The Seybold REPORT

ISSN 1533-9211

INVESTIGATING THE INFLUENCE OF CYBERSECURITY ON CUSTOMER CONTENTMENT: AN EMPIRICAL EXAMINATION IN THE SERVICES OF KUALA LUMPUR INTERNATIONAL AIRPORT

NAZAHAN NAZRI

International Institute of Applied Science of Swiss School of Management.

Abstract

The abstract discusses the evolution of Malaysia's aviation sector, specifically the separation of the Department of Civil Aviation (DCA) into regulatory and operational entities in 1991. Malaysia Airports, established in 1992, focuses on airport operations while DCA remains the regulatory body. Malaysia Airports Holdings Berhad (KLIA) became the first airport operator in Asia listed on a stock exchange in 1999. The study focuses on the cyber security impact on customer satisfaction at Kuala Lumpur International Airport (KLIA), highlighting KLIA's diverse airport portfolio and its transformation into a multimodal destination. The empirical study conducted a cyber-security assessment of KLIA's ICT network, revealing the need for a comprehensive assessment to address vulnerabilities. The study emphasizes the importance of cyber security in KLIA's services and its role in enhancing customer satisfaction, proposing action plans under KLIA's Cyber Security Strategic Roadmap to improve cyber security maturity.

Keywords: Cyber Security, Customer Satisfaction, Kuala Lumpur International Airport, KLIA, Malaysia, ICT.

I. INTRODUCTION

The evolution of airport management and governance structures has been a subject of considerable interest within the broader context of the aviation industry. The case of Malaysia presents a unique paradigm shift in 1991 when the Malaysian Parliament enacted a bill leading to the separation of the Department of Civil Aviation (DCA) into two distinct entities [1].

The regulatory functions were entrusted to the DCA, maintaining its oversight of the airports and aviation industry in Malaysia. Simultaneously, Malaysia Airports emerged as a new entity in 1992, specifically designed to concentrate on the operational, managerial, and maintenance aspects of airports.

The incorporation of Malaysia Airports Holdings Berhad (KLIA) as a publicly listed company in 1999 marked a pivotal moment in the global aviation landscape [2]. KLIA's status as the first airport operator in Asia and the sixth worldwide to be listed on a stock exchange underscored its pioneering role. This financial restructuring set the stage for the transformation of Malaysia Airports into a unique player with a diverse portfolio of airports, encompassing international gateways, domestic airports, and short take-off and landing ports (STOLports) catering to rural and remote areas.

The distinctive characteristic of Malaysia Airports as the sole airport company with such a diverse airport portfolio place it in a league of its own. This evolution is not merely confined to administrative restructuring; it extends to a broader vision of redefining the role of airports.

ISSN 1533-9211

KLIA, as a flagship airport within the Malaysia Airports portfolio [3], is at the forefront of this transformation. The airport is actively positioning itself as a multimodal destination, seamlessly integrating cargo and logistics, aerospace, leisure, and customer services to enhance overall passenger satisfaction.

As airports globally transition into multifaceted hubs of economic and urban growth, the imperative for ensuring their cybersecurity becomes paramount. In the contemporary era, where airports rely extensively on Information and Communication Technology (ICT) networks, the vulnerabilities in cyberspace pose a significant threat to operational integrity and passenger safety [4]. The case of KLIA, being a trailblazer in the industry, brings forth the importance of cybersecurity in ensuring the resilience and security of airport operations.

This research paper contributes to the existing body of knowledge by addressing the critical intersection of cybersecurity and customer satisfaction in the aviation industry, with a specific focus on KLIA [5]. While existing literature recognizes the broader significance of cybersecurity in aviation, there is a noticeable gap in understanding its direct impact on customer satisfaction, especially in the context of a diversified airport operator like KLIA.

The empirical study embarked upon in this research aims to fill this gap by conducting an end-to-end cybersecurity assessment of KLIA's ICT network [6], with the objective of identifying and mitigating vulnerabilities that may compromise both operational efficiency and customer experience.

By examining KLIA's cybersecurity posture in the light of industry best practices, the study seeks to provide actionable insights for KLIA's Cyber Security Strategic Roadmap. The findings are expected to not only contribute to the enhancement of KLIA's cybersecurity maturity level but also serve as a benchmark for other airports navigating the complex terrain of securing digital infrastructure while maintaining a focus on customer satisfaction [7].

