3-2024

Technology Assessment for Cybersecurity Organizational Readiness: Case of Airlines Sector and Electronic Payment

Sultan Ayed Alghamdi
Portland State University

Tugrul Daim
Portland State University, tugrul@etm.pdx.edu

Saeed Mohammed Alzahrani
Portland State University, salzahrani27@gmail.com

Citation Details

Published as: Alghamdi, Sultan Ayed; Daim, Tugrul; and Alzahrani, Saeed Mohammed, "Technology Assessment for Cybersecurity Organizational Readiness: Case of Airlines Sector and Electronic Payment" (2024). IEEE Transactions on Engineering Management.

Technology Assessment for Cybersecurity Organizational Readiness: Case of Airlines Sector and Electronic Payment

Sultan Alghamdi, *Member, IEEE*, Tugrul Daim, *Senior Member, IEEE*, and Saeed Alzahrani, *Member, IEEE*

Abstract— **Payment processing systems have advanced significantly in the airline business. Because e-payments are easy, they have captured the attention of many companies in the aviation industry and are quickly becoming the dominant means of payment. However, as technology advances, fraud grows at a comparable rate. Over the years, there has been a surge in payment fraud incidents in the airline sector, reducing the platform's trustworthiness. Despite attempts to eliminate e-payment fraud, decision-makers lack the technical expertise required to use the finest fraud detection and prevention assessments. This research recognizes the lack of an established decision model as a hurdle and seeks to fix the problem. In response, this research aims to develop a decision model for the airline industry to evaluate the e-payment fraud detection and prevention capabilities of airlines. The literature examines the scope of airline payment fraud to formulate the optimal framework to handle the problem. Guided by the results, the study proceeds to develop an HDM model from experts' validation, quantification, and desirability inputs. The results of the factors' validation and quantification show that the Economic and Financial, and the Security perspectives have the most impact on decision-making. Airline companies can use the developed framework to examine whether they are ready to adopt online fraud prevention technologies to increase their success rate. To measure payment organizations' readiness for digital payment fraud protection technologies, a scoring methodology was developed in this research and applied to two case studies.**

Index Terms—**Decision Making in Technology Management, Electronic Payment, Fraud Detection, Technology Adoption, Technology Acquisition, Technology Assessment.**

I. INTRODUCTION

The airline industry has experienced technological advancements in payment-processing methods. Technological development in the e-payment systems has improved the sector [1]. Since e-payments are convenient, these tools have attracted the attention of many airline players and are becoming the primary mode of payment [2] [3]. In addition, electronic payments have significantly changed with the introduction of mobile payments (M-payments) and more flexible options [4] [5]. With such advancements, fraud continues to grow similarly [6] [7]. Over the years, there has been an increase in payment fraud cases in the airline industry, reducing the platforms' reliability [2]. Modern technology has helped major airline companies adopt the electronic payment method as the easiest booking mode [8]. Therefore, the adoption of new e-payment methods has made it so that the majority of commercial airline operations are more competitive and efficient [9] [8]. According to a report by Rivest–Shamir–Adleman (RSA) Security, airlines are deeply affected by e-payment fraud. Some airlines have had a fraud rate as high as 46% of transactions reported as fraudulent [10]. In 2018 and 2019 alone, fraudulent attacks on the airline industry increased substantially to a rate of 61% in a span of one year. According to the International Air Transport Association (IATA), fraud costs the airline industry an estimated 1 billion USD annually [11]. The value of related fraudulent air ticketing has a higher percentage of occurrence, with many scammers targeting the upper-tier product line[6]. According to the American Association of Fraud Examiners (AAFE), 15% of all reported fraud-related cases involve credit card payments [2]. To prevent loss through fraud, payment fraud detection systems have become a major priority within e-commerce. Fraud can be understood as manipulative activities aimed at personal gains [12] [13]. In all areas that depend on electronic payment, fraud has become a leading concern. This includes the airline industry, which has experienced an increase in online technologies [14]. However, as fraudsters adjust to security mechanisms in these systems, fraud detection and prevention software fail to provide the needed protection [15]. As a result, fraud across online payments and other e-commerce platforms has increased by 178% as of 2022 [16] . As reported by the IATA, there is an exponential growth in e-payments losses. This calls for the need to equip management teams with reliable decision-making criteria for selecting the best solution [17]. In

Manuscript received XX XX, XX; revised XXX XX, XXXX; and accepted XX XX, XXXX. Review of this manuscript was arranged by Department Editor XXX. (Corresponding author: Tugrul Daim.)

Sultan Alghamdi is with the Department of Management Information System, Jeddah University, Jeddah, KSA (email: salghamdi1@@uj.edu.sa).

Tugrul Daim is with the Portland State University, Portland, OR 97201 USA, and also with the Chaoyang University of Technology, Taichung City 41281, Taiwan (e-mail: tugrul.u.daim@pdx.edu).

Saeed Alzahrani is with the Department of Management Information System, King Saud University, Riyadh, KSA (e-email: salhariri@ksu.edu.sa).

This article has been accepted for publication in IEEE Transactions on Engineering Management. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TEM.2024.3376314

the airline industry, countries such as Brazil, Mexico, and Argentina experience the highest number of attempts [6]. Among other risk factors, payment fraud has a grievous impact on airline profit bottom-line. Therefore, management teams are faced with the decision of trying to decide the best fraud prevention method to implement [18]. In making these decisions, they must consider multiple factors related to payment processing, including the cost, efficiency, security, and reliability of the options available to them. This calls for a multi-criterion decision-making process that can be improved by decision-making models [19]. The efficiency of the fraud prevention framework depends on the system's properties, reliability, and cost. However, the decision about the best payment method often falls on the shoulders of management entities who lack an intricate understanding of the technical aspect of the fraud prevention system, therefore, their decision may fall short of the expectation, be biased, or incomplete with the needs of the organization [20]. While management is primarily responsible for this decision process, developing and adopting a new fraud detection and prevention system is challenged by senior management's inadequate understanding of the economic, financial, and technical aspects [21] [22] [23]. Thus, a management team requires assistive decision-making models that they can depend on to make the best decision based on the multiple variables at play.

While such decision models do exist in the airline sector, the literature shows that the development of these models to assist in e-payment fraud prevention is limited, and management lacks the proper tools to make decisions reliably [12]. This study highlights various gaps in the existing literature. The first gap is the costly mistakes that can happen if the selected fraud prevention does not fit the organization's needs. A number of studies point out that developing fraud prevention software to aid in safeguarding electronic payment in America has not fully been adopted because of its high cost [2]. A study by Caldera et al. claims that installing fraud prevention software is expensive for organizations [24]. From the literature, the airline industry needs a reliable anti-fraud system that delivers loss reduction[25] [26]. However, deciding on the best tool that meets all their needs is limited by decision-making problems. The second gap indicates that while there are multiple options for fraud detection and prevention tools, not all solutions are reliable, which mandates developing a model to assess the exiting solutions. Hackers often dupe the available fraud detection systems, outmaneuvering their defense mechanisms [25] [27] [28]. Even though literature tries to understand the issue in detail on why it happens, there are inconsistencies in the payment system that airlines and other e-commerce sectors cannot solve efficiently[29]. Furthermore, how fraud controls are designed does not adequately allow them to respond to the changing landscape of fraud [29] [30]. Therefore, there is a need to explore further whether these factors if integrated into the decision-making tool will help the adopted system achieve higher reliability. Lastly, poor preparedness in decision-making when dealing with fraud exists. Fraud happens through myriad routes, making them difficult to predict [26] [31] [32] [33]. Whenever technology develops, it creates new avenues for fraud. Most fraudsters use existing technology to surpass and devise ways to outmaneuver existing protection [26]. This implies that, in one way or the other, fraudsters are experts who understand the existing technology, and they use sophisticated equipment with the ability to surpass the available fraud prevention software [26]. This means that the airline industry is never ready to deal with such issues as fraudsters are constantly changing their methods [26]. Therefore, there is a need for a system of decision-making pathways that will equip airlines with the capacity to detect and prevent fraud. A hierarchical decision model (HDM) is one important tool that the study employs to solve existing problems in the airline sector. The HDM outlined by this research allows corporations to assess their organizational readiness to adopt fraud detection and prevention techniques. In short, the model assesses how well organizations are responding to frustrations caused by fraudulent activity. The purpose of this research is to improve decision-making efficiency by developing a hierarchical decision model that fits the e-payment fraud prevention needs of the airline industry. This research addresses the existing challenges in selecting a fraud prevention method, and improves the reliability and efficiency of decision-making processes by employing a multi-criterion weighing of possible scenarios to arrive at the best solution. This study consults with industry professionals on perspectives and factors that are critical to the functioning of a fraud-prevention solution. The output is decision-making criteria that balances the weight of these variables against an organization’s level of readiness and needs.

II. Literature Review

A. E-Commerce and E-Payment

In a generic e-commerce model, companies offer their products and services online, and customers visit these shopping platforms to make purchases [34]. Companies offer real-time support that allows customers to reach the needed services, which in turn has increased businesses’ efficiency [8] [26]. E-commerce is considered an efficient way to reach customers at a lower cost [35]. A generic model of e-commerce that has been adopted in the airline sector involves e-commerce, goods/services, and customers. For example, in the airline industry, customers can use an online system to pay for flights at their leisure, and a payment for service is confirmed by electronic ticketing including a boarding pass, which a customer can download [18]. In the airline sector, e-commerce has increased efficiency in service delivery [18]. E-payment schemes facilitate e-commerce, and the most common e-payment schemes can be seen in the automated payment cards (credit or debit), online payment portals, and ATMs. They are responsible for facilitating online money transfers in real-time [36]. This implies that much security consideration is needed to ensure the safety of the operation of e-payment systems [37] [38]. The transaction is executed with the help of a third party or a payment gateway. The online payment scheme involves customer, merchant, payment gateway, customer financial institute, and merchant financial institute. At the epicenter of e-payments is continuous innovation. The use of mobile payments has become one of the greatest investments. and is a widely adopted method of payment in the airline industry due to their convenience and flexibility [39] [25] [31]. E-payments helped to increase convenience in the airline sector's swift and remote booking systems as well. However, e-payments have a myriad of challenges. As with any other sector, airlines are developing effective methods of responding to these challenges [40].

B. E-payment Systems and Touchpoints in the Airline Sector

The airline industry has adopted different types of e-payment, and has collaborated with payment companies, such as Mastercard International, to allow their credit and debit cards to be used. Visa and Mastercard are acceptable cards by almost any airline [41]. Moreover, M-Payments have also been introduced due their growth and ease of adoption [42]. However, there is still a long way to go in increasing the efficiency of mobile payment. Mobile payments account for 8% of online retail sales and 16% of online visits with a return customer rate of 23% as of 2011 [42]. The natural development and acceptance of the electronic payments technologies in general accompanied by the recent pandemic resulted in mass adoption of mobile payment leading to mobile payment users reaching 2.1 billion worldwide [43]. Through mobile payments, customers can easily reserve their seats with and pay later [44].

Despite these gains, the major challenges with electronic payments include a lack of proper systems to capture fraudulent attempts, high costs in completing e-system, and the general high risk of cyber-attack [45]. The outcome of such challenges has been the loss of billions, which necessitates the development of a fraud prevention system [46] [45]. Rudimentary fraud detection has become less feasible [45]. In the past years, banking and money transactions have expanded from the traditional methods to more robust approaches [47]. In most cases, electronic payment systems are expected to automate the processes and increase payment efficiency [48].

C. Benefits of Software in Payment Systems

E-payment involves the virtual transfer of currency or other payment mediums from one party to another. Payment methods have significantly evolved over the years with banks embracing a wide range of payment methods in response to customer needs [49]. As indicated in the literature, electronic payments have several advantages, such as security, accessibility, perceived convenience, and ease of payment [32]. All these components make electronic payments an effective replacement for traditional methods [32]. With recent technological development, electronic payments have become very common. Since the world is now operating through online platforms, e-payments have been linked with the increase in online businesses [50]. An advantage of e-payment is the automatic generation of records [14]. The advantages associated with online payment systems have increased their adoption into global systems; however, these advantages cannot be fully realized without proper e-payment fraud prevention. Adopting the right software will help the airlines attain many benefits including increased confidence in the reliability of the payment as there will be very few cases of fraud reported, the safety of payment will increase customer confidence, fraud prevention software will help the organization escape financial losses due to chargebacks, organizations will be better prepared to respond to market risks, and safety in online payment comes with good business relations. The travel industry is a chain of service providers focused on creating relationships anchored on trust and reliability.

