuzzy based MCDM techniques.

To compare these two said MCDM techniques, a standard way of comparison must be used. In this comparative study, a Kendall tau rank correlation coefficient is used. Kendall's Tau rank correlation coefficient can be used to measure the strength of the association between two variables or two MCDM approaches in a comparison. (Karami 2011; Yuniwati, 2016; Bahri, 2022). The higher the value of Kendall's Tau coefficient, the better and more consistent is that MCDM technique (Bahri, 2022). The Tau coefficient takes into account the ranks of the two MCDM techniques and checks for a consistency among the ranks. Using it then discordant and concordant pair are generated. When data is sorted by quantity, Kendall rank correlation is used to look for trends. Kendall's correlation coefficient uses pairs of data to determine the degree of link based on the pattern of concordance and discordance between the pairings, whereas other types of correlation coefficients rely on observations as the basis of the correlation.

A simple AHP-TOPSIS analysis was conducted with the data set used in the research study for risk prioritization using FAHP-FTOPSIS. In the TOPSIS part of AHP-TOPSIS, a group decision making approach is used where the number of experts is greater than one. The Table 5.1 shows the final closeness consistency index (CCI) values and scores obtained from both the

MCDM techniques used. The most important risks are shown by the degree of vulnerability through a radar diagram in Figure 5.1 and Figure 5.2. To manage the risks in a supply chain, firms should do a risk analysis for identifying the most vulnerable risks (Junaid et al., 2020). Similarly, for identifying the most important risks of RFID in baggage management, a risk analysis was conducted using two MCDM techniques. The higher the CCI the higher the harmfulness of the risk (Junaid et al., 2020).

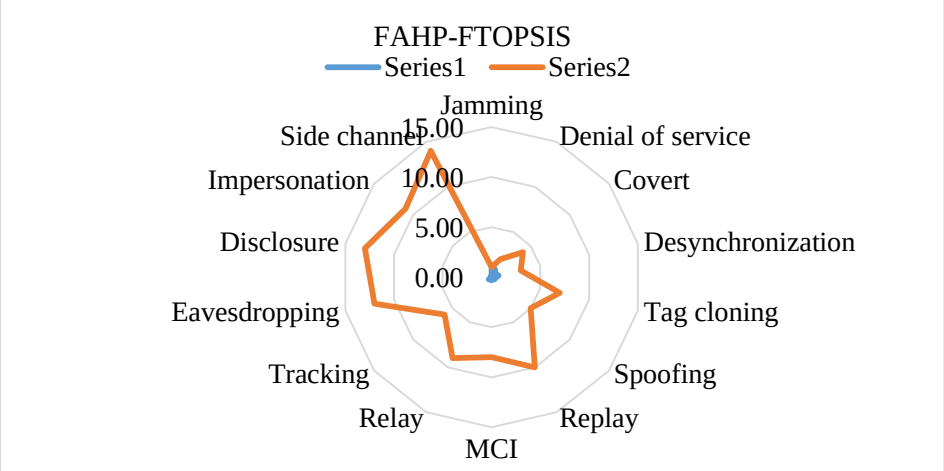

Figure 5.1 Radar diagram for ranking of risks through FAHP-FTOPSIS

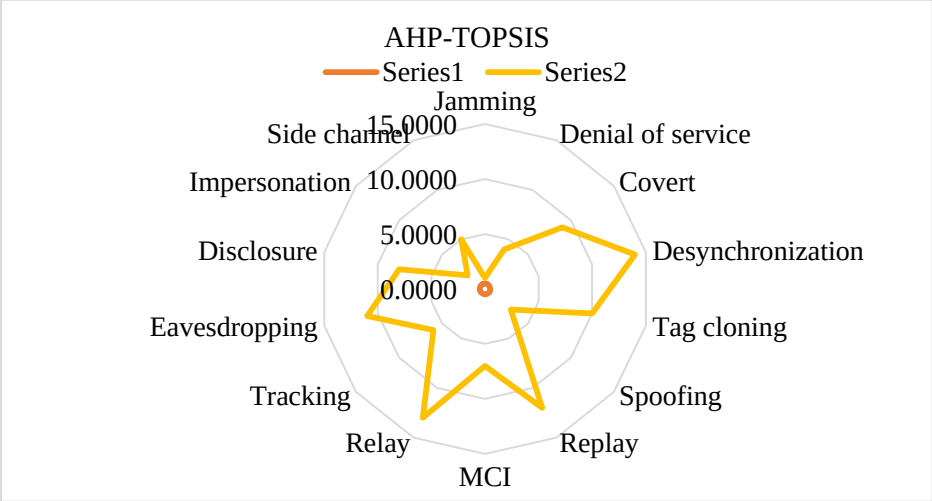

Figure 5.2 Radar diagram for ranking of risks through AHP-TOPSIS

In the Table 5.2, the different values of CCI for both the multicriteria decision making techniques have been shown. Since the CCI values for both the methods vary the end ranks obtained for the risks are different. The table shows that none of the ranks is same for both the techniques. The Table 5.2 shows the respective CCI values and ranks obtained from using

respective MCDM techniques. The red zone risks which must be mitigated first are different for both cases.

Table 5.2 Comparative analysis of MCDM techniques with scores of risks

No.	Risks	FAHP-FTOPSIS	Rank	AHP- TOPSIS	Rank
R1	Jamming	0.89	1	0.4999	1
R2	Denial of service	0.74	3	0.4978	4
R3	Covert Channel	0.29	9	0.4914	9
R4	Desynchronization	0.73	4	0.4660	14
R5	Tag cloning	0.45	6	0.4910	10
R6	Spoofing	0.72	5	0.4983	3
R7	Replay	0.07	14	0.4874	12
R8	MCI	0.36	8	0.4973	7
R9	Relay	0.26	11	0.4792	13
R10	Tracking	0.84	2	0.4976	6
R11	Eavesdropping	0.19	10	0.4899	11
R12	Disclosure	0.09	13	0.4926	8
R13	Impersonation	0.30	7	0.4984	2
R14	Side channel	0.05	12	0.4977	5

The red risks obtained for both MCDM techniques are shown in Table 5.3 and Table 5.4. Depending upon the percentage contribution of a risk on the overall risks, three different categories are identified. The most important category is assigned the red color to show the significance of working on it. It is to focus the resource implementation for mitigating these red zone risks. The Table 5.3 and Table 5.4 show the red zone risks obtained for both the MCDM techniques.

Table 5.3 Ranks of red zone risks from FAHP-FTOPSIS

No.	Risks	FAHP- FTOPSIS
R1	Jamming	1
R10	Tracking	2
R2	Denial of Service	3
R4	Desynchronization	4
R6	Spoofing	5

It can be noted that the red category risks (most important) for both the FAHP-FTOPSIS and AHP-TOPSIS are different. Which implies that the subjective nature of MCDM varies the risks to be targeted.

Table 5.4 Ranks of red zone risks from AHP-TOPSIS

No.	Risks	AHP- TOPSIS
R1	Jamming	1
R13	Impersonation	2
R6	Spoofing	3
R2	Denial of Service	4
R14	Side Channel	5

The graphical representation of the ranks obtained from two MCDM are as shown in Figure 5.3. The graph shows the final scores for risks obtained which can be then used for further computation in the research study.