In essence, this literature review sets the stage for understanding the broader evolution of airport management, the unique case of Malaysia Airports, and the imperative of cybersecurity in the contemporary aviation landscape, paving the way for the empirical investigation outlined in the research abstract.

II. PROBLEM STATEMENT

Airports are critical infrastructure that plays a vital role in ensuring the safe and efficient movement of people and goods. However, with the increasing reliance on technology, Malaysian International Airport (KLIA) face a growing number of cybersecurity risks.

These risks can impact the safety and security of passengers and customers, as well as the operations of the airport itself.

The Seybold REPORT
ISSN 1533-9211

Here are some of the problems that passengers and customers can face due to KLIA airport cybersecurity issues [8], [9]:

1. Personal data breaches: Passengers and customers are required to provide personal information, such as their name, address, passport number, and payment details when booking flights or purchasing goods at the airport. If the airport's cybersecurity is compromised, this information could be stolen and used for identity theft or other fraudulent activities.
2. Flight disruption: Cyberattacks on airport systems can cause significant disruption to flight operations. For example, an attack on the airport's air traffic control system could cause delays or cancellations of flights, inconveniencing passengers and customers.
3. Airport security: Airport security is critical to ensuring the safety of passengers and customers. Cybersecurity vulnerabilities can potentially compromise physical security systems, such as CCTV cameras, access control systems, and perimeter security systems, putting the safety of people and assets at risk.
4. Malware and ransomware: Malware and ransomware attacks can infect airport systems, leading to data loss, system downtime, and financial loss. This could impact airport operations, disrupt services, and result in a loss of revenue.
5. Unauthorized access to networks and systems: Cyber attackers can gain unauthorized access to airport networks and systems, allowing them to steal data, manipulate systems, or launch further attacks. This could put sensitive information, such as flight schedules, passenger data, and airport infrastructure, at risk.
6. Cyberterrorism: The consequences of a cyberattack on an airport could be catastrophic. Cyberterrorists could disrupt airport operations, cause panic, and potentially harm passengers and customers.

Cybersecurity is a critical concern for KLIA as it can impact the safety, security, and operational efficiency of the airport. The potential consequences of a cybersecurity breach at an airport are significant and could impact the safety and well-being of passengers and customers. It is therefore essential for airports to invest in robust cybersecurity measures to protect against cyber threats and ensure the safety of all stakeholders.

III. LITERATURE REVIEW

Cybersecurity for airports is today more than ever a crucial issue. From protecting passengers and employees against acts of terrorism to enforcing governmental and local rules, airport security personnel must evolve in a fast-paced environment to mitigate security breaches and other critical security challenges.

1. Airport Security is Challenged by Many Different Factors

As a matter of fact, airport security is ensured through a complex whole of security, safety, communications and building automation factors that include [10]:

- Strict regulations (such as the NIS Directive on security of network and information systems) and policies that need to be addressed
- Ever-increasing need for operational efficiencies and reduction of operating costs
- Sharing of crucial data with other airport departments such as customs, police and airport operations
- Monitoring many different areas, i.e., airfields, hangars, terminals, parking areas, shops, restaurants, etc.
- Managing a wide variety of different access authorizations
- Protecting huge premises and extensive airport perimeters often located in residential or rural areas with poor lighting and limited means to monitor perimeter crossing, detect intrusion or potential breaches, filter out false alarms, detect object left behind, etc.

To compete and respond to these challenges, airports have raised their security relying on new innovations in IP-based video surveillance technology and advanced video analytics. Airport authorities have also enhanced their infrastructure to evolve in smart facilities [11]. As airports have raised their security and infrastructure to new heights, new challenges have come up.

Some other factors that challenge airport security include the constantly evolving threat landscape and the emergence of new security risks [12]. Cybersecurity threats have become increasingly prevalent, posing a significant risk to airport operations, data security, and passenger safety. The increasing use of connected devices and the internet of things (IoT) in airport infrastructure also presents new risks, as cybercriminals can exploit vulnerabilities in these systems to gain unauthorized access to sensitive data [13].

Airports also face challenges in managing the flow of passengers, luggage, and cargo through security checkpoints. Long wait times and inefficient processes can create bottlenecks, leading to frustration among passengers and increasing the risk of security breaches [14]. To address these challenges, airports are exploring new technologies such as biometrics, which can help streamline the security screening process and improve the passenger experience.