D. Challenges Facing E-Commerce and E-Payment

The E-payment method adoption has increased payment processing efficiency [51] . In one way or another, banking institutions are experiencing a significant increase in efficiency. For example, the availability of diverse online payment methods has increased access to financial services. In addition, the automation of front office operations has facilitated the improvement of customer service over time [47]. However, e-payments and e-commerce have experienced many challenges, including fraud cases [41]. For example, there are reported cases of online fraud from different e-commerce segments every day. Where money takes the lead, fraud issues have been rising, making e-payment transactions challenging. The lack of a proper protection system is associated with an insufficiently skilled workforce. Most people in the financial sector have no knowledge of fraud detection and control [42]. It means that while e-commerce sectors adopt e-payments they, at the same time, do not have experts capable of fraud detection and control [31]. Therefore, the thriving e-commerce segment comes with the risk of transaction fraud.

There has been an increase in the number of complaints related to online fraud over the past few years [52]. This rise in complaints is estimated to increase further in the years to come. One of the main challenges of e-payments and e-commerce, according to Kim et al., is the unavailability of a comprehensive legal framework to address related crimes [52]. For instance, there are limited procedures for dealing with fraud and its detection. There has been developmental intervention on legal frameworks that would help deal with the issues of online money laundering, but this is in its early stages [52]. In addition, the universal nature of online fraud makes detection and prevention challenging. The current options available include adopting software that can help deal with fraud and hiring experts to oversee the processes [41].

E. Decision-Making Criteria in E-fraud Prevention

Research institutions and industry participants have allocated significant resources for developing fraud detection and prevention systems [2]. For example, Delta Airlines has positively incorporated fraud prevention software to deal with these issues. A challenge in fraud detection and prevention software development is high costs. For instance, Delta Airlines has spent over 50 million on developing effective fraud prevention platforms [53]. Similarly, travel agencies invest approximately 1.4 billion dollars every year to deal with the problem of fraud. Due to the limited knowledge of the technical aspects of fraud prevention software, the efficiency of decision-making has been generally slow as the management fails to evaluate available options reliably [26], resulting in an improper fit.

If the correct fit is achieved, fraud detection software is a major tool that will be responsible for reducing the financial costs of adoption[26] [54]. An analytical approach to decision-making in fraud prevention requires that before the fraud is detected by the fraud protection process, all possible outcomes must be evaluated [26]. This analysis can reveal variables that aid in understanding the problems, and that have the ability to design a system that can prevent fraud. Despite understanding the problem, a key limitation is the failure to test all variables against a common scale when making a decision concerning the best approach [55]. The key variables that decision-makers must weigh when selecting the best e-payment method may involve security issues, effect on organization trust, and internal and external issues. After the identification of an issue, the decision-maker must decide about the security issues/threat it poses as well as how these affect its partners [55] [14] [56]. These parameters are considered alongside the internal and external business environment. By measuring the proposed systems' properties against each other, regarding the components above, a hierarchical decision-making tool can rapidly overcome the limitation in knowledge faced by the top management.

F. *Significance of the Solution in Fraud Prevention*

The development of e-payment fraud detection and prevention software is critical given that fraud instances are increasing with the increased adoption of technology, and there is an urgent need to come up with solutions [57]. Finding a solution must begin with mapping factors that influence sector fraud [35]. Even though it is hard to predict all origins of fraud, areas of vulnerabilities and their impact can be identified [10] [58]. A problem in fraud prevention is the high cost required to fund software development projects [59]. Developing new software is costly, and would require vital investment by the companies. Most companies have lost so much on frauds that they are unwilling to commit to such development. This occurs when the software is misaligned to the problem perspectives [60]. Correct identification of these perspectives is, therefore, essential. These solutions provide a composite assessment of factors associated with fraud in the airline sector [61]. Furthermore, expert input provides a framework for understanding the challenges and developing fitting solutions [60]. In addition, multi-criterion decision-making allows for quick response, thus giving existing systems the evolutionary potential to evolve in the best way to beat fraudsters through fast decision-making [60]. The study adds to existing literature and emphasizes the difficulties with implementing various online payment schemes. One of the significant factors contributing to the failure or slow adoption of online payment is a lack of comprehensive and structured knowledge of the various perspectives around online payment in the airline business, including economic and financial, technological, legal, security, and organizational perspectives. In this model, we find the most highly rated elements that must be taken into account during the implementation and adoption procedures.

III. Methodology

A. *HDM Model*

The HDM is a multi-criteria decision-making tool that was introduced by Dundar F. Kocaoglu 1981. Implicit in the structure of decision models is a complex network in which various degrees of criticality are assigned to the decision elements. It has the capability to break complex decision problem such as the fraud detection and prevention problem into manageable tasks. The model's objective function coefficients are the decision variables' weighted contribution. The probability model can measure the relative chance of occurrence of various elements [19]. Particularly, by assessing the history of financial fraud, how it occurs, and its impact on the financial system, a criterion can be developed with attributes and parameters that measure the impact of interrelated actions and result when the emerging model is applied [19]. The role of a decision-making process is to solve strategic (S), tactical (T), and operation (O) solutions to existing organizational problems [62]. A decision process is multilayered and hierarchical in structure. Financial fraud in airline ticketing presents a cost problem to the airline industry [63]. Thus, deploying a decision model that would fix the problem demands understanding the associated risks. Currently, the airline industry ticketing framework is exposed to fraudulent financial activities that are common to all payment systems that relies on technology to communicate. Understanding the origin of fraud is pertinent to fraud detection and prevention [16]. Fraud needs to be detected and predicted before it occurs. The HDM model perspectives are significant in undertaking a decision framework [64].The given perspectives originate from different literature on fraud detection and prevention in e-payment systems in the airline industry.

After determining the impact of individual variables relative to the objective function of the HDM model, the overall importance of the decision paths can be obtained by multiplying their importance with desirability. The following mathematical equation is often used [65] [66] [67] [68].

$$\text{AF Score} = \sum_{n=1}^{N} \sum_{Jn=1}^{Jn} \left(S_{n,Jn}^{AF}\right)(D,Jn)$$

Where AF = variables with possible impact on the outcome $(D, Jn) =$ $desirability\ value\ of\ performance\ measures\ relative\ to\ jn$ ^{AF} success attribute with respect to the nth perspective.
$(S_{n,Jn}^{AF}) = the\ relative\ value\ of\ the\ jn^{AF}$ success measure relative to the nth variable, and in relation to factors affecting the project.

B. Desirability Curves

Experts quantified the model parameters and assessed the desirability metrics to be consistent [20] [66] [67] [69]. Experts should consider how the model parameters can be used to assess the efficacy of the framework, and the various metrics will clarify the importance of these factors to the decision process. Desirability curves typically quantify the degree to which a factor is desirable by highlighting its relative importance [70] [71] [72] [73]. Experts assign a point between 0 and 100 to each category based on the expert's assessment of importance. Using the desirability curves, an evaluator can determine the usefulness and applicability of individual factors. The appendix shows the desirability curves for the factors. The benefit of desirability curves is that the model results in the flexibility needed to perform beyond the capabilities of other methods. The formula is presented below to calculate the readiness score for the solution’s adoption [23] [74] [75] [76]:

$$E\,(a_i) = \sum_{p=1}^{P}\ \sum_{c=1}^{C}\ P_i C_k^{l}\, \mathrm{d}(m_i, cp) \qquad \text{for } i=1,\dots,\mathrm{I}$$

Let:
I: Available solutions.
C: Available selection criteria.
P: Available perspectives.
E (a_{i}) = solution’s readiness score with regard to alternative i.
P_{p}: perspective p weight to the decision objective.
C_C^p: The relative impact a of criterion c in relation to perspective p and the decision objective.
d(m_{i},c_p): performance metric desirability rating of alternative (i) under c^{th} criterion within perspective (p$^{\mathrm{th}}$).

IV. Model Development and Results

This paper proposes a hierarchical decision-making model (HDM) to identify and assess the key perspectives to fraud prevention tool selection choices. An HDM approach is introduced to identify fraud prevention tool decision factors. The model will be fully validated with the assessment of panelists' responses, then iteratively redesigned for a process evaluation. Network diagrams will illustrate the relationships between decision factors under each of the core perspectives shown in the table below. A total of 43 subject matter experts in the e-payment fraud detection and prevention in the airlines industry are distributed across 12 expert panels based on their expertise with respect to the topic under investigation for the validation and quantification of the model constructs.

A) Model Validation

Experts were invited to take part in the study. Their role was to validate if the framework is appropriate for the assessment of the fraud detection and prevention in the airline industry. The objective of the validation phase is to ensure that the model is as close to reality as possible, and can be used as an assessment tool for e-payment fraud detection and prevention capabilities in the airlines industry based on the inputs from the experts in the topic. Each model element is considered when two-thirds of the experts approve it. If an element is not proved by two-thirds of the experts, then it is removed. Without loss of generality, elements of the second level of the model are substantiated by an indifferent rating. Qualtrics surveys were used to gather data on and in with interviews on observations of experts, collecting participants’ judgments of variables, underlying science, and concepts as well as behavioral patterns that affect the selection of the best fraud prevention tool. A total of 37 experts were distributed across 6 panels to complete the validation phase. Expert feedback necessitates some changes to the model’s factors. From economic and financial perspectives, the expert recommended the addition of the cost of “financial risk and uncertainty” as a factor. From a technology perspective, the respondents opted for the addition of “scalability” and “capability” to the model. From a legal perspective, the respondents recommended “governance” as a factor. Under security, the respondents recommended “security infrastructure” and “data protection” as additional factors. Under organization perfectives, the respondents recommended “reporting” as an additional influential factor. The tables below show the validated model element.

Table 1: Perspectives

Perspective	Definition	References
Economic & Financial	This is the cost of fraud prevention systems, and the legal or financial perspective of the loss from unsuccessful applications of software.	[5] [10] [45] [61] [58]
Technological	This is to what extent the solution will fit in within the multiple technical perspectives. For example, whether a communication protocol would serve a good use under the current circumstances.	[61] [77] [78]
Legal	The regulatory and legal perspective provides important details for operations executives and managers to understand in the airline sector in order to successfully implement their fraud prevention systems. It helps to know which laws and regulations a company will need to comply with as it interacts with customers or collects their personal information.	[58] [79]

Security	The developed solution provides a high level of security through advanced encryption technologies, allowing for access to files with the advanced level of security throughout the process eliminating the risk of security breaches.	[19] [78] [80] [81]
Organizational	Corporate culture can be a very important aspect of any successful organizations, but it can negatively impact adoption of a new technology. Organizations must ensure that to avoid technical misfit which leads to poor adoption of the fraud prevention technology.	[82] [78] [83]

1) Economic & Financial Perspective

This is the cost of fraud prevention systems, and the legal or financial perspective of the loss from unsuccessful applications of software.

TABLE 2: ECONOMIC & FINANCIAL PERSPECTIVE

Criteria	Definition	References
Economic & Financial perspective		
Financial Instability	Unpredictability in patterns of fraudulent activities is costly to an organization if the solution adopted cannot respond in time to these risks. Financial stability is the summation of cost of updates, and the prevention of losses that would otherwise have occurred through various means including chargeback over time.	[84] [85] [86] [87] [88]
Financial output	Fraud results into significant losses in an airline. This factor measures the cost advantages that an airline enjoys by selecting a particular fraud prevention tool over another, including operation costs. Financial output of a solution is the gain that comes from failed fraud attempts. It is the retention of revenues that would otherwise been lost to fraud.	[79] [87] [88] [89]
Economic investment	The initial installation of a fraud prevention solution including buying, and installation costs, the cost of investment should be within the organization financial capability.	[79] [88] [89]
Economic efficiency	The ability of the solution to be distributed or allocated to in the most valuable economic uses and waste is eliminated or minimized.	[79] [88] [89] [90]
Cost	This is a factor that measures the cost of operations including human resource training, power, and effect of the organization's financial bottom-line.	[32] [91] [92] [93]
Financial risk and uncertainty	This is a measure of the capabilities of an airline company to measure risks and financial costs associated with a selected solution. Such costs include the network, transactional, scalability, and maintenance among others.	[32] [91] [92] [93]

2) Technological Perspectives

To what extent the solution will fit in within the multiple technical perspectives. For example, whether a communication protocol would serve a good use under the current circumstances.