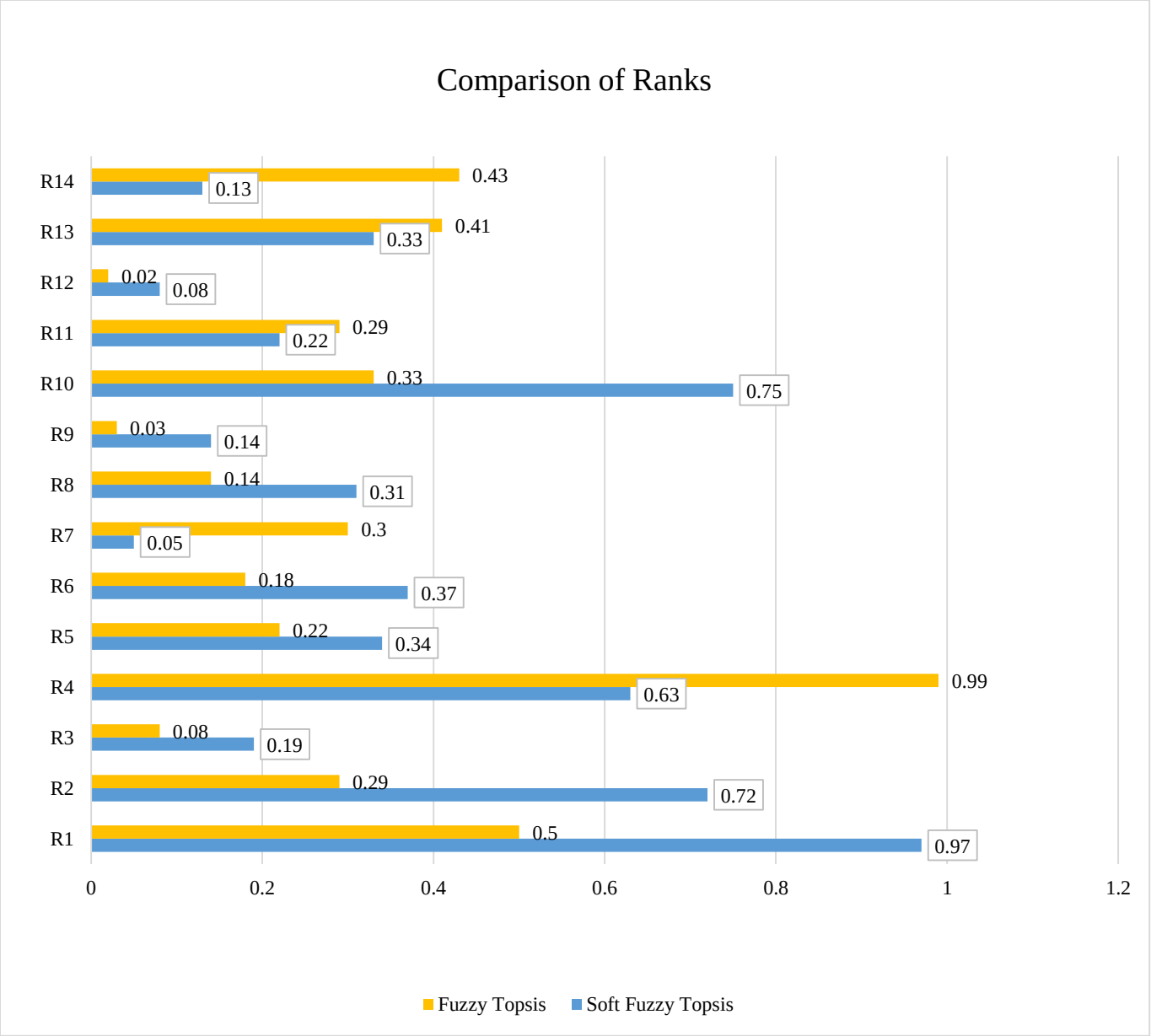

Figure 5.3 Comparison of MCDM techniques

MCDM issues are often so complicated that no one can anticipate an ideal solution; as a result, techniques aim for a compromise solution (bargain computing) rather than an optimal one from mathematical computations (Zeleny, 1974). It is usually advised to use a strategy based on the features of the problem, such as the number of choices and criteria, the workload required, the possibility to add real-world components, and so on. Using the simplest approaches appears

sensible; yet, it is not advised since these approaches are unlikely to be capable of accurately representing a scenario (Munier et al., 2019).

Once, risk comparison next step is to validate the accuracy of the results of this study. To evaluate the rankings obtained from using the two MCDM techniques, this research uses Kendall Tau rank correlation coefficient. The Kendall Tau rank correlation coefficient is widely used in the literature to compare two variables or Multicriteria decision making techniques. In one study, Karami (2011) suggests a comparison of two methods of MCDM can use Kendall's Tau b correlation to determine the strength of the relationship between two variables or two methods of MCDM. The formula used to calculate the correlation Kendall's Tau b is given in eq. 5.31.

$$b = \frac{P-Q}{P+Q} \tag{5.31}$$

In eq. 5.31 the P and Q are the number of concordant pairs and the number of discordant pairs respectively. Using this method the following graph in Figure 5.4 was obtained. The computation of coefficient is done by Table 5.5. The higher the value of Kendall Tau rank correlation coefficient means that the closer the two MCDM methods are. Since the value for coefficient is 0.29 meaning that there is a low positive correlation, hence the FAHP-FTOPSIS methodology is better and more consistent. Result was confirmed by SPSS as in Table 5.6.

Table 5.5 Comparison of ranks AHP-TOPSIS vs. FAHP-FTOPSIS using correlation coefficient

Risk	Reference	Order	FAHP-FTOPSIS	AHP-TOPSIS	Concordant	Discordant
R1	1	1	R1	1	13	0
R2	2	2	R10	6	8	4
R3	4	3	R2	4	9	2
R4	3	4	R4	14	0	10
R5	7	5	R6	3	8	1
R6	5	6	R5	10	5	5
R7	10	7	R8	7	5	2
R8	8	8	R13	2	6	0
R9	9	9	R3	9	6	2
R10	6	10	R9	13	0	4

Table 5.5 (continued).