Additionally, geopolitical events and social unrest can also impact airport security, leading to increased levels of vigilance and heightened security measures [15]. Natural disasters such as earthquakes, floods, and hurricanes can also disrupt airport operations, potentially compromising security measures and exposing vulnerabilities.

In conclusion, airport security is a complex and multifaceted challenge that requires constant vigilance and innovative solutions [16]. As airports continue to evolve and adopt new technologies, they must also stay vigilant to new threats and risks, ensuring that their security measures are effective and resilient. By working collaboratively with stakeholders across the

The Seybold Report
ISSN 1533-9211

aviation industry, airports can continue to enhance their security and provide a safe and secure environment for passengers, employees, and stakeholders

2. Cybersecurity for Airports Provided by Vanguard NCM Solution

New physical and cybersecurity challenges have indeed emerged due to the increased use of smart devices in airport facilities. As airports have now a variety of ICT applications operating within their perimeter, the needs for both physical security and cyber security have increased and become more complicated [17]. Since cyber-attacks and incidental or malicious actions are new vulnerabilities in today's airports, cybersecurity for airports has become a key enabler for safety. Vanguard, Nelysis's Network Cyber Management solution, was specifically designed to help critical infrastructures such as airports to protect people and assets throughout the world.

Nowadays airports require specialized cybersecurity solutions to meet elevated threat levels. Vanguard, unlike other advanced cybersecurity solutions, was specifically designed for physical and network security to detect, recognize and mitigate incidental or malicious threats [18]. The unique selling points of this solution for cybersecurity for airports include [19]:

- Vanguard is a patent-based system designed by developers with in-depth experience in technological systems for the physical security world.
- Vanguard provides cybersecurity protection for the airport network (including IoT devices like perimeter sensors, access control devices, CCTV cameras, alarm and fire detection devices) without disrupting the integrity of the physical security and control networks.
- Vanguard protects the airport operational continuity because it warns and prevents against any sabotage or manipulation of any of security devices.
- Vanguard provides seamless IT/ security management reducing human factor mistakes. The system identifies and visualizes all the network elements to detect and identify behavior anomalies comparing the events against the initial baseline profile and presenting the network at a both logical and physical level. The security staff receives information and scoring rate about the different edge devices or sub-systems based on values such as the manufacturer name, the running operating system and firmware version, the used protocols and bandwidth, the number of flows, the IP address, the MAC address, the physical port on the network switch, etc.
- Since it is not based on digital signatures, Vanguard is able to detect new threats.
- Vanguard was designed for closed LANs (air gapped networks) and specifically optimized for Security IoT devices.
- Vanguard allows to store several months of traffic information for fast and easy built-in post-event analysis.

Vanguard NCM provides a comprehensive solution for cybersecurity for airports, addressing the unique security needs of airport infrastructure. The solution is specifically designed to protect both physical and network security, ensuring the safety and security of people and assets within the airport perimeter [20]. One of the key features of Vanguard NCM is its ability to provide cybersecurity protection for airport networks, including IoT devices such as perimeter sensors, access control devices, CCTV cameras, alarm and fire detection devices [21]. This protection is provided without disrupting the integrity of the physical security and control networks, ensuring the smooth and uninterrupted operation of airport security systems.

Vanguard NCM also provides seamless IT/security management, reducing the risk of human error and enabling security staff to quickly and easily identify and visualize all network elements, detect behavior anomalies, and compare events against the initial baseline profile [22]. The system presents the network at both a logical and physical level, allowing security staff to quickly identify and respond to potential threats. In addition to these features, Vanguard NCM is also designed to detect new threats, since it is not based on digital signatures. The solution is optimized for security IoT devices, and allows for the storage of several months of traffic information for easy post-event analysis [23]. Overall, Vanguard NCM is a powerful and effective solution for cybersecurity for airports, providing robust protection for both physical and network security, enabling airport operators to effectively manage the risks associated with cybersecurity threats, and ensuring the safety and security of passengers, employees, and assets within the airport perimeter.

3. Airport Service Quality and Customer Satisfaction

Customer satisfaction is always top of mind for airports. Unhappy or disengaged customers naturally mean fewer passengers and less revenue. It’s important that customers have an excellent experience every time they travel. Higher customer satisfaction increases customer loyalty, resulting in customers who are willing to purchase more and spend more on products and services [24].