TABLE 3: TECHNOLOGICAL PERSPECTIVE

Criteria	Definition	References
Technological perspective		
Infrastructure and platform features	Fraud is a constantly evolving problem, and the technological solutions available to airlines must have the capacity to evolve with the environment. This factor measures the rate and degree of advancement in the technology.	[3] [61] [94]
Ease of use	The staff's technical capacity to operate a technological solution successfully or the ability to interact easily and effortlessly with a technological solution, including the accompanying concepts.	[3] [61] [95] [77] [85] [96]
Interoperability	Describes systems and software applications that are diversified and allows for communication, data exchange, and analysis to ensure proper system functionality.	[83] [96]
Impact on productivity	The ability of the system-based application to enhance the job performance and service provided	[61] [95]
Capability	The technological and functional capability of the preferred solution to detect fraud, trigger alarm and respond to intrusion attempts. The system should also have reporting capabilities	[10] [95] [77] [85] [96] [97]

Scalability	Fraud is an expanding problem, the solution selected by an organization should be easily scalable to the prevailing organizational conditions	[10] [78] [97]

3) Legal Perspectives

The regulatory and legal perspective provides important details for operations executives and managers to understand in the airline sector in order to understand and implement their fraud prevention systems. It helps to know which laws and regulations a company will need to comply with as it interacts with customers or collects their personal information.

TABLE 4: LEGAL PERSPECTIVE

Criteria	Definition	References
Legal perspective		
Legal uncertainty	Within the legal frameworks, there are differences between applicable laws in different countries provide. The airlines have to follow legal provisions of many different countries which makes the legal landscape a complicated problem. The solution implemented need to conform to legal provisions in these destinations.	[98] [99] [100]
Legal compliance	Fraud prevention solutions deal with personal data and are expected to comply with requirements spelled out in legal guidelines concerning data usage. The factor measures conformity to the legal requirements with regard to quality and usability standards.	[101] [98] [99] [100]
Legal incentives	This factor measures the available incentives that would help in dealing with payment problems in the airlines industry. The incentives start from being lower level to higher levels. They are needed to promote the different elements available.	[82] [95] [98] [100]
Legal approval	Legal frameworks should be approved to make it appropriate and available in the airlines industry. Without approval by the relevant authority, its usage can be drawn into question of legality in its application to prevent fraud. Approval ensures that the solution is confirmed to be safe for use.	[95] [99] [100]
Governance	For any information technology system, there is a need for a system of IT governance to control its access and use. Governance described the established rules that control system access privileges	[77] [96]

4) Security Perspectives

The developed solution provides a high level of security through advanced encryption technologies, allowing for access to files with the advanced level of security throughout the process. Such specificities are very important to payment data, due to the risk of security breaches.

TABLE 5: SECURITY PERSPECTIVE

Criteria	Definition	References
Security perspective		
Security infrastructure	Security architecture is the ability of software within the organization to detect any form of fraud. Adequacy guarantees security and the options available helps in engaging the entire processes with the right alternatives. It will engage different issues with the right elements that would be made.	[91] [92] [102]
Security design	The design should reflect suitable security elements that is mandatory and in line with the most current technology. Since technology changes fast, the design should be adaptive to new technological requirements.	[32] [67] [92] [99] [103] [104] [105]
Security personnel	The company's personnel are responsible for using and maintaining the system in the best form to prevent fraud. It measures the security personnel level of skills to implement and ensure optimal operations of the fraud prevention security solution.	[91] [92] [93] [103]
Data protection	The system should be supported with an advanced-level data encryption and access feature. These lines of defenses are to avoid security breaches. The access control is determined by the sensitivity of data to unauthorized access	[22] [47] [96] [106] [107]
Security governance	At the data access level, security governance concerns the authorization and authentication procedures in place	[22] [47] [96] [106]

5) Organizational Perspectives

Corporate culture can be a very important aspect of any successful organizations, but it can negatively impact adoption of a new technology. Organizations must ensure the technology is a good fit, as technical misfit leads to poor adoption of the fraud prevention technology.

TABLE 6: ORGANIZATIONAL PERSPECTIVE

Criteria	Definition	References
Organizational Perspective		
Management support	Management support is vital in fraud detection and prevention in the airlines industry. The management should work with other departments in determining the best course of action and must be brought on board to ensure the success of the proposed system.	[10] [47] [106]
Organizational readiness	This factor measures the level of preparedness and readiness of an organization to deal with fraud. The available fraud detection software will be responsible in undertaking the processes.	[10] [47] [106]
Training and skills	Training is essential to develop a pool of experts who will be able to maintain the fraud prevention solution. The level of personnel training to work with the security architecture should be considered.	[47] [61] [106]
Organizational strategy	Organizations are driven by mission and vision, which then shapes the organization strategy. The strategy is an aspect that helps in designing a pathway for problem solving. The selected solution should be aligned with the organization processes and the operational framework of the organization.	[10] [61]
Reporting capabilities	The technological system should be able to develop real-reporting o security events within the system.	[10] [47] [83] [106]

B) Quantification Results

The hierarchy model in decision-making for the HDM involves expressions of judgement on the impact of factors on a given outcome [66] [67] [82] [108] [109]. Experts in this phase go through a set of pairwise comparisons evaluating the perspectives of the decision to be made. The measure of this procedure depends on the number of perspectives that experts will need to clear quantify. Given that five perspectives will require straight comparisons, the number of pairwise comparisons will be constrained to 10 [20] [99]. Quantifying perspectives and factors, and valuing both global and local weights is necessary for any degree of clarity in decision-making [74] [79]. We want to ask experts about the degree to which bracketing, Pareto ranking, data fusion, priorities, criteria for selection, policy-based metrics, and assessment of pairs of different criteria and variables impact decision making [74]. The goal of the experiment is to define what approaches and recommendations suit a fraud prevention tool selection process the best. Experts were distributed across 6 panels to quantify the model elements ranging from 11 to 13 experts per expert panel.

1) Model Weights

The quantitative section presents the results of the perspectives' and the factors' contributions to the research objective. These results show that the economic and financial, and the Security perspectives have the most impact on decision-making. By weight to the model, the Data Protection factor is the strongest (9.5%), followed by the cost factor (8.7%), and then infrastructure and platform features (7.8%).

2) Final Model Weights

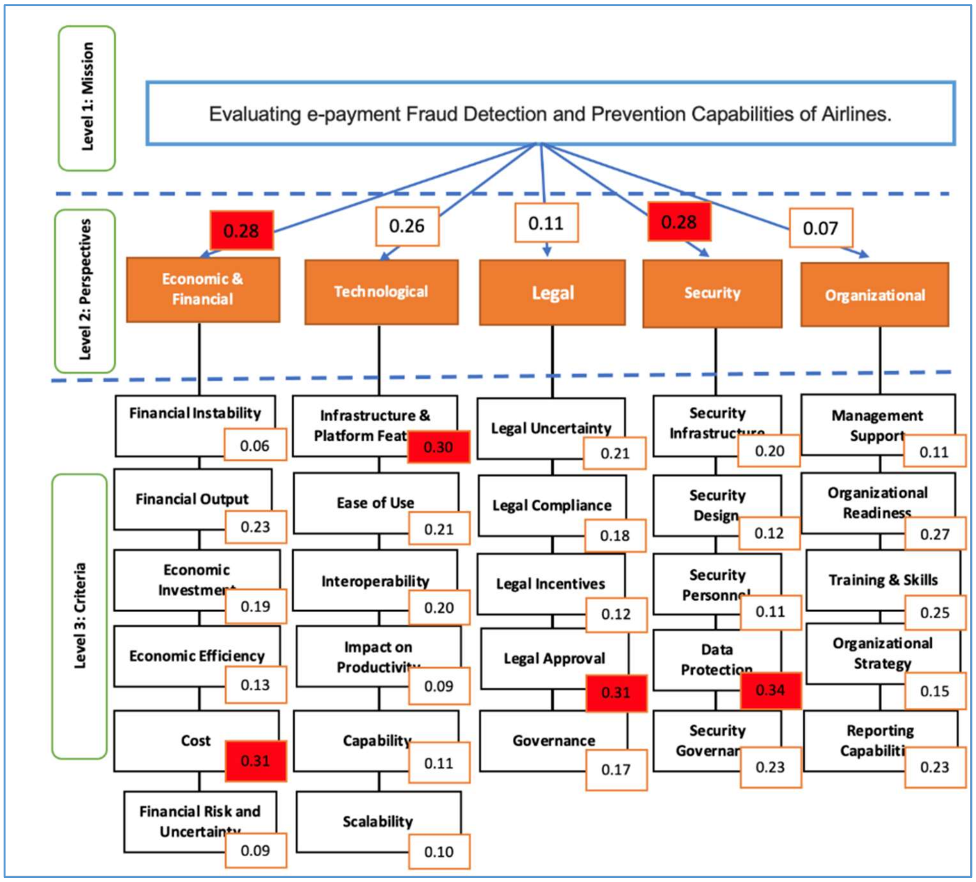


Figure 1: Final model weights

V. CASE STUDIES

Our research team has identified and matched a model that is a performance metric of fraud prevention in the airline industry. The model is valuable to businesses through its quantitative results regarding the conditions that are favorable in designing their fraud prevention strategies. Testing the model with a real organization allows for the evaluation of the model's real-world significance and improves it based on the results. For this research, two cases have been selected, which are the Saudia Airlines and Swiss International Airlines.

A. Case 1: Saudia Airlines

King Abdulaziz International Airport in Jeddah is the primary operating base for Saudia Airlines. Riyadh King Khalid International Airport and Dammam King Fahd International Airport are secondary hubs. Saudia Airlines, a Saudi company based in Jeddah, has four primary objectives: supplying quality and competitive services, focusing on customer satisfaction, technological improvements, and sophisticated payment processing. Saudia Airlines is at the forefront of technical advancements, with sophisticated payment processing capabilities. To stay abreast of technological advances and new technologies that may have a positive impact on their services, Saudia Airlines tracks, studies, and monitors them. To allow the case study to be developed, an interview was conducted with executives of Saudia Airlines, who have both academic and professional IT experience. Saudia Airlines has partnered with online payment gateways to establish new technology cooperation, drive innovation, and develop a fraud-resistant payment system. The goal of the initiative is to develop a solution to the problem. The airline seeks to develop startup-led items, services, and tools to address credit card fraud.

B. Case 2: Swiss International Airlines

Swiss International Airlines is among the airline companies that are recognized nationally and internationally for its state-of-the-art services, and that strives to implement the most rigorous safety and care for consumer data. The airline is working towards reducing the risk of payment fraud. It has built a strong technology infrastructure over the past several years to deliver top-quality services. It has been recognized as one of the most technologically sophisticated companies in the industry thanks to its IT solutions. Among the IT solutions are authentication procedures, for example. It also keeps track of new technologies as they emerge through several initiatives. While the organization is advancing in the use of technology to reduce operational costs, it has been cautious in the process resulting in an often-calculated approach to the market. Regardless of the speed of the adoption, the company is among the first adopters of the online payment system.

C. Rationale Behind the Case Studies

Using a robust research design to study real-world applications is important in ensuring the research's accuracy. It is necessary to test whether or not a research design works in the real world. These cases provide a deeper understanding of how airlines might perform in a developed readiness model.