R11	12	11	R11	11	1	2
R12	13	12	R12	8	1	1
R13	11	13	R7	12	0	1
R14	14	14	R14	5	0	0
					62	34
				P+Q/P-Q		0.29

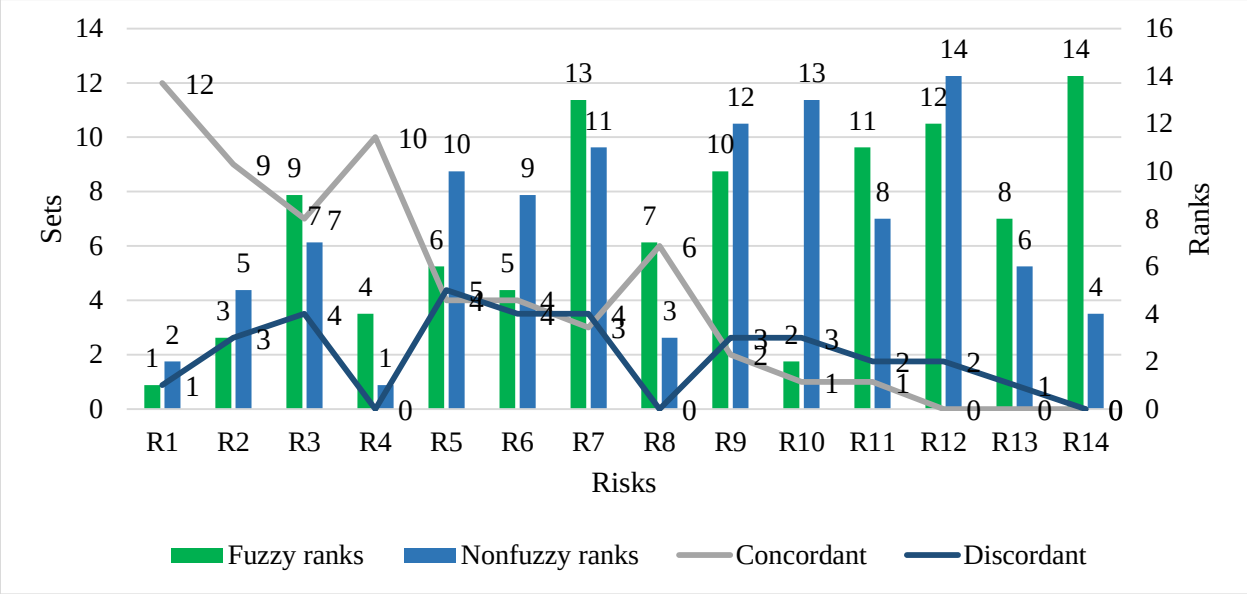

Figure 5.4 Kendall Tau coefficient values for AHP-TOPSIS and FAHP-FTOPSIS

Table 5.6 Kendall Tau b correlation for comparative analysis

			FAHPFTOPSIS	AHPTOPSIS
Kendall's Tau_b	FAHPFTOPSIS	Correlation Coefficient	1.000	.29
		N	14	14
	AHPTOPSIS	Correlation Coefficient	.29	1.000
		N	14	14

The better methodology is now selected on basis of discrimination of scores. This is also a good indication since the greater the discrimination the better, because low discrimination is related with very close values between alternatives and even ties, which makes it difficult for the DM to make a selection (Munier et al., 2019). From Figure 5.5 it can be seen that FAHP-FTOPSIS has higher discrimination between CCI values and hence is a better MCDM to be used for this study.

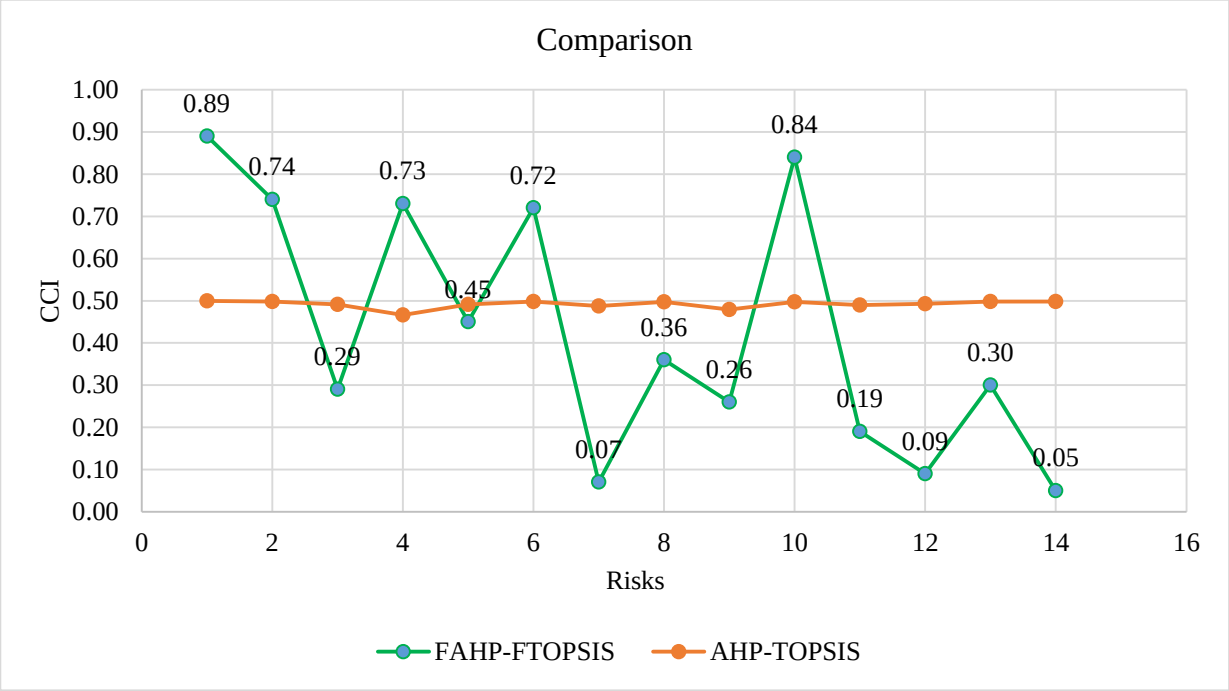

Figure 5.5 CCI values for AHP-TOPSIS and FAHP-FTOPSIS

5.4 Data Validation

To validate that the FAHP- FTOPSIS used in this research yields better results than the AHP-TOPSIS approach, the research takes the cases used in the literature for prioritization of alternatives such as risk assessment or selection of a site etc. Two experimental studies from literature are taken for the validating the use of Fuzzy based MCDM technique used in this paper. The first case study is ‘risk analysis of textile industry using AHP-TOPSIS by Bathrinath et al., (2020). The goal of this article is to identify and investigate the potential hazards that lead to accidents and crucial alternatives in the garment industries. This work was completed at one of southern India's premier textile industries. The second case is for quantifying risks in a supply chain through integration of fuzzy AHP and fuzzy TOPSIS by T.S. Chan et al., 2012. This study

aims towards quantifying the risks in a supply chain and then consolidating the values into a comprehensive risk index by using FAHP-FTOPSIS.

Case 1: Risk Analysis of Textile Industry-Bathrinath et al (2020)

For the first case of data validation, both non fuzzy based and fuzzy based AHP-TOPSIS were performed. The weights obtained by using these multicriteria decision making techniques is shown in Figure 5.6.