Airport Service Quality (ASQ) is the world’s leading airport passenger service programme benchmarking customer satisfaction of services at the airport. ASQ provides objective measurement to help airports drive their performance and deliver competitive services to passengers. With the aim to help airports better assess their performance in passenger services and experience and understand passengers’ expectation, ASQ offers a wide range of products and surveys, including the signature ASQ Departure Survey, the Arrivals Survey, the Employee Survey for Customer Experience, the Commercial Survey and more [25].

As part of the programme, ASQ awards recognize airports that deliver the best experience in the opinion of their own passengers. The awards represent the highest possible recognition for airport operators around the world [26]. Airport members in Asia-Pacific and the Middle East are active participants in the programme demonstrating their dedication to consistently raise the bar in customer service excellence. Airport Service Quality (ASQ) is an important program that plays a critical role in assessing the performance of airports in terms of customer satisfaction. The ASQ program provides airports with objective measurement and benchmarking services to drive their performance and improve the services offered to passengers [27]. By participating in the ASQ program, airports can better assess their performance in passenger services and experience, and understand passengers' expectations.

ASQ offers a wide range of products and surveys, including the signature ASQ Departure Survey, the Arrivals Survey, the Employee Survey for Customer Experience, and the Commercial Survey, among others [28]. These surveys provide valuable insights into the passenger experience and can help airports identify areas for improvement. In addition to providing valuable measurement and benchmarking services, ASQ also recognizes airports that deliver the best experience in the opinion of their own passengers. The awards represent the highest possible recognition for airport operators around the world, and they serve as a testament to the dedication and commitment of airport operators to delivering exceptional customer service. Airports in Asia-Pacific and the Middle East are particularly active participants in the ASQ program, demonstrating their commitment to consistently raising the bar in customer service excellence [29]. By participating in the ASQ program, airports can improve customer satisfaction, enhance passenger loyalty, and ultimately drive revenue growth. In today's competitive marketplace, customer satisfaction is critical to the success of any airport, and the ASQ program provides a valuable tool for airport operators to meet and exceed the expectations of their passengers.

4. KLIA Cyber Security

The Malaysian Parliament passed a bill to separate the Department of Civil Aviation (DCA) into two entities with different spheres of responsibilities. DCA remains as the regulatory body for the airports and aviation industry in Malaysia whilst the newly created entity, Malaysia Airports, was established in 1992 to focus on the operations, management and maintenance of airports [30].

Malaysia Airports Holdings Berhad (KLIA) as the main Malaysian International Airport was thereafter incorporated as a public listed company in the Main Board of Bursa Malaysia Securities Berhad in 1999, which became the first airport operator in Asia and the sixth worldwide to be listed in a stock exchange [31]. Malaysia Airports is the only airport company with such a diverse airport portfolio, putting it in a league of its own. Airports under its stable of operations range from 5 international gateways, 16 domestic airports, to 18 short take-off and landing ports (STOLports) that serves the rural and remote areas in Malaysia [32]. Currently, KLIA is close to completing its second five-year business plan, Runway to Success 2020 (RtS2020), which charts its business direction for 2016 to 2020 [33-35]. RtS2020 places priority on establishing KLIA or KUL* as a preferred ASEAN hub, improving airport experience for all stakeholders, developing the acropolis, and expanding its presence overseas.

KLIA is redefining the role of airports as centres of economic and urban growth, developing them into multimodal destinations for cargo and logistics, aerospace as well as leisure and business. KLIA aims to create value through synergistic collaborations with its business partners and customers in order to achieve mutual benefit and provide solutions in terms of supply chain, human capital, infrastructure & equipment and technology as well as user experience [36-40]. However, for KLIA to be a more reliable partner and provide heightened user experience, it must first demonstrate that it is capable to ensure its own safety and security

The Seybold REPORT
ISSN 1533-9211

in cyberspace. As KLIA continues to expand its operations and services, it is essential that it prioritizes the safety and security of its customers and stakeholders in cyberspace [41-43]. Cybersecurity threats are a growing concern for airports around the world, and KLIA must take steps to protect its network and data from potential attacks.