Fraud prevention might be applied to these two cases, each of which comes from a distinct system, and that plays a distinct role in frontline payment fraud prevention. The solution might be used to enhance the two organizations' payment systems in addition to management and interoperability challenges. The model will be used to assess whether it reacts in line with the nature of these two cases. These two organizations have shown their cooperation and interest in exploring criterial factors and applying the model in examining their decision criteria.

D. Case Study Analysis

This research used the HDM model developed in the previous sections to determine the overall readiness scores for the two case studies introduced in the previous section. The experts from each case study were asked to provide values for each factor based on their knowledge. The interviews were conducted to obtain these values. The mathematical algorithms discussed previously were used to compute the overall readiness scores. Scenario analysis will then be used to determine how sensitive the model is, and how it will impact each case across various scenarios. The importance of the model is assisting decision-makers in the selection of the best solution to adopt.

1) Readiness Scores

TABLE 7: CASES OF SAUDIA AIRLINES & SWISS INTERNATIONAL AIRLINES

Perspective	Value	Factor	Global Weights	Case 1 VS	Case 1 FS	Case 1 VS	Case 1 FS
Economic & Financial	0.28	Financial Instability	1.7%	80	1.34	84	1.41
		Financial Output	6.4%	90	5.80	90	5.80
		Economic Investment	5.3%	71	3.78	68	3.62
		Economic Efficiency	3.6%	70	2.55	100	3.64
		Cost	8.7%	70	6.08	80	6.94
		Financial Risk and Uncertainty	2.5%	90	2.27	54	1.36
Technological	0.26	Infrastructure & Platform Features	7.8%	95	7.41	77	6.01
		Ease of Use	5.5%	75	4.10	70	3.82
		Interoperability	5.2%	75	3.90	83	4.32
		Impact on Productivity	2.3%	75	1.76	100	2.34
		Capability	2.9%	95	2.72	80	2.29
		Scalability	2.6%	75	1.95	72	1.87
Legal	0.11	Legal Uncertainty	2.3%	75	1.73	78	1.80
		Legal Compliance	2.0%	95	1.88	100	1.98
		Legal Incentives	1.3%	50	0.66	68	0.90
		Legal Approval	3.4%	50	1.71	100	3.41
		Governance	1.9%	85	1.59	82	1.53
Security	0.28	Security Infrastructure	5.6%	90	5.04	93	5.21
		Security Design	3.4%	90	3.02	70	2.35
		Security Personnel	3.1%	90	2.77	72	2.22
		Data Protection	9.5%	100	9.52	100	9.52
		Security Governance	6.4%	80	5.15	59	3.80
Organizational	0.07	Management Support	0.8%	80	0.62	66	0.51
		Organizational Readiness	1.9%	90	1.70	58	1.10
		Training and Skills	1.8%	100	1.75	70	1.23
		Organizational Strategy	1.1%	70	0.74	64	0.67
		Reporting Capabilities	1.6%	90	1.45	53	0.85
					82.96		**80.49**

2) Strengths and Weaknesses

The cases scored highly in several areas of readiness and capability when adopting a new fraud prevention solution, but there are many ways to improve the adoption. For Case 1, Saudia Airlines, the needed infrastructure exists in the company. It also has the technological capacity to install innovative fraud prevention programs, and the company sees fraud prevention solutions as a matter of compliance. The organization sees that the need to guarantee data protection is a priority, and it also has people trained and skilled personnel equipped for these roles. However, the case has some areas of weaknesses. The economics of fraud prevention is weak, installing new fraud prevention will come at an extra cost, it has little legal incentive to install a new system, and the new system does not add significant value by a legal approval, and currently, new fraud prevention is not a key part of organization strategy. For Case 2; Swiss International Airlines, the strengths include the expectation to improve the general efficiency of its financial system, to enjoy the advantage of efficient fraud detection, and meet data management, and security compliance. The solution is also legal, and not in violation of the laws. However, the organization must put more emphasis on the need to reduce financial risk and uncertainty through planning, and by developing a governance structure that dictates the access and the use of their resources, by creating and becoming more prepared for smooth operations of the software, and by making use of the system reporting capabilities to improve service delivery. This comparison yields a better understanding of how organizations respond to adoption factors and how airlines of a similar nature are likely to score similarly.

The level of technological readiness in both cases points to areas of commonalities in strengths. There is commonness in the need for infrastructure to support the development as well as the expectation of the advantage of efficiency in fraud detection software leading to improvement in productivity. There are also commonalities in compliance with the requirements in data management, and security as a priority. Even with the input of the software, the companies are concerned about real gains in the direction of the economics of new fraud prevention is weak and certainty of fraud reduction through planning. In addition, organizations are concerned with the quality of reporting capabilities.

3) Suggested Enhancements

Fraud prevention has become a priority for e-commerce businesses to avoid loss. Fraud can be defined as deceptive activities aimed at personal gains [51]. The increased use of electronic payments in the airline industry has made fraud detection and prevention software increasingly ineffective [110]. Fraudsters alter their tactics as security mechanisms change in these electronic payment systems, making them less protected. According to the 2012-2018 Gergo Report, online payments and e-commerce fraud increased by 40% [16], and credit card payments fraud increased by 16% [111]. Borrowing from the scenario analysis, the following are the suggested improvements to the cases.

TABLE 8: SUGGESTED IMPROVEMENTS FOR BOTH CASES

Perspective	Factor	New VC CS1 Score	New CS1 Score	Action	New VC CS2 Score	New CS2 Score	Action
Economic & Financial	Financial Instability	100	1.68	Organization needs more financial incentives to invest	100	1.68	Organization needs more financial incentives to invest
	Financial Output	90	5.80	No Action	90	5.80	No Action
	Economic Investment	71	3.78	No Action	90	4.79	More budgetary allocation to fraud prevention solution
	Economic Efficiency	90	3.28	Consideration to economic benefits	100	3.64	No Action
	Cost	70	6.08	No Action	90	7.81	Cost reduction at installation
	Financial Risk and Uncertainty	90	2.27	No Action	90	2.27	Reduction of financial risk and uncertainty through planning
Technological	Infrastructure & Platform Features	95	7.41	No Action	95	7.41	Infrastructural allocations
	Ease of Use	75	4.10	No Action	90	4.91	The technology should be easily usable by the staff
	Interoperability	75	3.90	No Action	90	4.68	The system should be operable across multiple platforms
	Impact on Productivity	75	1.76	No Action	100	2.34	No Action
	Capability	95	2.72	No Action	80	2.29	No Action
	Scalability	90	2.34	Technology solution adopted should be highly scalable	90	2.34	Technology solution adopted should be highly scalable
Legal	Legal Uncertainty	100	2.31	Mapping legal uncertainty	100	2.31	Mapping legal uncertainty
	Legal Compliance	95	1.88	Legal compliance as a service standard	100	1.98	No Action
	Legal Incentives	90	1.19	There should be incentives attached to technology development	100	1.32	There should be incentives attached to technology development
	Legal Approval	90	3.07	Technology adopted should be legally sound	100	3.41	No Action
	Governance	90	1.68	Technology governance is needed for smooth operations	100	1.87	Technology governance is needed for smooth operations
Security	Security Infrastructure	90	5.04	No Action	93	5.21	No Action
	Security Design	90	3.02	No Action	70	2.35	No Action
	Security Personnel	90	2.77	No Action	72	2.22	Personnel training is critical
	Data Protection	100	9.52	No Action	100	9.52	No Action
	Security Governance	80	5.15	No Action	90	5.80	Need security governance
Organizational	Management Support	100	0.77	More management support is needed	100	0.77	More management support is needed
	Organizational Readiness	90	1.70	No Action	90	1.70	Organizational preparedness is a question of necessity for smooth operations of the software
	Training and Skills	100	1.75	No Action	100	1.75	Need for personal training
	Organizational Strategy	90	0.95	Fraud prevention solution should be part of organization strategy	90	0.95	Fraud prevention solution should be part of organization strategy
	Reporting Capabilities	100	1.61	Put more emphasis on reporting capabilities	100	1.61	Put more emphasis on reporting capabilities
Improvement Scores			**87.51**			**92.72**	

VI. DISCUSSION

Online fraud is a major problem that requires the adoption of preventative solutions. Most present initiatives to combat online fraud require improvements to be effective. Online fraud prevention is a new technology, and present models are insecure, difficult to maintain, understudied, and have not been validated in mission-critical applications. Online fraud prevention is changing and being implemented more quickly than ever before. As a result, efforts to curb online fraud have shown to be ineffective for corporations. In addition to the technology itself, airlines confront a slew of significant hurdles in the face of an upsurge in online fraud. Several online fraud protection programs have been shut down or scaled back in terms of goals and timelines, according to recent reports. A literature review was conducted to identify and evaluate current sources of information on the evaluation of existing payment fraud solutions used in the airline industry. The influence of each decision standpoint was considered. Digital payment protection technology has grown in popularity in recent years. As a result, most airlines utilize payment management platform technologies that enable faster and more reliable transfers, but they are vulnerable to abuse. Nonetheless, there is a scarcity of research that regularly and carefully evaluates the factors influencing digital payment fraud prevention solution adoption in the airline industry. This research looks into five perspectives: economic and financial, technical, legal, security, and organizational.

A. Financial and Economic Perspective

Six criteria, according to experts, are crucial and can be used in selecting the best fraud prevention solution with respect to economic and financial perspectives. The following factors were used in the model: financial instability, financial output, economic investment, economic efficiency, cost and financial risk and certainty with each having local weights of 6%, 23%, 19%, 13% and 31% respectively. Thus, cost was the most important factor from a financial and economic perspective, and is trailed by financial output, economic investment, financial risk and uncertainty, and financial instability. To be effective, airlines must commit to building and sponsoring online fraud prevention activities. Payment organizations must be committed to preventing online fraud at reasonable costs.

Online fraud protection is still in its infancy in terms of maturity and depth. Cases of real-world applications are rapidly rising, and estimating the cost is challenging. Payment institutions should be ready to address uncertainties and plan for the numerous expenses connected with using the technology, such as the extension of their fraudulent financial transaction protection network, service charges, administration, and scalability.

Airlines that invest in fraud prevention must assess the return-on-investment metrics before implementing online fraud protection technologies. Companies may fail to recognize the positive return on investment provided by online fraud protection. Some suggestions for lowering the cost of fraud detection and prevention include automating human contact verification, minimizing costly mistakes, eliminating unneeded middlemen, decreasing record duplication, and shortening the time and effort required for data collection. Using verification methodologies and measures, payment organizations should undertake a cost analysis to determine the financial gains from a solution. The six factors have been proved to be important in adoption. Airlines must understand their financial situation and manage it accordingly to achieve successful adoption.

B. Technological Perspective

Six factors were identified as important by experts and quantified from a technological perspective. These included the infrastructure and platform features, ease of use, interoperability, impact on productivity, capability and scalability. The quantification of technological aspects reveals that infrastructure and platform features (30%) and ease of use (21%) are the most important considerations. These are trailed by interoperability 20%, capability 11%, scalability 10%, and impact on productivity 9%. Airlines must be aware of technological requirements as well as their applications to fraud prevention.

Incompatible technological applications impede data interchange. The majority of fraud protection suppliers do not develop suitable software. An effective system must be operable to standardize with the prevailing needs of the organization, technology suppliers, and changes in the fraud landscape. This research analyzes the organizational readiness of corporations to keep up with evolving fraud tactics. One of the most serious difficulties is the incapability of the fraud prevention solution to meet operational needs. To standardize online fraud protection, authorities, developers, and digital payment services must work together. A payment institution must have a defined plan in place for the management of data related to the online fraud prevention system.

C. Legal Perspective

Five variables have been identified by experts as critical in the regulatory and legal industry. These include: legal uncertainty, legal compliance, legal incentives, legal approval and governance. Legal approval is the most essential aspect, according to the quantification results, with a relative relevance of 31%. This is followed by legal uncertainty and compliance as the second and third most significant concerns, with 21% and 18% relevance, respectively. Governance and legal incentives are also important aspects in legal perspectives with a weight of 17% and 12% respectively. Approval of the method used by an organization in relevance to the current rules and regulations is a key factor in the spread and application of technology. Approval is also related to the capacity of online fraud prevention technologies to comply with payment legislation and legal norms that safeguard the use of personal information such as data sharing, system privacy, and security.