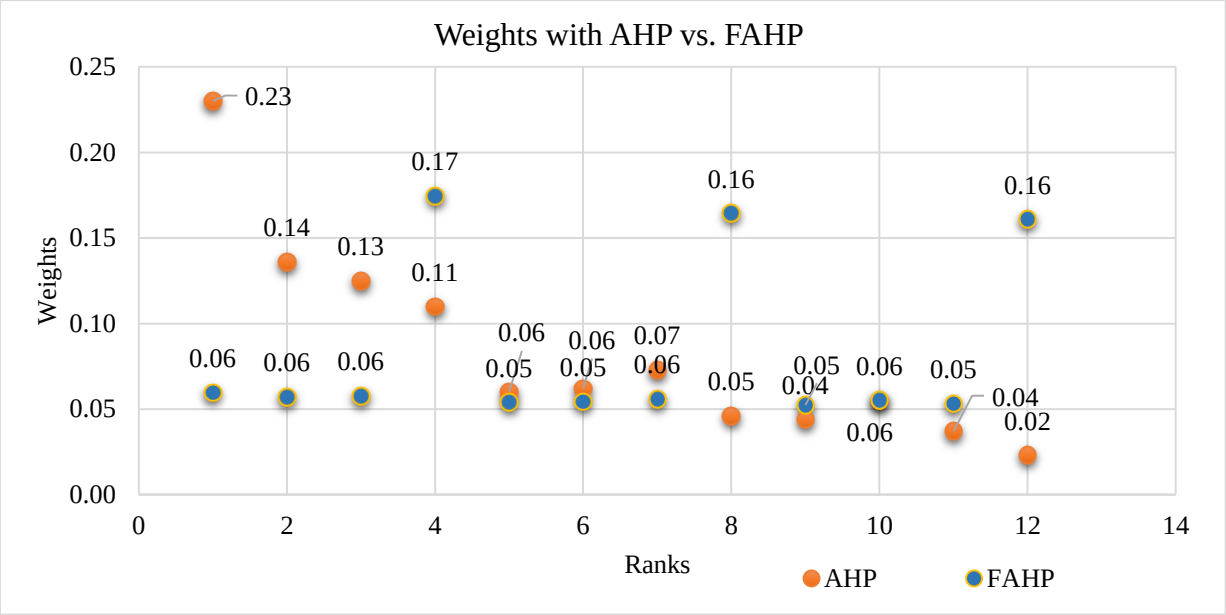

Figure 5.6 Rank spread for AHP and FAHP for case 1

The Figure 5.7 shows the scores and ranks obtained for risks by using TOPSIS and FTOPSIS. The numerical computation performed for the purpose of checking the results is shown

Table 5.7 Kendall Tau comparison for ranks from AHP-TOPSIS vs. FAHP-FTOPSIS

Ref	FAHP-FTOPSIS	Concordant	Discordant	AHP-TOPSIS	Concordant	Discordant
R1	1	3	0	1	3	0
R4	3	1	1	3	1	1
R2	4	0	1	2	1	0
R3	2	0	0	4	0	0
	Sum	4	2		5	1
		P-Q/P+Q				0.67

in Table 5.7. The Kendall tau rank correlation coefficient for FAHP-FTOPSIS is higher than the one obtained for non-fuzzy MCDM approach. Hence, we conclude that the former method is more consistent.

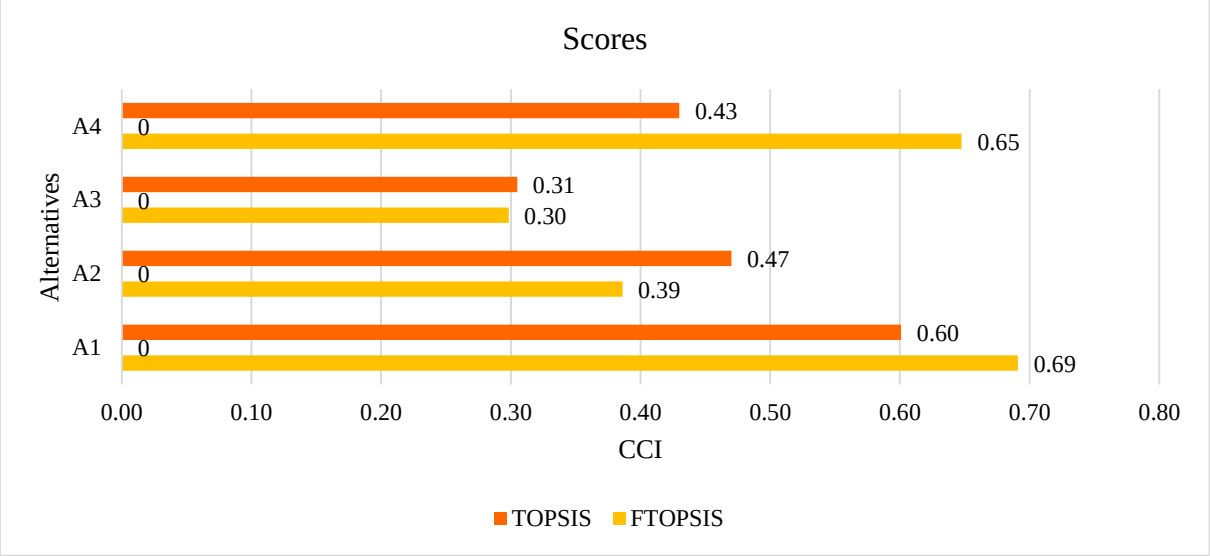

Figure 5.7 Scores obtained for TOPSIS and FTOPSIS

Moreover, a point wise evaluation of the results for correlation coefficient is shown in the Figure 5.8 through a graph. The columns here represent the MCDM methods and the lines are representing the concordant and discordant pairs.

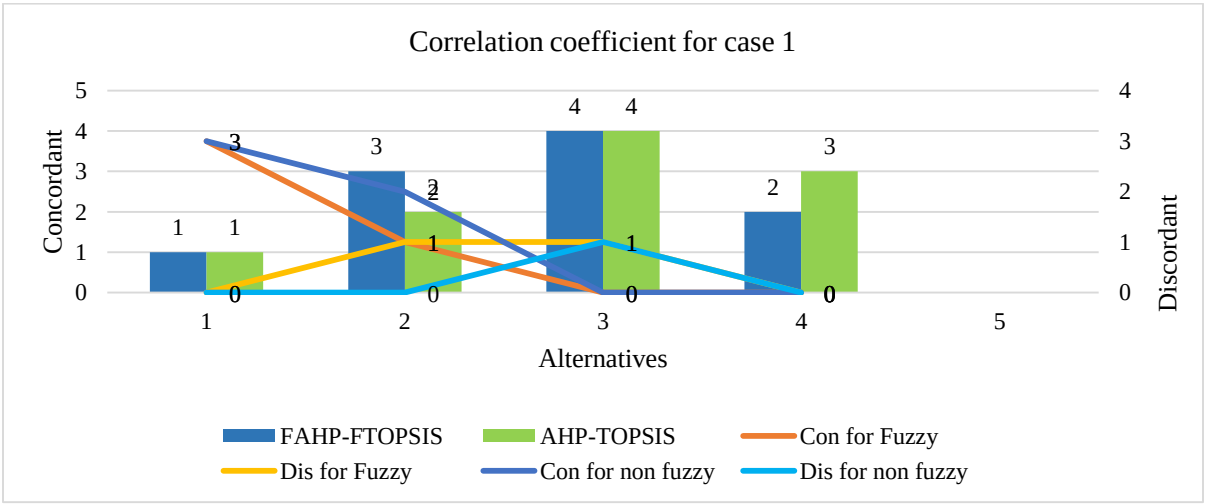

Figure 5.8 Scores obtained for TOPSIS and FTOPSIS

Table 5.8 Kendall Tau b correlation coefficient for case 1 validation

			FAHPFTOPSIS	AHPTOPSIS
Kendall's Tau_b	FAHPFTOPSIS	Correlation Coefficient	1.000	.667
		N	4	4
	AHPTOPSIS	Correlation Coefficient	.667	1.000
		N	4	4

Since the coefficient value is moderate to high, it can be said that either of the MCDM can be used for ranking in this case.