To achieve this goal, KLIA must conduct a comprehensive cybersecurity assessment of its ICT network to identify vulnerabilities and mitigate potential threats. This assessment should include a review of current security policies and practices, an analysis of the network infrastructure, and a review of access controls and user permissions [44]. Once vulnerabilities have been identified, KLIA should take steps to address them, including implementing new security protocols and investing in advanced cybersecurity technologies [45]. This may include the use of advanced firewalls, intrusion detection and prevention systems, and advanced threat intelligence solutions. Additionally, KLIA should prioritize the training and education of its employees on cybersecurity best practices to ensure that they are equipped to identify and respond to potential threats [46]. Regular security audits and vulnerability assessments should also be conducted to ensure that the network is always up-to-date and protected against new and emerging threats [47]. By prioritizing cybersecurity, KLIA can enhance its reputation as a reliable and secure airport operator, and provide its customers and stakeholders with a heightened level of trust and confidence [48]. As the airport continues to grow and evolve, it must remain vigilant in its efforts to protect its network and data, and ensure that it is always up-to-date with the latest cybersecurity technologies and best practices.

IV. FINDINGS AND RESULTS

The gathering of data occurred prior to the Covid-19 conference and comprised a total of 4188 reviews that were handed in over the course of a year. Because the purpose of this research is to determine the nature of the relationship that exists between the variables of interest, the dataset was analysed in search of missing values in which at least one of the eight characteristics of the service was not rated. This may be the case, for example, because the passenger did not have the opportunity to experience the attribute, and as a result, they did not find it to be relevant to their review. After removing reviews that were incomplete in some way, the total number of reviews in the sample was 2278. Because of the nature of the question that was being investigated, it was necessary for the analysis to make use of variables that were rated on an objective scale. During the analysis, ten different variables were considered. At first, two variables, namely the overall satisfaction rating (SATIS) and whether the passenger would recommend the airport (RECO), were considered to be potential dependent variables. SATIS stands for "satisfaction," while RECO stands for "recommendation." The eight characteristics of the provided service were utilised as predictor variables. The predictor variables are labelled as follows: queueing times (QT), terminal cleanliness (TCL), terminal seating (TS), terminal signs and directions (TSD), cyber security (FB), airport shopping (SHP), airport Wi-Fi service (WF), and satisfaction with airport services (STF). Figure 1 illustrates these relationships.