Furthermore, the technology's adaptability to changing rules and regulations is critical. Online fraud protection technology is new and as a result, rules governing the technology remain ambiguous. Payment organizations must collaborate in fraud prevention networks. If incentives were offered to early adopters, organizations would be motivated to implement online fraud detection and prevention and data sharing.

D. Security Perspective

From the security perspective, five crucial characteristics have been confirmed and measured by experts. These variables are security infrastructure, security design, security personnel, data protection and security governance. Data protection is seen as the most important of the five components, with a weight of 34%. This is followed by governance, security infrastructure, security design and security personnel at 23%, 20%, 12% and 11% respectively. With a relative value of 8%, security personnel are viewed as the least significant component.

Because the industry is still in its early stages, payment institutions must spend heavily on expertise and education. There are a dearth of acceptable skill sets in the market, causing a lack of adequate experience and knowledge to build online fraud protection. This issue has not yet been successfully addressed by the digital fraud prevention ecosystem [58]. As a result, the growth of digital fraud protection expertise is increasing. Airlines must stay current on the development of online fraud protection technology and hire the appropriate professionals (workers) to run online detection and prevention projects.

Several parties, notably payment organizations at all levels, should recognize the potential of digital detection and prevention technology to interrupt the credit system and solve several of the present payment difficulties. It is the instructional character of digital fraud detection and prevention adoption that makes it challenging, not its technological complexities. As a result, the importance of online fraud protection is underappreciated. It is not as simple as just doing it. Aside from educational challenges, there are unrealized potential benefits. It is tough to persuade businesses to join an online fraud protection network [86]. Market players must work together to build widely used online fraud protection technology and foster an atmosphere of shared value.

E. Organization Perspective

Experts identified five aspects that are critical and may be quantified in developing the model. These include: management support, organizational readiness, training and skills, organizational strategy and reporting capabilities with relative weights of 11%, 27%, 25%, 15% and 23% respectively. Organization-level preparedness is required for the successful integration of fraud protection systems. At the organizational level, there is a need for understanding and awareness of the impact of the system.

Understanding the function of digital payment fraud detection and prevention innovation adoption is crucial to achieving a higher-level strategic objective. It is vital to recognize that online fraud protection should help improve payment, promote payment participation, raise efficiency and reduce the operational cost, improve service delivery and results in a better functioning system. While the deployment of online fraud protection should be aligned with the payment organization's IT strategy, there is a need for airlines to identify the skills and training necessary to undertake and sustain the change.

F. Insights from the Case Studies

The model developed in this study was implemented in a case study scenario to assess the decision-making process at Saudia Airlines and Swiss International Airlines. The use of case studies gives some intriguing insights into fraud prevention technology. The model measured how the perspectives and factors affect the outcomes, as well as how the features and interactions with the organization impact system acceptability. The use of the case with the same model gives a clear image of the decision-making criteria for a digital payment fraud prevention solution.

With respect to the Case 1, Saudia Airlines, for the technological perspective, it had a higher rating for infrastructure and platform features because the needed infrastructure exists in the company. Similarly, the organization has the technological capacity to install innovative fraud prevention programs. From a legal perspective, legal compliance had a higher score indicating that fraud prevention solution is a matter of compliance. With respect to the security perspective, the organization values data protection factors. It recognizes the need to guarantee data protection. In the organizational perspective, Saudia Airlines values training and skills as it has trained and skilled personnel. Saudia Airlines also has some weaknesses. The economics of fraud prevention is weak, installing new fraud prevention will come at an extra cost, it has little legal incentive to install a new system, the new system does not add significant value by legal approval, and currently, new fraud prevention is not a key part of organization strategy.

Regarding Case 2, Swiss International Airlines, the strengths include the organization's expectations to increase its financial output by installing a new fraud prevention system, to benefit from the added capability of better fraud prevention is seen as an advantage and the that the organization is ripe for innovation. Swiss International Airlines' areas of improvement include the perception that the change is expected to have little impact on productivity, little legal incentive to install a new system, and the new solution is not part of the legal governance of the company.

VII. Conclusion and Contributions

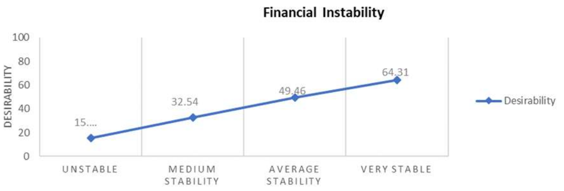
Fraud prevention and detection are critical for reducing financial losses. Fraud prevention is an important research direction for companies operating online. In this study, the loss associated with fraud in e-commerce is measured. This study investigates decision-making preferences in the prevention of e-payment frauds within the airline industry. This study uses expert judgment to value the weights of perspectives and factors that influence the suitability of payment fraud protection solutions applicable to the airline industry. The results of this study show that the economic and financial, and security perspectives have the most impact on decision-making. Furthermore, among the evaluated factors, the cost, infrastructure and platform feature, legal approval, and data protection are the most important factors. Airlines can use the developed framework to examine whether they are ready to adopt online fraud prevention technologies to increase their success rate. To measure payment organizations' readiness for digital payment fraud protection technologies, a scoring methodology was developed in this research.

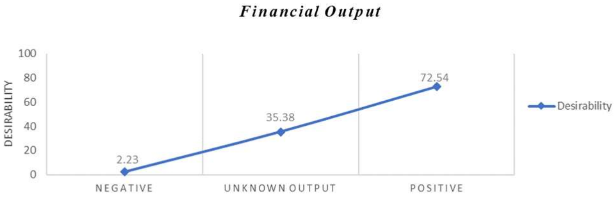
This research offers advice to airlines on decision-making criteria when selecting a fraud prevention tool. These suggestions are grouped into two groups. The first set is derived from criteria weights on factors critical to the selected solution based on expert judgement. The second set is derived from the case study of Saudia Airlines and Swiss International Airlines. Experts ascribed weights to factors identified to have a critical impact on the decision process. The deployment of online fraud protection should be optimized for each significant component. Based on the factors' weights with respect to payment fraud protection technologies in the airlines industry, the recommendations include that airlines should allocated more financial resources to invest in such solutions, technology solution adopted should be highly scalable, mapping legal uncertainty, technology adopted should be legally sound, technology governance is needed for smooth operations, more management support is needed, and fraud prevention solution should be part of organization strategy. Furthermore, another set of recommendations based on the evaluation of the cases' scores on the desirability curves are highlighted. These recommendations involve more budgetary allocation to fraud prevention solution, cost reduction at installation, reduction of financial risk and uncertainty through planning, infrastructural allocations, the technology should be easily usable by the staff, the system should be operable across multiple platforms, technology governance is needed for smooth operations, development of security infrastructure, and personnel training is critical.

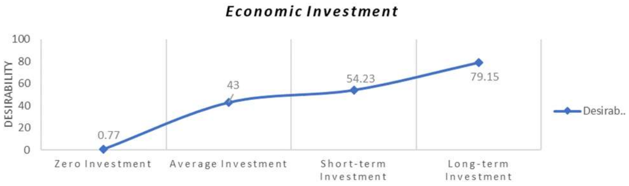
Finally, this research contributes to knowledge on technology management, particularly on the assessment of the evolving technology such as the online payment technology in airline fraud using strong and holistic decision-making models such as the HDM. The key aim of this study is to increase information regarding how airlines assess, implement, and adopt online payment technology for the management of airline fraud. The scoring model is effective in lowering the failure rate of online payment system acceptance because it gives early signs for elements and perspectives that require improvement before and during deployment. The suggested framework is probably the first to provide a complete analysis of fraud prevention systems that encompasses the key aspects that influence this technology's adoption and examines its implications in the aviation sector. There is a lack of a comprehensive framework of evaluation, thus this research expands on studies of the elements and viewpoints in assessing technology adoption. In practice, this research allows airline organizations to have a better understanding of online payment technology including the progress in the adoption process, the challenges, and the target for the adoption. The model is applicable at different stages of the adoption process. It can be used at the start and during the implementation process. Besides, it can gauge the organization's ability to proceed with the adoption process.