Case 2: Quantifying Risks in a Supply Chain- T.S. Chan et al (2012)

The second case taken from the literature is that of quantification of risks in a supply chain. A supply chain is always vulnerable to risks- thus for avoiding disruption top risks must be identified and mitigated. The case was studied with both AHP-TOPSIS and FAHP-FTOPSIS to see and analyze the ranks obtained. The Figure 5.9 shows the graph with weights obtained by using the MCDM methods.

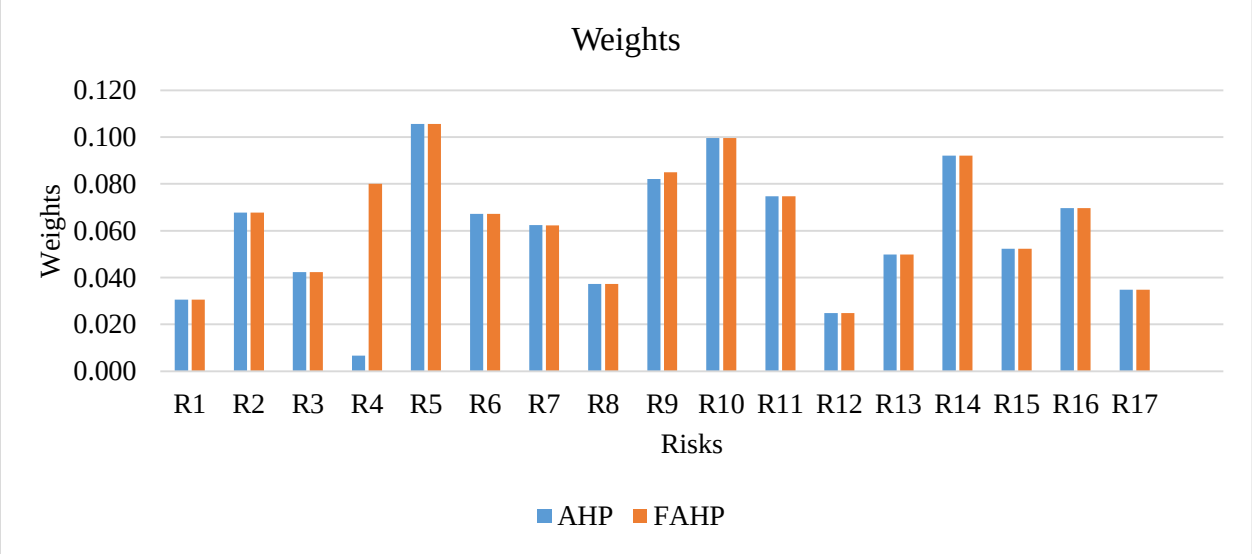

Figure 5.9 Weights obtained for AHP and FAHP

The Figure 5.10 shows the scores obtained from using FAHP-FTOPSIS and AHP-TOPSIS for case 2.