ISSN 1533-9211

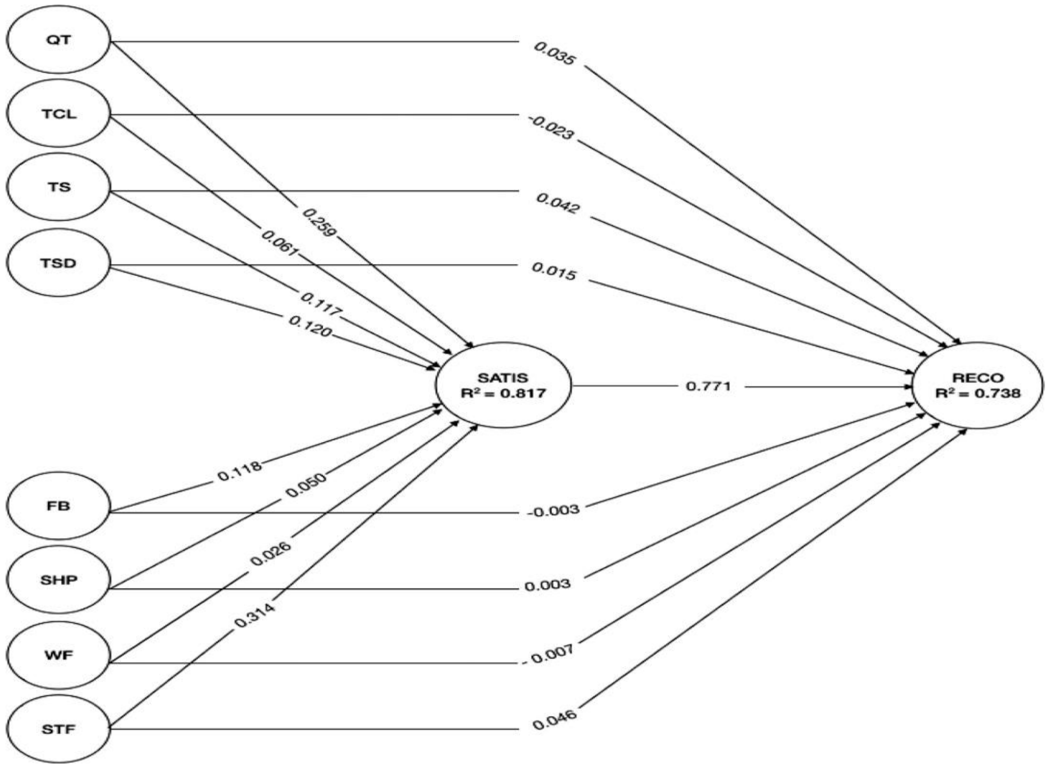

Figure 1: Structural Model

Because the analysis found that passengers' overall satisfaction fully mediated the effect of service attributes on their recommendation of KLIA airport services, the dependent variable for the evaluation of the effect of service failure carried out in this study was passengers' overall satisfaction. In light of this, the estimated model takes into consideration the eight aspects of the service in question as potential predictor variables, while the overall rating of satisfaction serves as the model's response variable. This study operationalizes the overall satisfaction rating given by reviewers as a proxy Net Promoter Score (NPS). This was done in light of the fact that online reviews play a significant role in the process of influencing prospective customers. The Net Promoter Score (NPS) is a metric that is utilised by a large number of businesses—for example, more than two-thirds of the companies that make up the Fortune 1000—to evaluate the level of satisfaction that exists within their customer relationships. Additionally, the NPS serves as a predictor of the expansion of KLIA's cyber security services.

Additionally, airports of varying sizes across Malaysia make extensive use of it. Because previous research has shown a strong correlation between the two measures (for example, see Eger & Micak, 2017), the decision to use the overall satisfaction rating as a proxy for NPS was made because of this correlation.

The Seybold Report
ISSN 1533-9211

The overall satisfaction rating was broken down into three categories, each of which was based on the NPS classification:

(1) Promoters (score of nine to ten),

(2) Passives (score of seven to eight), and

(3) Detractors (score of one to six).

Promoters are devoted enthusiasts who will continue to use the airport and refer others, thereby contributing to the expansion of the business. Passengers who are satisfied with the airport may recommend it to others, but they are typically less enthusiastic than promoters and are more susceptible to being won over by alternative options. People who aren't happy with the airport are likely to spread unfavourable word of mouth about it, which will be detrimental to the airport's reputation and could slow down its expansion. After identifying the dependent and independent variables, the current chapter of this thesis addresses the research questions presented in the first chapter of this thesis by conducting an investigation into the likelihood of a passenger being satisfied with the cyber security services provided by KLIA. The analysis will be presented in the following section. To determine the effect of cyber security service failure, this study uses a standard multinomial logit model to compute the probability of a passenger being passive or a promoter given that a particular service attribute fails while all other factors are kept constant.

Table 1: Results of the Structural Model Estimation

	Direct effects			Indirect effects		
Variables	Coefficient	t statistic	p value	Coefficient	t statistic	p value
QT - > RECO	0.035	1.532	0.126^{ns}	0.091	5.797	0.000***
TCL - > RECO	−0.023	1.159	0.247 ^{ns}	0.200	12.247	0.000***
TS - > RECO	0.042	1.823	0.068*	0.038	2.535	0.011**
TSD - > RECO	0.015	0.740	0.460 ^{ns}	0.242	13.185	0.000***
FB - > RECO	−0.003	0.117	0.907 ^{ns}	0.047	3.409	0.001***
SHP - > RECO	0.003	0.136	0.892 ^{ns}	0.090	5.624	0.000***
WF - > RECO	−0.007	0.391	0.696 ^{ns}	0.092	6.962	0.000***
STF - > RECO	0.046	1.805	0.071*	0.020	1.833	0.067*
STF - > SATIS	0.314	15.662	0.000***			
QT - > SATIS	0.259	14.012	0.000***			
TCL - > SATIS	0.061	3.470	0.001***			
TS - > SATIS	0.117	5.791	0.000***			
TSD - > SATIS	0.120	7.108	0.000***			
FB - > SATIS	0.118	6.021	0.000***			
SHP - > SATIS	0.050	2.554	0.011**			
WF - > SATIS	0.026	1.850	0.064*			
STF - > SATIS	0.314	15.662	0.000***			
	SATIS	RECO				
R^2	0.817	0.738				
R^2 Adjusted	0.816	0.737				
Q^2	0.799	0.719				
SRMR	0.000					
N	2278					

Note: *** significant at $p \leq .01$; ** significant at $p \leq .05$; * significant at $p \leq .10$; ^{ns} not significant.