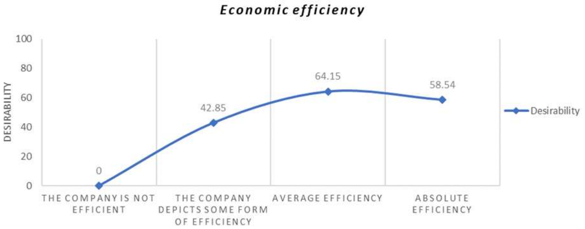
APPENDIX

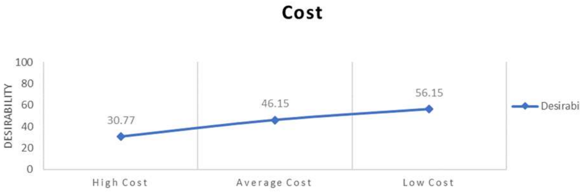
Desirability Curves

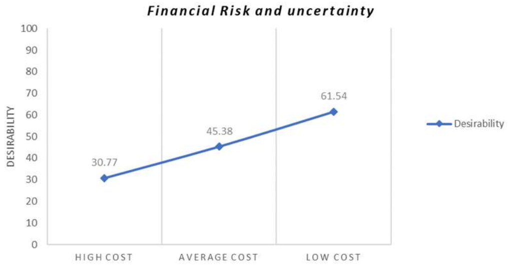


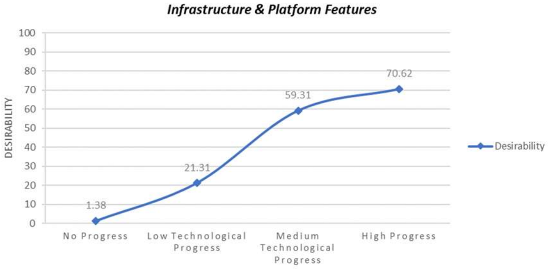




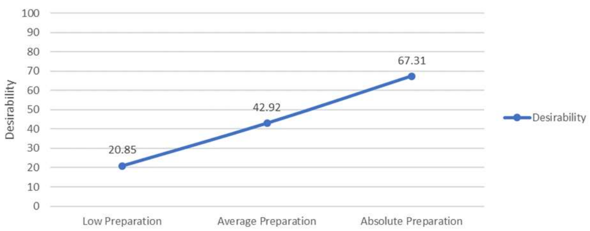




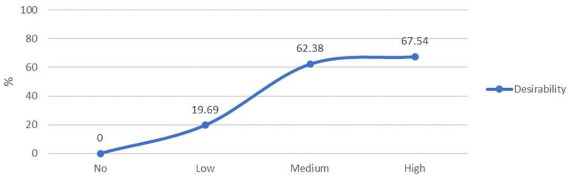




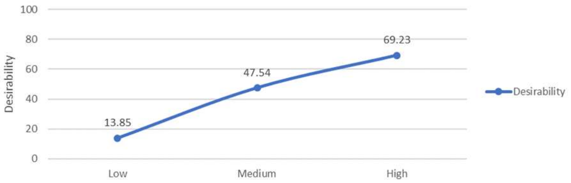
Ease of Use



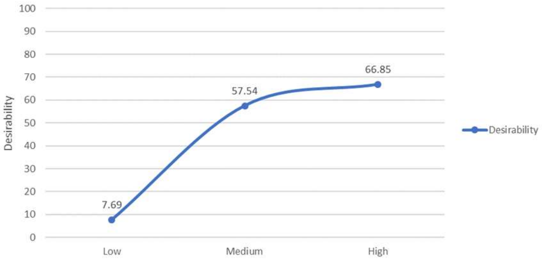
Interoperability



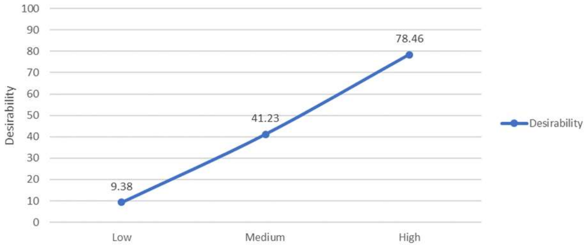
Impact on Productivity



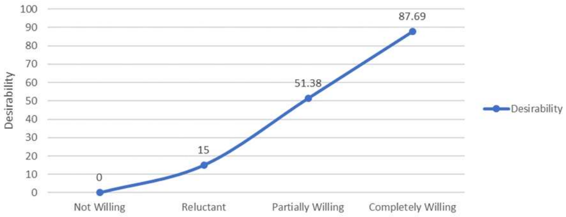
Capability



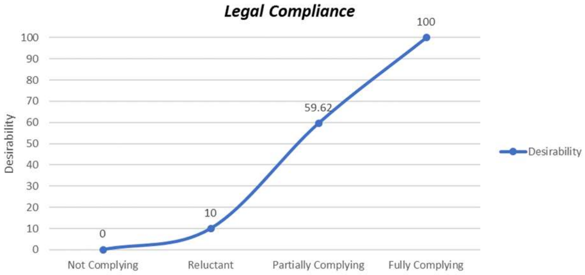
Scalability



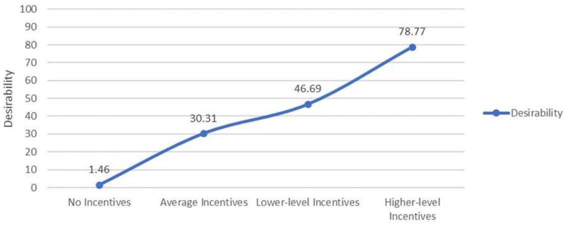
Legal Uncertainty



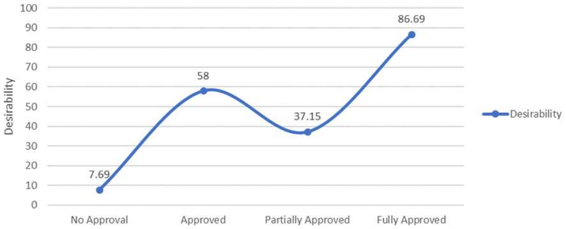
Legal Compliance



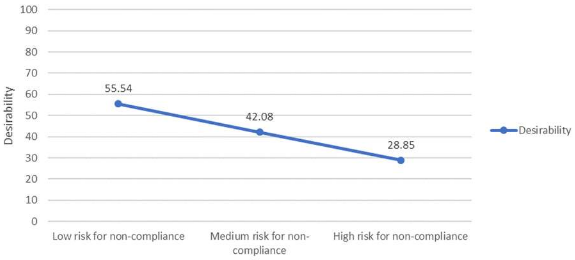
Legal Incentives



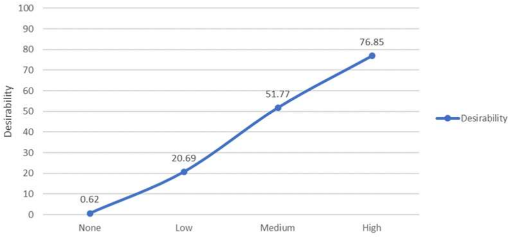
Legal Approval



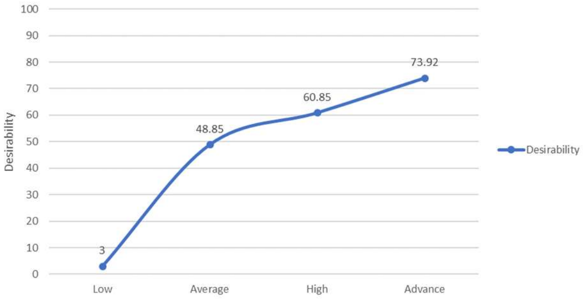
Governance

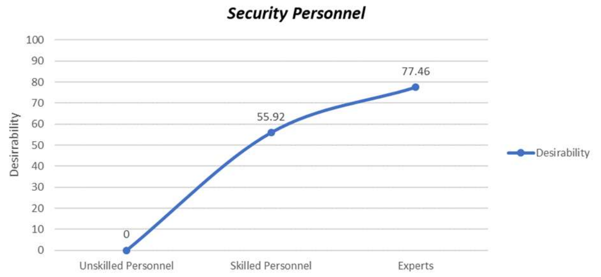


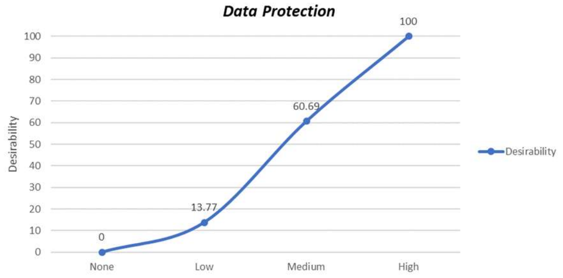
Security Infrastructure

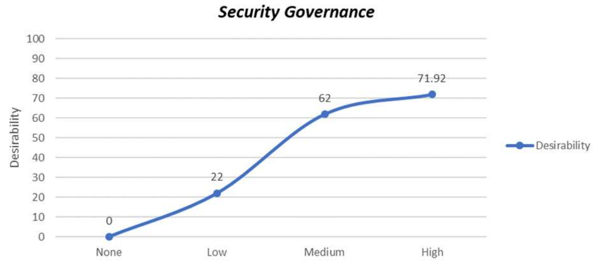


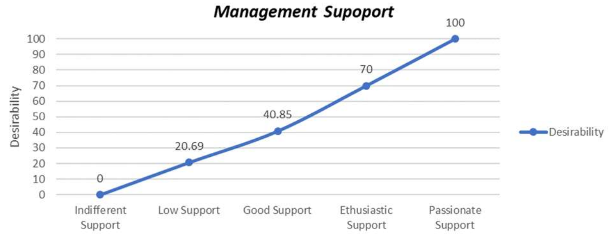
Security Design

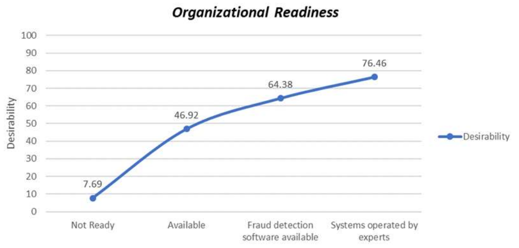


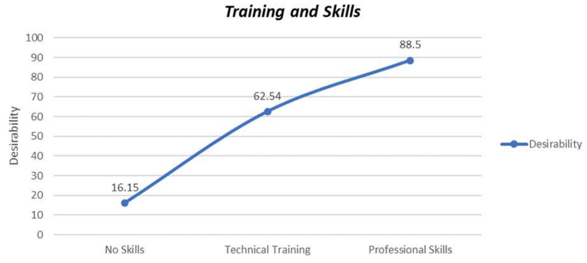


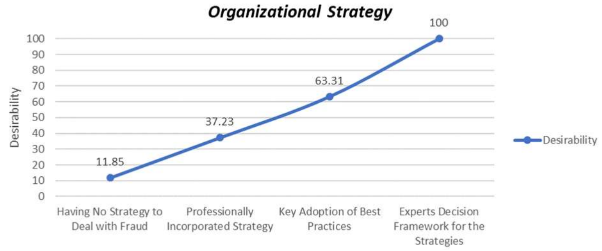


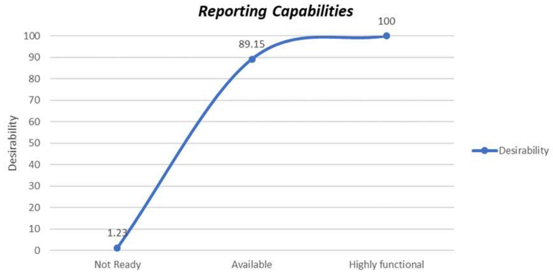












References

[1] T. Tsiakis and G. Sthephanides, "The concept of security and trust in electronic payments," *Computers & Security*, vol. 24, no. 1, pp. 10–15, Feb. 2005, doi: 10.1016/j.cose.2004.11.001.

[2] S. Carta, G. Fenu, D. Reforgiato Recupero, and R. Saia, "Fraud detection for E-commerce transactions by employing a prudential Multiple Consensus model," *Journal of Information Security and Applications*, vol. 46, pp. 13–22, 2019, doi: 10.1016/j.jisa.2019.02.007.

[3] C. Csáki, L. O'Brien, K. Giller, J. B. McCarthy, K. Tan, and F. Adam, "The use of E-Payment in the distribution of social welfare in Ireland:Charting the daily experience of recipients," *Transforming Government: People, Process and Policy*, vol. 7, no. 1, pp. 6–26, 2013, doi: 10.1108/17506161311308142.

[4] F. KARNOUSKOS, STAMATIS; FOKUS, "Mobile payment: A journey through existing procedures and standardization initiatives.," *IEEE Communications Surveys & Tutorials*, vol. 6, no. 4, pp. 44–66, 2004.

[5] O. Gentiana, Gjino; Ilollari, "Mobile banking - near future of banking," *Review of Applied Socio- Economic Research*, vol. 7, no. 1, pp. 43–51, 2014.

[6] International Air Transport Association, "Fraud in the airline industry why carriers need to think of themselves as crimefighters," *IATA*, no. July, 2020.

[7] S. K. Hashemi, S. L. Mirtaheri, and S. Greco, "Fraud Detection in Banking Data by Machine Learning Techniques," *IEEE Access*, vol. 11, pp. 3034–3043, 2023, doi: 10.1109/ACCESS.2022.3232287.

[8] R. Law and R. Leung, "A study of airlines' online reservation services on the internet," *Journal of Travel Research*, vol. 39, no. 2, pp. 202–211, 2000, doi: 10.1177/004728750003900210.

[9] R. AlGhamdi, S. Drew, and W. Al-Ghaith, "Factors Influencing e-commerce Adoption by Retailers in Saudi Arabia: a qualitative analysis," *The Electronic Journal of Information Systems in Developing Countries*, vol. 47, no. 1, pp. 1–23, 2011, doi: 10.1002/j.1681-4835.2011.tb00335.x.

[10] J. Yomas and C. Kiran, "A Critical Analysis on the Evolution in the E-Payment System, Secuiry Risk, Threats and Vulnerability," *Communications on Applied Electronics*, vol. 7, no. 23, pp. 21–29, Dec. 2018, doi: 10.5120/cae2018652800.

[11] C. Walker, "Fighting fraud in the airline industry," *RAVELIN TECHNOLOGY LTD*, 2017.

[12] A. Koponen, "E-COMMERCE, ELECTRONIC PAYMENTS," *Telecommunications Software and Multimedia*, pp. 1–27, 2006.

[13] N. M. Hussien and Y. M. Mohialden, "An Overview of Fraud Applications and Software on Social Media," in *Advances in Multimedia and Interactive Technologies*, A. J. Obaid, G. H. Abdul-Majeed, A. Burlea-Schiopoiu, and P. Aggarwal, Eds. IGI Global, 2023, pp. 1–11. doi: 10.4018/978-1-6684-6060-3.ch001.

[14] D. Mangala and P. Kumari, "Corporate Fraud Prevention and Detection: Revisiting the Literature," *Journal of Commerce and Accounting Research*, vol. 4, no. 1, 2015, doi: 10.21863/jcar/2015.4.1.006.

[15] C. Wang, S. Chai, H. Zhu, and C. Jiang, "CAeSaR: An Online Payment Anti-Fraud Integration System With Decision Explainability," *IEEE Trans. Dependable and Secure Comput.*, pp. 1–14, 2022, doi: 10.1109/TDSC.2022.3186733.

[16] G. Varga, "E-Commerce Fraud up by 178% over the Holidays: Trends and Predictions," *Global Trade Magazine*, Jan. 2022.

[17] IATA, "IATA Industry Fraud Prevention," 2017.

[18] R. Y. Abdulahi and A. Y. Demisse, "Challenges of E-payment service in Commercial Bank of Ethiopia," *Proceedings - International Conference on Management and Service Science, MASS 2009*, pp. 1–4, 2009, doi: 10.1109/ICMSS.2009.5304469.