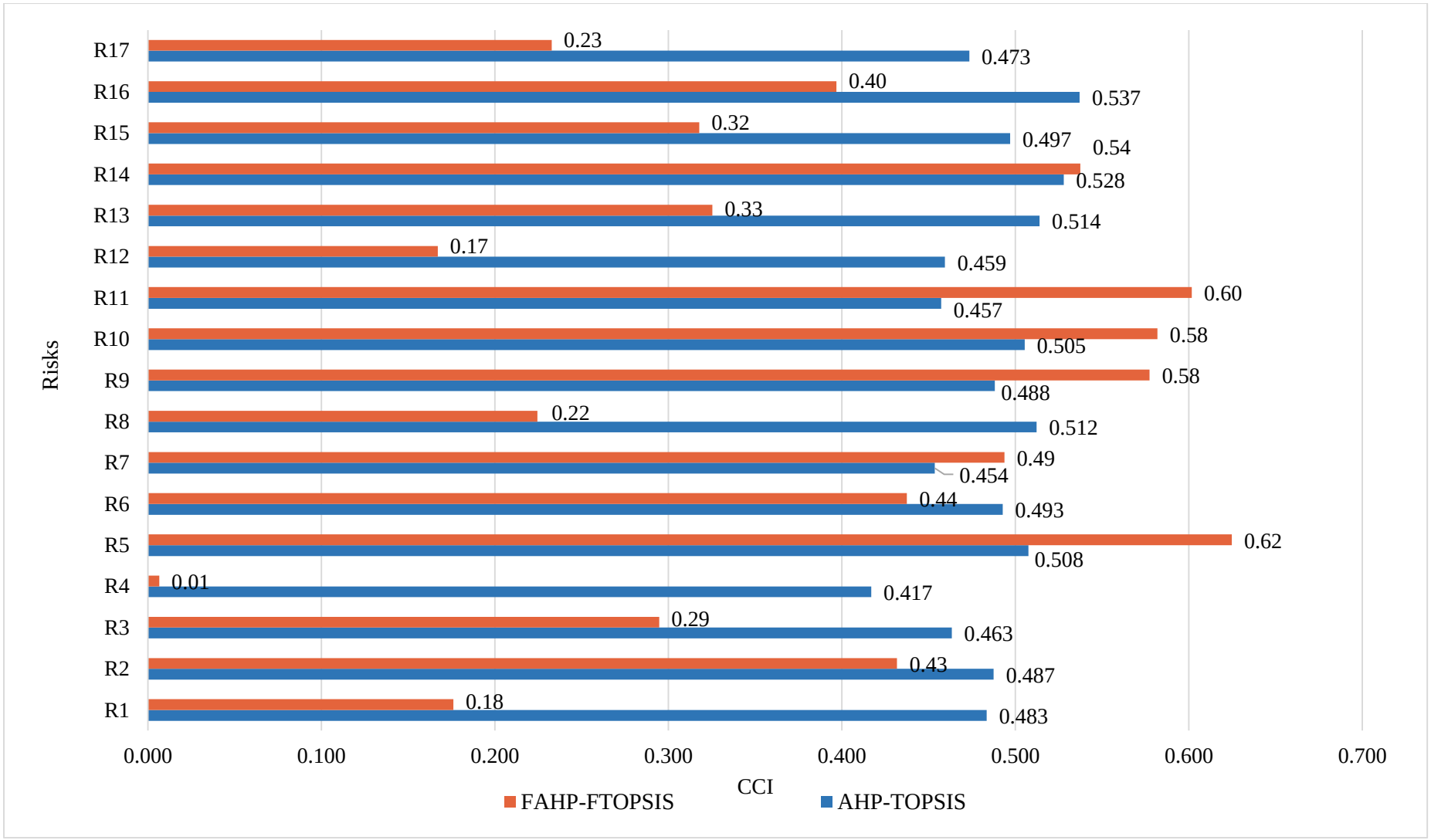

Figure 5.10 CCI values obtained from TOPSIS and FTOPSIS

After obtaining weights from using analytical hierarchy processes, TOPSIS both fuzzy and non-fuzzy was used to observe the final ranks obtained which fell in three categories of red, yellow and green risks. This is shown in Figure 5.10. After obtaining the final scores, a Kendall tau rank correlation coefficient analysis is performed to check the ranks consistency and see which method gives better and more consistent results. The coefficient value is 0.235. The value is towards a lower positive correlation side which implies that the use of FAHP-FTOPSIS gives better and more consistent results than the AHP-TOPSIS multi-criteria decision making technique. The correlation coefficient pairwise values are given in Figure 5.11 which is validated through SPSS analysis as shown in Table 5.9.

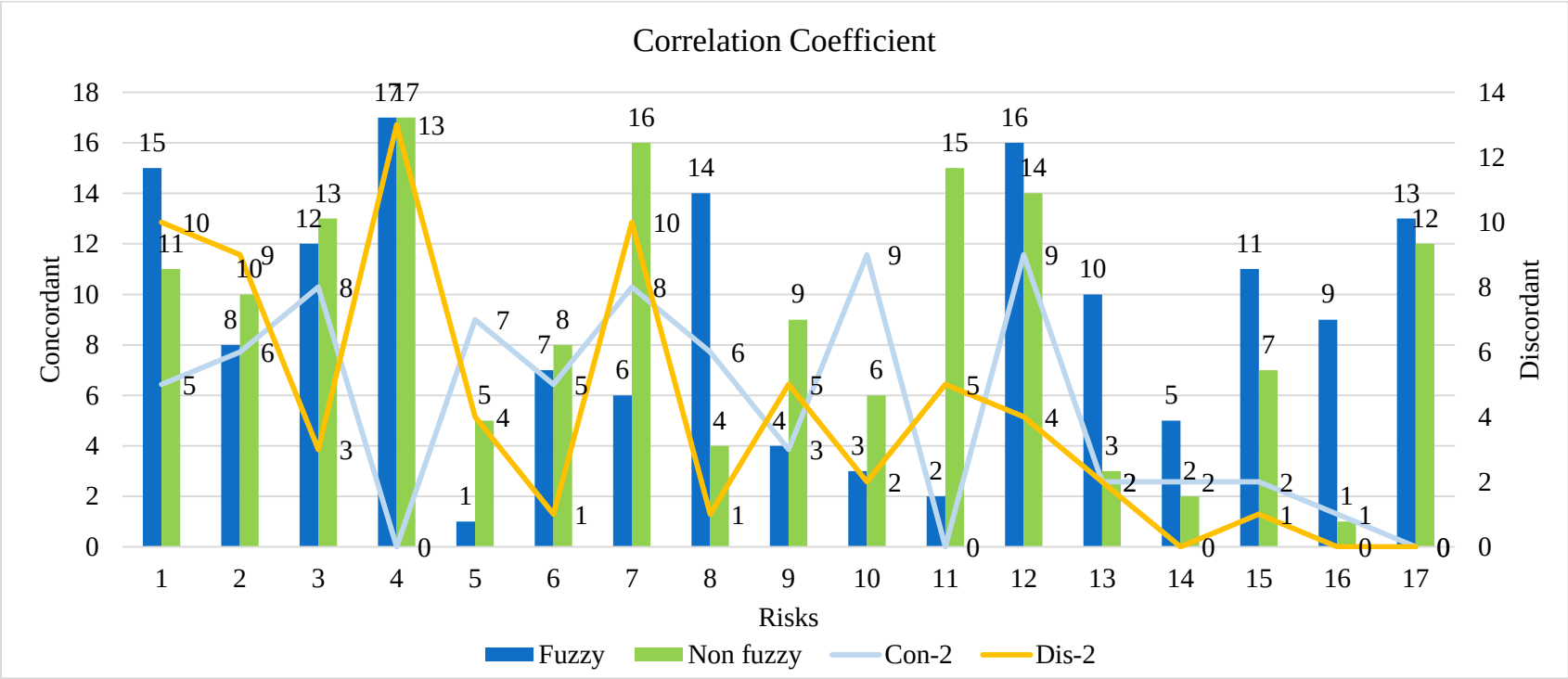

Figure 5.11 Kendall Tau coefficient obtained for AHP-TOPSIS and FAHP-FTOPSIS for case 2

Table 5.9 Kendall Tau b correlation coefficient for case 2 validation

			FAHPFTOPSIS	AHPTOPSIS
Kendall's Tau_b	FAHPFTOPSIS	Correlation Coefficient	1.000	.235
		N	17	17
	AHPTOPSIS	Correlation Coefficient	.235	1.000
		N	17	17

5.5 Comparison of Risk Assessment Frameworks

Every organization or business has risks involved in its operations which can hamper the normal working of the processes. Similarly, supply chains and logistics flows have many inherent risks that need focus and timely management. The focus of this research has been on conducting the risk assessment of using RFID technology in airport logistics operation of baggage management. Different definitions have also been given to integrated risk assessments (if at all). The degree of inclusiveness and level of analysis vary greatly, for example, in terms of the scope of the risks treated and the method of dealing with complex risks and uncertainties (Assmuth, 2008). For the purpose, a risk assessment framework was proposed and risk assessment was carried out using it. However, there are a number of risk assessment frameworks used for different domains. Nevertheless the framework proposed in this research is novel in its approach as it minimizes risks in a unique way.

To mention the risk assessment frameworks, some of the mostly used are SCOR, FMEA, EVITA, HEAVENS, MITIGATE, NIST, SCRMP, SCRA, CEA and House of Risk. Each of these risk assessment framework has a different way of solving risk analysis. However, the four key stages of risk assessment stay same for all the frameworks i.e. risk identification, risk analysis, risk mitigation and risk minimization. Nevertheless, some frameworks focus more on one stage than other which distinct them in the analysis. The proposed risk assessment framework is holistic in a way that it focuses on all the four stages of risk assessment. The novel integrated framework focuses on the last two stages more. In the second stage it uses a fuzzy based hybrid multi-criteria

decision making technique that produces brilliant results but it has been used in previous researches for ranking risks (F. Aqlan et al., 2015).

In the last two stages of risk mitigation and risk minimization, two novel phenomenon for risk analysis have been proposed. In the third stage, a risk mitigation taxonomy is developed followed by the development of a risk mitigation matrix (RMM). The RMM is used to consolidate the data for risk values before and after risk mitigation and calculate the risk reduction score. Once that has been performed using the proposed algorithm, next the last stage is performed. In the last stage, risk modelling is carried out and solved using a weighted goal programming approach on computer software. Moreover, for risk minimization a concept of risk reduction maximization is introduces under budget constraint to make the utilization of resources effective and time saving activities.

Since the aforementioned risk assessment frameworks focus less on risk minimization by effective implementation of mitigation strategies, this proposed risk assessment framework is novel in this respect.

Chapter 6. Conclusion

With each passing year, the traffic of passengers and the luggage at the airports is exponentially increasing. To achieve operational efficiency and customer satisfaction, airports are becoming smart and are using new technologies into their system. In airports, the issue of baggage handling has been critical over the years. There have been incidents of baggage mishandling, lost baggage and delayed baggage. To achieve competitive advantage, smart airports are using RFID based tagging system for real time monitoring of these flows through the journey of passengers. With the implementation of RFID based tags, the incidents of baggage mishandling have considerably reduced. However, with use of such technology, new vectors of attacks are opened.

This research proposes and used a new integrated risk assessment framework to do a risk analysis of attacks on RFID system deployed for baggage management at smart airports. For the purpose, a questionnaire was designed that was discussed and filled in by the experts. The framework used four steps namely risk identification, risk prioritization, risk mitigation and risk optimization to complete the assessment of risks. The results show that using FAHP-FTOPSIS, the top five risks that require urgent attention are jamming, tracking, denial of service, desynchronization and spoofing attacks. There can be many facilitators of these attacks to happen inside an airport such as frequency matching, cellular devices, other IoT devices and third party adversary. To protect airports from damage of customer goodwill, operational disruption and financial loss, next a set of risk mitigation strategies are identified.

Once the mitigation strategies were identified an analysis was run to see and select those mitigation strategies that can reduce the occurrence and impact of more than one risks. For this purpose, a risk mitigation taxonomy was developed which indicated how one mitigation strategy reduced more than one risk at time. Following that, a risk mitigation matrix was developed and filled in with the experts data collected via questionnaire. On getting response, the risk reduction scores were accumulated and collected. The results obtained from the risk mitigation matrix were then used as input for the risk minimization step.

A numerical analysis is then completed using a weighted goal programming approach in computer software. The goal programming was used to see the compromise between the two goals.

It shows that cost reduction and risk reduction are two opposing goals when it comes to risk minimization. It depends upon the policy and decision makers to see what goal is more important to them. This RMM can be used for decision making at tactical, operational and strategic level. Furthermore, in today's complicated and competitive corporate world, multi-criteria decision making has become a vital strategic choice. For this purpose a FAHP-FTOPSIS has been used to provide optimal ranking of the risks that are closer to the real ranks.

This study also performs a comparative analysis of two major multi-criteria decision making techniques AHP-TOPSIS and FAHP-FTOPSIS. Furthermore, it also validates the results by considering two cases from the literature in the form of research articles from well-known journals. It also validates the results by using a Kendall tau rank correlation coefficient to identify and conclude which MCDM technique outperforms the other. The results obtained have been explained comprehensively through tables and graphs in Chapter 5.

This research study contributes to the risk mitigation literature by first proposing a novel risk assessment framework. Furthermore, it studies the RFID implementation in airport baggage management from a risk lens which was missing from the literature. It offers and presents the most optimal set of mitigation strategies for under consideration risks that can practically be implemented by the McCarran International Airport, Las Vegas, America. Moreover, all the smart and non-smart airports around the globe can utilize this study to analyze whether the airport should implement on broad scale the technology keeping in mind the risks that come with its usage.

The research can be extended by considering more parameters for solving Risk Mitigation Matrix (RMM). Moreover, the study can extend the risk taxonomy developed in this research- which only considers positive correlation between different mitigation strategies- to considering negative correlation as well. Furthermore, the study can accommodate more risk measuring parameters when the RMM is formulated. Since, RFID is also being implemented in the cargo management process at the airport logistics, the study can be extended and be applied on the RFID bases cargo handling as well.

References

Afify, F., Badawy, M., & Tolba, M. (2014). Proposal Security Solutions to Protect Automation System from Denial of Service in Airports. *Int. J. Sci. Eng. Res, 5*, 1093-1099.

Ahmed, T., Calders, T., & Pedersen, T. B. (2015). Mining risk factors in RFID baggage tracking data. 2015 16th IEEE International Conference on Mobile Data Management.

Bathrinath, S., Bhalaji, R., & Saravanasankar, S. (2021). Risk analysis in textile industries using AHP-TOPSIS. *Materials Today: Proceedings, 45*, 1257-1263.

Cannon, A. R., Reyes, P. M., Frazier, G. V., & Prater, E. L. (2008). RFID in the contemporary supply chain: multiple perspectives on its benefits and risks. *International Journal of Operations & Production Management*.

Chan, C.-K., Chow, H. K., Ng, A. K., Chan, H. C., & Ng, V. T. (2012). An RFID case study for air cargo supply chain management. International Multi-Conference of Engineers and Computer Scientists. Hong Kong, China.

Chang, Y. S., Son, M. G., & Oh, C. H. (2011). Design and implementation of RFID based air-cargo monitoring system. *Advanced Engineering Informatics, 25*(1), 41-52.

Dutta, P., Choi, T.-M., Somani, S., & Butala, R. (2020). Blockchain technology in supply chain operations: Applications, challenges and research opportunities. *Transportation research part e: Logistics and transportation review*, *142*, 102067.

Etemadi, N., Borbon-Galvez, Y., Strozzi, F., & Etemadi, T. (2021). Supply chain disruption risk management with blockchain: a dynamic literature review. *Information*, *12*(2), 70.

Floerkemeier, C., & Sarma, S. (2008). An overview of RFID system interfaces and reader protocols. 2008 IEEE International Conference on RFID.

Fritsch, L. (2009). Business risks from naive use of RFID in tracking, tracing and logistics. 5th european Workshop on RFID Systems and Technologies.

Gabsi, S., Kortli, Y., Beroulle, V., Kieffer, Y., Alasiry, A., & Hamdi, B. (2021). Novel ECC-based RFID mutual authentication protocol for emerging IoT applications. *IEEE Access, 9*, 130895-130913.

Gao, X., Xiang, Z., Wang, H., Shen, J., Huang, J., & Song, S. (2004). An approach to security and privacy of RFID system for supply chain. IEEE international conference on e-commerce technology for dynamic e-business.

Giusti, I., Cepolina, E. M., Cangialosi, E., Aquaro, D., Caroti, G., & Piemonte, A. (2019). Mitigation of human error consequences in general cargo handler logistics: Impact of RFID implementation. *Computers & Industrial Engineering*, *137*, 106038.

Gładysz, B., & Santarek, K. (2014). Fuzzy TOPSIS/SCOR-based approach in assessment of RFID technology (ART) for logistics of manufacturing companies. In *Logistics Operations, Supply Chain Management and Sustainability* (pp. 129-141). Springer.

Gomez, L., Laurent, M., & El Moustaine, E. (2012). Risk assessment along supply chain: A RFID and wireless sensor network integration approach. *Sensors & Transducers*, *14*(2), 269.