[19] T. U. Daim and D. F. Kocaoglu, *Hierarchical Decision Modeling Essays in Honor of Dundar F. Kocaoglu*. Cham: Springer International Publishing, 2016. doi: 10.1007/978-3-319-18558-3.

[20] S. Alzahrani, T. Daim, and K. K. R. Choo, "Assessment of the Blockchain Technology Adoption for the Management of the Electronic Health Record Systems," *IEEE Transactions on Engineering Management*, 2022, doi: 10.1109/TEM.2022.3158185.

[21] J. H. Lee, R. Phaal, and S. H. Lee, "An integrated service-device-technology roadmap for smart city development," *Technological Forecasting and Social Change*, vol. 80, no. 2, pp. 286–306, 2013, doi: 10.1016/j.techfore.2012.09.020.

[22] E. Taylor, "Mobile payment technologies in retail: a review of potential benefits and risks," *International Journal of Retail & Distribution Management*, vol. 44, no. 2, pp. 159–177, Feb. 2016, doi: 10.1108/IJRDM-05-2015-0065.

[23] M. S. Abbas, "Consistency Analysis for Judgment Quantification in Hierarchical Decision Model," *ProQuest Dissertations and Theses*, p. 173, 2016.

[24] K. Caldera, Jose;Hain, Joseph M; Sherlock, "Enhanced automated anti-fraud and anti-money-laundering payment system," 2016

[25] X. Zhang, Y. Han, W. Xu, and Q. Wang, "HOBA: A novel feature engineering methodology for credit card fraud detection with a deep learning architecture," *Information Sciences*, vol. 557, no. xxxx, pp. 302–316, 2021, doi: 10.1016/j.ins.2019.05.023.

[26] R. Praetsch, "Airlines need better anti-fraud data," Netherlands, Jan. 2019.

[27] J. Akhilomen, "Data Mining Application for Cyber Credit-Card Fraud Detection System," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 7987 LNAI, 2013, pp. 218–228. doi: 10.1007/978-3-642-39736-3_17.

[28] C. F. Barnhardt , David Wayne; Pigg, "Fraud Protection," 7575157, 2009

[29] S. Callanan, D. Ie, E. H. Stern, Y. Heights, N. Y. Us, and R. C. Weir, "CLICK-FRAUD PREVENTION," US 11/617,127, 2008

[30] A. Tselykh and D. Petukhov, "Web service for detecting credit card fraud in near real-time," in *Proceedings of the 8th International Conference on Security of Information and Networks*, Sep. 2015, vol. 08-10-Sep-, pp. 114–117. doi: 10.1145/2799979.2800039.

[31] R. Kemp, "Mobile payments: Current and emerging regulatory and contracting issues," *Computer Law and Security Review*, vol. 29, no. 2, pp. 175–179, 2013, doi: 10.1016/j.clsr.2013.01.009.

[32] A. Tella and I. Abdulmumin, "Predictors of Users' Satisfaction with E-payment System: a Case Study of Staff at the University of Ilorin, Nigeria," *Organizacija*, vol. 48, no. 4, pp. 272–286, 2015, doi: 10.1515/orga-2015-0018.

[33] S. Viaene and G. Dedene, "Insurance Fraud: Issues and Challenges," *Geneva Papers on Risk and Insurance: Issues and Practice*, vol. 29, no. 2, pp. 313–333, 2004, doi: 10.1111/j.1468-0440.2004.00290.x.

[34] M. A. Ali, M. A. Azad, M. Parreno Centeno, F. Hao, and A. van Moorsel, "Consumer-facing technology fraud: Economics, attack methods and potential solutions," *Future Generation Computer Systems*, vol. 100, pp. 408–427, Nov. 2019, doi: 10.1016/j.future.2019.03.041.

[35] R. A. Rahman and I. S. K. Anwar, "Effectiveness of Fraud Prevention and Detection Techniques in Malaysian Islamic Banks," *Procedia - Social and Behavioral Sciences*, vol. 145, pp. 97–102, 2014, doi: 10.1016/j.sbspro.2014.06.015.

[36] C. K. Ayo and W. I. Ukpere, "Design of a secure unified e-payment system in Nigeria : A case study," *African Journal of Business Management*, vol. 4, no. 9, pp. 1753–1760, 2010.

[37] B. Terry, "Understanding COVID-19'S Impact on The Airline Sector | Deloitte Global," 2020.

[38] L. Li, S. Das, R. J. Hansman, R. Palacios, and A. N. Srivastava, "Analysis of flight data using clustering techniques for detecting abnormal operations," *Journal of Aerospace Information Systems*, vol. 12, no. 9, pp. 587–598, 2015, doi: 10.2514/1.I010329.

[39] M. Zareapoor, Seeja. K. R. Seeja.K.R, and M. Afshar Alam, "Analysis on Credit Card Fraud Detection Techniques: Based on Certain Design Criteria," *International Journal of Computer Applications*, vol. 52, no. 3, pp. 35–42, 2012, doi: 10.5120/8184-1538.

[40] W. Taddesse and T. G. Kidan, "E-payment: Challenges and Opportunities in Ethiopia," *Economic commission for Africa*, no. October, pp. 1–59, 2005.

[41] G. Newman, S., & Sutter, "Electronic Payments—The Smart Card: Smart Cards, e-Payments, & Law—Part II," *Computer Law & Security Review*, vol. 18, no. 5, pp. 307–313, 2002.

[42] R. Kemp, "Mobile payments: Current and emerging regulatory and contracting issues," *Computer Law and Security Review*, vol. 29, no. 2, pp. 175–179, 2013, doi: 10.1016/j.clsr.2013.01.009.

[43] D. CURRY, "Mobile Payments App Revenue and Usage Statistics (2023)," *Business of Apps*, 2023. https://www.businessofapps.com/data/mobile-payments-app-market/ (accessed Mar. 25, 2023).

[44] M. Singh, "Fraud Detection in Payment Processing," 11/638,290, 2007

[45] H. S. Lallie *et al.*, "Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks during the Pandemic," *Computers & Security*, vol. 105, p. 102248, Jun. 2020, doi: 10.1016/j.cose.2021.102248.

[46] R. Y. Abdulahi and A. Y. Demisse, "Challenges of E-payment service in Commercial Bank of Ethiopia," *Proceedings - International Conference on Management and Service Science, MASS 2009*, pp. 1–4, 2009, doi: 10.1109/ICMSS.2009.5304469.

[47] G. Carmi and S. Y. Segal, "Mobile Security : a Review of New Advanced Technologies to Detect and Prevent E - Payment Mobile Frauds," *International Journal of Computer Systems*, vol. 292, no. 04, pp. 2394–1065, 2394.

[48] P. Katsaros, "A roadmap to electronic payment transaction guarantees and a Colored Petri Net model checking approach," *Information and Software Technology*, vol. 51, no. 2, pp. 235–257, 2009, doi: 10.1016/j.infsof.2008.01.005.

[49] A. Tella and I. Abdulmumin, "Predictors of Users' Satisfaction with E-payment System: a Case Study of Staff at the University of Ilorin, Nigeria," *Organizacija*, vol. 48, no. 4, pp. 272–286, 2015, doi: 10.1515/orga-2015-0018.

[50] A. Surekha, P. M. Rubesh Anand, and I. Indu, "E-payment transactions using encrypted QR codes," *International Journal of Applied Engineering Research*, vol. 10, no. 77, pp. 460–463, 2015.

[51] A. Seetharaman and J. R. Raj, "Evolution, Development and Growth of Electronic Money," *International Journal of E-Adoption (IJEA)*, vol. 1, no. 1, pp. 76–94, 2009, doi: 10.4018/jea.2009010106.

[52] C. Kim, W. Tao, N. Shin, and K. S. Kim, "An empirical study of customers' perceptions of security and trust in e-payment systems," *Electronic Commerce Research and Applications*, vol. 9, no. 1, pp. 84–95, 2010, doi: 10.1016/j.elerap.2009.04.014.

[53] J. L. Garcia, "Using technology to fight Fraud," *Health management technology*, vol. 23, no. 1, pp. 32–33, 2002.

[54] C. Wang and H. Zhu, "Representing Fine-Grained Co-Occurrences for Behavior-Based Fraud Detection in Online Payment Services," *IEEE Trans. Dependable and Secure Comput.*, vol. 19, no. 1, pp. 301–315, Jan. 2022, doi: 10.1109/TDSC.2020.2991872.

[55] S. Alwahaishi, V. Snášel, and A. Nehari-Talet, "Web site assessment in the airline industry: An empirical study of GCC airline companies," *2nd International Conference on the Applications of Digital Information and Web Technologies, ICADIWT 2009*, pp. 193–198, 2009, doi: 10.1109/ICADIWT.2009.5273863.

[56] A. Hedayati, "An analysis of identity theft : Motives, related frauds, techniques and prevention," *Journal of Law and Conflict Resolution*, vol. 4, no. January, pp. 1–12, 2012, doi: 10.5897/JLCR11.044.

[57] N. Malini and M. Pushpa, "Analysis on credit card fraud identification techniques based on KNN and outlier detection," *Proceedings of the 3rd IEEE International Conference on Advances in Electrical and Electronics, Information, Communication and Bio-Informatics, AEEICB 2017*, pp. 255–258, 2017, doi: 10.1109/AEEICB.2017.7972424.

[58] A. M. Al-Khatib, "Electronic Payment Fraud Detection Techniques," *World of Computer Science and Information Technology Journal (WCSIT)*, vol. 2, no. 4, pp. 137–141, 2012.

[59] W. Kou, *Payment Technologies for E-Commerce*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2003. doi: 10.1007/978-3-662-05322-5.

[60] K. A. Kaminski, T. Sterling Wetzel, and L. Guan, "Can financial ratios detect fraudulent financial reporting?," *Managerial Auditing Journal*, vol. 19, no. 1, pp. 15–28, Jan. 2004, doi: 10.1108/02686900410509802.

[61] D. Malekian and M. R. Hashemi, "An adaptive profile based fraud detection framework for handling concept drift," *2013 10th International ISC Conference on Information Security and Cryptology, ISCISC 2013*, 2013, doi: 10.1109/ISCISC.2013.6767338.

[62] M. Behzadian, R. B. Kazemzadeh, A. Albadvi, and M. Aghdasi, "PROMETHEE: A comprehensive literature review on methodologies and applications," *European Journal of Operational Research*, vol. 200, no. 1, pp. 198–215, Jan. 2010, doi: 10.1016/j.ejor.2009.01.021.

[63] A. Getaye, Temesgen; Addis, "Current Practices, Challenges and Prospects of Using Credit Cards as a Payment Method: The Case of Ethiopian Airlines Enterprise," *Journal of Business Research*, no. October, pp. 0–76, 2017.

[64] N. U. Shahid and N. J. Sheikh, "Proposed Framework for the Assessment of Business Intelligence Platforms for Medium-to-Large Hospitals Using Hierarchical Decision Modeling and Expert Judgments," *Open Journal of Business and Management*, vol. 10, no. 01, pp. 525–542, 2022, doi: 10.4236/ojbm.2022.101029.

[65] H Barham, T Daim, "The Use of Readiness Assessment for Big Data Projects Case of Smart City ", Sustainable Cities and Society, Vol 60, 2020

[66] M. G. Morgan, "Use (and abuse) of expert elicitation in support of decision making for public policy," *Proceedings of the National Academy of Sciences*, vol. 111, no. 20, pp. 7176–7184, May 2014, doi: 10.1073/pnas.1319946111.

[67] E Gibson, T Daim T and M Dabic " Evaluating University Industry Collaborative Research Centers", Technological Forecasting and Social Change, Volume 146, September 2019, Pages 181-202

[68] R. Handfield, S. V Walton, R. Sroufe, and S. A. Melnyk, "Applying environmental criteria to supplier assessment : A study in the application of the Analytical Hierarchy Process," *European Journal of Operational Research*, vol. 141, pp. 70–87, 2002.

[69] E. Garces, T. U. Daim, and M. Dabic, "Evaluating R&D Projects in Regulated Utilities: The Case of Power Transmission Utilities," *IEEE Trans. Eng. Manage.*, vol. 70, no. 2, pp. 533–553, Feb. 2023, doi: 10.1109/TEM.2021.3052857.