Gopalakrishnan, K., Govindarasu, M., Jacobson, D. W., & Phares, B. M. (2013). Cyber security for airports. *International Journal for Traffic and Transport Engineering*, *3*(4), 365-376.

Grover, A., & Berghel, H. (2011). A survey of RFID deployment and security issues. *Journal of information processing systems*, *7*(4), 561-580.

Haibi, A., Oufaska, K., & El Yassini, K. (2019). Tracking luggage system in aerial transport via RFID technology. The Proceedings of the Third International Conference on Smart City Applications.

Hamdam, Y. (2020). Airport Cargo Logistics and Economic Outcome of Supply Chain: An Empirical Analysis. *Int. J Sup. Chain. Mgt*, *9*(1), 256.

Honari Choobar, F., Nazari, A., & Rezaee Nik, E. (2012). Power plant project risk assessment using a fuzzy-ANP and fuzzy-TOPSIS method. *International Journal of Engineering*, *25*(2), 107-120.

Hou, J. L., & Huang, C. H. (2006). Quantitative performance evaluation of RFID applications in the supply chain of the printing industry. *Industrial Management & Data Systems*.

Hwang, Y. H. (2015). Iot security & privacy: threats and challenges. Proceedings of the 1st ACM workshop on IoT privacy, trust, and security.

Irani, Z., Gunasekaran, A., & Dwivedi, Y. K. (2010). Radio frequency identification (RFID): research trends and framework. *International Journal of Production Research*, *48*(9), 2485-2511.

Isssource. (2012). *Firewall Costs; Hidden Costs*. Retrieved 5 May from https://www.isssource.com/firewall-costs-hidden-costs/

Kapoor, G., Zhou, W., & Piramuthu, S. (2009). Challenges associated with RFID tag implementations in supply chains. *European Journal of Information Systems*, *18*(6), 526-533.

Karygiannis, A., Phillips, T., & Tsibertzopoulos, A. (2006). RFID security: A taxonomy of risk. 2006 First International Conference on Communications and Networking in China.

Kaur, M., Sandhu, M., Mohan, N., & Sandhu, P. S. (2011). RFID technology principles, advantages, limitations & its applications. *International Journal of Computer and Electrical Engineering*, *3*(1), 151.

Koning Gans, G. d., & Garcia, F. D. (2010). Towards a practical solution to the RFID desynchronization problem. International Workshop on Radio Frequency Identification: Security and Privacy Issues.

Kumar, A., Jain, A. K., & Dua, M. (2021). A comprehensive taxonomy of security and privacy issues in RFID. *Complex & Intelligent Systems*, *7*(3), 1327-1347.

Lai, F., Hutchinson, J., & Zhang, G. (2005). Radio frequency identification (RFID) in China: opportunities and challenges. *International Journal of Retail & Distribution Management*.

Lee, S. M., Hwang, Y. J., Lee, D. H., & Lim, J. I. (2005). Efficient authentication for low-cost RFID systems. International Conference on Computational Science and Its Applications.

Li, H., Chen, Y., & He, Z. (2012). *The survey of RFID attacks and defenses* 8th International Conference on Wireless Communications, Networking and Mobile Computing.

Lin, C. Y., & Ho, Y. H. . (2009). RFID technology adoption and supply chain performance: an empirical study in China's logistics industry. *Supply Chain Management: An International Journal*.

Lykou, G., Anagnostopoulou, A., & Gritzalis, D. . (2008). Smart airport cybersecurity: Threat mitigation and cyber resilience controls. *Sensors*, *19*(1), 19.

Mishra, A., & Mishra, D. (2012). Application of RFID in Aviation Industry: An Exploratory Review. *Traffic Transportation*, *22*(5), 363-372.

Nădăban, S., Dzitac, S., & Dzitac, I. (2016). Fuzzy topsis: A general view. *Procedia Computer Science,*, *91*, 823-831.

Ngai, E. W. T., Cheng, T. C. E., Lai, K. H., Chai, P. Y. F., Choi, Y. S., & Sin, R. K. Y. (2007). Development of an RFID-based traceability system: Experiences and lessons learned from

an aircraft engineering company. *Production and operations management,, 16*(5), 554-568.

Palczewski, K., & Sałabun, W. (2019). The fuzzy topsis applications in the last decade. *Procedia Computer Science,, 159,* 2294-2303.

Panuparb, P. (2022). Cost-benefit analysis of a blockchain-based supply chain finance solution. In MIT (Ed.).

Parthiban, P. (2019). Fixed UHF RFID reader antenna design for practical applications: A guide for antenna engineers with examples. *IEEE Journal of Radio Frequency Identification, 3*(3), 191-204.

Rouchdi, Y., El Yassini, K., & Oufaska, K. (2018). Resolving security and privacy issues in radio frequency identification middleware. *International Journal of Innovative Science, Engineering & Technology, 5*(2), 2348-7968.

Sari, A. (2014). Security issues in RFID Middleware Systems: Proposed EPC implementation for network layer attacks. *Transactions on Networks and Communications, 2*(5), 01-06.

Saygin, C. a. N., B. (2010). RFID-based baggage-handling system design. *Sensor Review, 30*(4), 324-335.

Shepherd, A., Kesa, C., & Cooper, J. (2020). Internet of Things Medical Security: Txonomy and Perception. *Issues in Information Systems, 21*(3).

SITA. (2019). *SITA Baggage IT Insights 2019*. https://www.sita.aero/resources/surveys-reports/baggage-it-insights-2019/

Sitlia, H., Selouani, S. A., & Hamam, H. (2009). Technical solutions for privacy protection in RFID. *European Journal of Scientific Research, 38*(3), 500-508.

Sutar, A., Kocharekar, T., & Goilkar, P. M. (2018). Smart bag with theft prevention and Real Time Tracking. *International Journal of Trend in Scientific Research and Development,, 2*(2), 1118-1120.

Tikhonov, A. I., Sazonov, A. A., & Novikov, S. V. 2019. (2019). Digital aviation industry in Russia. *Russian Engineering Research,, 39*(4), 349-353.

Türeli, N. Ş., Durmaz, V., Bahçecik, Y. S., & Akay, S. S. (2019). An analysis of importance of innovatice behaviors of ground handling human resources in ensuring customer satisfaction. *Procedia Computer Science, 158,* 1077-1087.

Vishwakarma, V., Prakash, C., & Barua, M. K. (2016). A fuzzy-based multi criteria decision making approach for supply chain risk assessment in Indian pharmaceutical industry. *International Journal of Logistics Systems and Management,*, *25*(2), 245-265.

Wang, L. (2018). Application of Wireless Sensor Network and RFID Monitoring System in Airport Logistics. *International Journal of Online Engineering*, *14*(1).

Ying, C., & Fu-Hong, Z. (2008). A system design for UHF RFID reader. 2008 11th IEEE International Conference on Communication Technology.

Zhang, X., Dong, Q., & Hu, F. . (2012). Applications of rfid in logistics and supply chains: An overview. . *Logistics for Sustained Economic Development—Technology and Management for Efficiency*, *2012*, 1399-1404.