[70] R. Abotah and T. U. Daim, "Towards building a multi perspective policy development framework for transition into renewable energy," *Sustainable Energy Technologies and Assessments*, vol. 21, pp. 67–88, Jun. 2017, doi: 10.1016/j.seta.2017.04.004.

[71] D. F. Kocaoglu and M. Guven Iyigun, "Strategic R&amp;D program selection and resource allocation with a decision support system application," in *Proceedings of 1994 IEEE International Engineering Management Conference - IEMC '94*, pp. 225–232. doi: 10.1109/IEMC.1994.379926.

[72] J. R. Lavoie, T. Daim, and E. G. Carayannis, "Technology Transfer Evaluation: Driving Organizational Changes Through a Hierarchical Scoring Model," *IEEE Trans. Eng. Manage.*, vol. 69, no. 6, pp. 3392–3406, Dec. 2022, doi: 10.1109/TEM.2020.3042452.

[73] M. Khanam and T. Daim, "A market diffusion potential (MDP) assessment model for residential energy efficient (EE) technologies in the U.S.," *Renewable and Sustainable Energy Reviews*, vol. 144, p. 110968, Jul. 2021, doi: 10.1016/j.rser.2021.110968.

[74] H. Chen and D. F. Kocaoglu, "A sensitivity analysis algorithm for hierarchical decision models," *European Journal of Operational Research*, vol. 185, no. 1, pp. 266–288, 2008, doi: 10.1016/j.ejor.2006.12.029.

[75] T. L. Saaty, "A scaling method for priorities in hierarchical structures," *Journal of mathematical Psychology*, vol. 281, pp. 234–281, 1977.

[76] B. Barnes and T. Daim, "Information Security Maturity Model for Healthcare Organizations in the United States," *IEEE Trans. Eng. Manage.*, pp. 1–12, 2022, doi: 10.1109/TEM.2021.3139836.

[77] N. J. Webb, *The digital innovation playbook : creating a transformative customer experience*. New York, United States: John Wiley & Sons Inc, 2011.

[78] S. Alzahrani and T. U. Daim, "Evaluation of the cryptocurrency adoption decision using hierarchical decision modeling (HDM)," *PICMET 2019 - Portland International Conference on Management of Engineering and Technology: Technology Management in the World of Intelligent Systems, Proceedings*, pp. 1–7, 2019, doi: 10.23919/PICMET.2019.8893897.

[79] S. G. Dimmock and W. C. Gerken, "Predicting fraud by investment managers," *Journal of Financial Economics*, vol. 105, no. 1, pp. 153–173, Jul. 2012, doi: 10.1016/j.jfineco.2012.01.002.

[80] T. Turan, M. Amer, P. Tibbot, M. Almasri, F. Al Fayez, and S. Graham, "Use of Hierarchal Decision Modeling (HDM) for selection of graduate school for master of science degree program in engineering," in *PICMET '09 - 2009 Portland International Conference on Management of Engineering & Technology*, Aug. 2009, pp. 535–549. doi: 10.1109/PICMET.2009.5262107.

[81] H Alanazi H, T Daim, "Health Technology Diffusion: Case of Remote Patient Monitoring (RPM) for the Care of Senior Population", Technology in Society, 2021

[82] A Giadedi, T Daim, "A Scoring Model to Evaluate Offshore Oil Projects", Engineering Management Journal, 2021

[83] K. C. Justice, Scott C; Hopper, Eric L; Obrist, "FRAUD PREVENTION SYSTEMAND METHOD," 10/355,376, 2003

[84] N. Fernandes, "Economic effects of coronavirus outbreak (COVID-19) on the world economy Nuno Fernandes Full Professor of Finance IESE Business School Spain," *SSRN Electronic Journal, ISSN 1556-5068, Elsevier BV,* pp. 0–29, 2020.

[85] A. Tella, "Determinants of E-Payment Systems Success: A User's Satisfaction Perspective," *International Journal of E-Adoption*, vol. 4, no. 3, pp. 15–38, 2012, doi: 10.4018/jea.2012070102.

[86] A. R. Goetz and T. M. Vowles, "The good, the bad, and the ugly: 30 years of US airline deregulation," *Journal of Transport Geography*, vol. 17, no. 4, pp. 251–263, 2009, doi: 10.1016/j.jtrangeo.2009.02.012.

[87] P. S. Dempsey, "Airline Deregulation and Laissez-Faire Mythology: Economic Theory in Turbulence," *Journal of Air Law and Commerce*, vol. 56, no. 2, p. 305, 1990.

[88] H. V. Heuer, Jeffrey S.; Musette, "Airlines in the Wake of Deregulation: Bankruptcy as an Alternative to Economic Reregulation," *Transp. LJ*, vol. 19, p. 247, 1999.

[89] M. L. W. William W. Bratton, "THE POLITICAL ECONOMY OF FRAUD ON THE MARKET," *University of Pennsylvania Law Review*, vol. 160, no. 1, pp. 69–198, 2011.

[90] M. R. Albert, "E-buyer beware: Why online auction fraud should be regulated," *American Business Law Journal*, vol. 39, no. 4, pp. 575–644, 2002, doi: 10.1111/j.1744-1714.2002.tb00306.x.

[91] J. Gaurav, S. Tyagi, and J. Ranjan, "An Intuitive Approach to Prevent Smart Card Fraud using Fingerprinting Authentication and Enhanced Data Encryption Standard (EHDES)," *International Journal of Computer Applications*, vol. 40, no. 16, pp. 6–10, 2012, doi: 10.5120/5062-7222.

[92] C. Song, Alexander; Song, Yuh-Shen; Lew, "Anti-fraud financial transactions system.," 13/656,611, 2013

[93] P. S.-W. Fong and S. K.-Y. Choi, "Final contractor selection using the analytical hierarchy process," *Construction Management and Economics*, vol. 18, no. 5, pp. 547–557, Jul. 2000, doi: 10.1080/014461900407356.

[94] A. M. Aburbeian and H. I. Ashqar, "Credit Card Fraud Detection Using Enhanced Random Forest Classifier for Imbalanced Data," 2023, doi: 10.48550/ARXIV.2303.06514.

[95] E. Huang and F.-C. Cheng, "Online Security Cues and E-Payment Continuance Intention," *International Journal of E-Entrepreneurship and Innovation*, vol. 3, no. 1, pp. 42–58, Jan. 2012, doi: 10.4018/jeei.2012010104.

[96] C. P. Lee, M. Warkentin, and H. Choi, "The Role of Technological and Social Factors on the Adoption of Mobile Payment Technologies," *10th Americas Conference on Information Systems, AMCIS 2004*, pp. 2781–2786, 2004.

[97] E. Caldeira, G. Brandao, and A. C. M. Pereira, "Fraud analysis and prevention in e-commerce transactions," *Proceedings - 9th Latin American Web Congress, LA-WEB 2014*, no. 2004, pp. 42–49, 2014, doi: 10.1109/LAWeb.2014.23.

[98] R. Steennot, "Allocation of liability in case of fraudulent use of an electronic payment instrument: The new Directive on payment services in the internal market," *Computer Law & Security Review*, vol. 24, no. 6, pp. 555–561, Jan. 2008, doi: 10.1016/j.clsr.2008.09.005.

[99] A. Semester, "Consumer liability in case of fraud with electronic payment instruments : an analysis of European and Russian rules," vol. 2015, no. December, pp. 1–51, 2015.

[100] N. A. Hamidi, R. G. K. Mahdi, A. Nafarieh, A. Hamidi, and B. Robertson, "Personalized security approaches in E-banking employing flask architecture over cloud environment," *Procedia Computer Science*, vol. 21, pp. 18–24, 2013, doi: 10.1016/j.procs.2013.09.005.

[101] F Aldhaban, T Daim, R Harmon, "Technology Adoption in Emerging Regions: Case of the Smartphone in Saudi Arabia", International Journal of Innovation and Technology Management, Vol 17, No 1, 2020

[102] W. A. Al-Khater, S. Al-Maadeed, A. A. Ahmed, A. S. Sadiq, and M. K. Khan, "Comprehensive Review of Cybercrime Detection Techniques," *IEEE Access*, vol. 8, pp. 137293–137311, 2020, doi: 10.1109/ACCESS.2020.3011259.

[103] G. Lykou, A. Anagnostopoulou, and D. Gritzalis, "Smart airport cybersecurity: Threat mitigation and cyber resilience controls," *Sensors (Switzerland)*, vol. 19, no. 1, 2019, doi: 10.3390/s19010019.

[104] J. B. Ferris and R. Bass, "The design, implementation, assessment, and evaluation of a power systems protection laboratory curriculum," *ProQuest Dissertations and Theses*, p. 311, 2014.

[105] L. Glass, "'Smart' Technology: Do You Buy It? Adoption of Digital Innovations," Portland, OR, Jan. 2019. doi: 10.15760/etd.7137.

[106] H. Zhang, G. Weber, W. Zhu, and C. Thomborson, "B2B E-Commerce Security Modeling: A Case Study," in *2006 International Conference on Computational Intelligence and Security*, Nov. 2006, pp. 1549–1554. doi: 10.1109/ICCIAS.2006.295321.

[107] A. Mashatan, M. S. Sangari, and M. Dehghani, "How Perceptions of Information Privacy and Security Impact Consumer Trust in Crypto-Payment: An Empirical Study," *IEEE Access*, vol. 10, pp. 69441–69454, 2022, doi: 10.1109/ACCESS.2022.3186786.

[108] A. Shaygan and T. Daim, "Technology management maturity assessment model in healthcare research centers," *Technovation*, vol. 120, p. 102444, Feb. 2023, doi: 10.1016/j.technovation.2021.102444.

[109] R. I. Khalifa and T. U. Daim, "Project Assessment Tools Evaluation and Selection Using the Hierarchical Decision Modeling: Case of State Departments of Transportation in the United States," *J. Manage. Eng.*, vol. 37, no. 1, p. 05020015, Jan. 2021, doi: 10.1061/(ASCE)ME.1943-5479.0000858.

[110] B. Teh, M. B. Islam, N. Kumar, M. K. Islam, and U. Eaganathan, "Statistical and Spending Behavior based Fraud Detection of Card-based Payment System," *Proceedings - 2nd 2018 International Conference on Electrical Engineering and Informatics, ICELTICs 2018*, pp. 78–83, 2018, doi: 10.1109/ICELTICS.2018.8548878.

[111] A. Patel, W. Qi, and C. Wills, "A review and future research directions of secure and trustworthy mobile agent-based e-marketplace systems," *Information Management & Computer Security*, vol. 18, no. 3, pp. 144–161, Jul. 2010, doi: 10.1108/09685221011064681.

Sultan Alghamdi, received his Ph.D. degree in Technology Management from Portland State University, Portland, OR, USA. His research revolves mostly around the areas of e-payment, e-commerce, and fraud software. Currently, He is an assistant professor of Management Information System at Jeddah University, Jeddah, KSA.

Tugrul Daim received the M.S. degree in mechanical engineering from Lehigh University, Bethlehem, PA, USA, in 1991, and the M.S. degree in engineering management and the Ph.D. degree in systems science: engineering management from Portland State University, Portland, OR, USA, in 1994 and 1998, respectively. He leads a research group on Technology Evaluations and Research Applications. His group has had more than 25 Ph.D. graduates. He has authored more than 200 refereed journal papers, more than 20 special issues and more than 20 books. He made more than 200 conference presentations. He is the 5th Editor-in-Chief for the IEEE TRANSACTIONS ON ENGINEERING MANAGEMENT. Prior to that he had led the International Journal of Innovation and Technology Management for a decade and made it a well-known journal in the field. In addition, he was an Associate Editor for other journals including *Technological Forecasting and Social Change*, *Technology in Society*, and *Engineering Management Journal*.

Saeed Alzahrani received the Ph.D. degree in Technology Management from Portland State University, Portland, OR, USA. He is currently an assistant professor of Management Information System at Kings Saud University, Riyadh, KSA. His research interest in technology adoption, technology assessment, Technology innovation, and Fintech.