Two reasons guided the choice of using a multinomial logit model versus alternatives such as ordered logit or probit models. Firstly, operationalization of the dependent and independent variables in this study required transformation: a five-point rating of service attributes into the

The Seybold REPORT
ISSN 1533-9211

zone of non-affection (score of one to three) and zone of affection (score of four to five), and a ten-point rating of overall satisfaction into detractors (score of one to six), passives (score of seven to eight), and promoters (score of nine to ten). While the categories (whose selection is based on extant literature), appear to be ordinal in nature, the underlying

Descriptive statistics for key variables are provided in Tables 2 and 3. Most of the reviews are by leisure versus business passengers, passengers departing and/or arriving versus transiting at the KLIA airport, and passengers at non-homeland versus homeland airports. On average, passengers are fairly neutral or dissatisfied with their experience of cyber security service attributes (with means of 2.37 to 2.91 on a five-point scale, with one being least satisfied and five being most satisfied). This is also reflected by the higher proportion of service failure.

The average overall satisfaction rating of 3.85 (on a scale of one to ten, with one being least satisfied and ten being most satisfied) further emphasizes the general level of dissatisfaction with airports. Three-quarters of reviews are categorized as detractors and only 13% as promoters.

Table 2: Descriptive Statistics for Control Variables

Control variable	Frequency	Percent
Purpose of travel	2278	100
-Leisure	1759	77.2
-Business	519	22.8
Trip type	2278	100
-Arrival and/or departure	1984	87.1
-Transit	294	12.9
Homeland airport	2278	100
-No	1370	60.1
-Yes	908	39.9
Airport location	2278	100
-Africa	67	2.9
-Asia Pacific	476	20.9
-Europe	1261	55.4
-Latin America/Caribbean	40	1.8
-Middle East	151	6.6
-North America	283	12.4
Size of airport	2275	100
-Small	298	13.1
-Medium	827	36.4
-Large	1150	50.5

Table 3: Descriptive Statistics for Predictor and Response Variables

Predictor variables	Mean	Std. Error	Std. Dev.	Service failure (%)	Service success (%)	
Queueing times (QT)	2.37	0.032	1.521	72.2	27.8	
Terminal cleanliness (TCL)	2.91	0.030	1.454	61.5	38.5	
Terminal seating (TS)	2.43	0.030	1.429	74.0	26.0	
Terminal signs and directions (TSD)	2.89	0.031	1.459	62.0	38.0	
Food and beverages (FB)	2.44	0.029	1.368	75.4	24.6	
Airport shopping (SHP)	2.49	0.029	1.371	74.2	25.8	
Airport wifi service (WF)	2.60	0.031	1.495	69.0	31.0	
Airport staff (STF)	2.43	0.031	1.496	71.1	28.9	
Response variable	Mean	Std. Error	Std. Dev.	Detractors (%)	Passives (%)	Promoters (%)
Overall satisfaction (SATIS)	3.85	0.064	3.077	74.9	12.0	13.0

Inferential Statistics

Inferential Statistics Model estimation results are shown in Table 4. Nagelkerke's rho- squared is used to evaluate model fit, which at 74.9% for the model without controls and 75.3% for the model with controls, suggests that a high proportion of the variation in the response variable is explained by the predictor variables.

Probabilities for each predictor variable are reported in Table 4. These probabilities quantify the likelihood of a reviewer being passive (P (pass)) or a promoter (P (prom)) when they have experienced service failure with a particular attribute. For the model without control variables, results show that when a passenger has cyber security experienced failure in KLIA with any of the eight service attributes then the probability of that passenger being a promoter becomes significantly small, ranging from 0.033 for airport staff to 0.154 for airport shopping.

The Seybold REPORT

ISSN 1533-9211

Table 4: Model Estimation

	Passives (pass)			Promoters (prom)		
	Coefficient	Sig.	$P_{(pass)}$	Coefficient	Sig.	$P_{(prom)}$
QT	−1.120	0.000***	0.232	−2.528	0.000***	0.057
TCL	−1.153	0.000***	0.218	−2.025	0.000***	0.091
TS	−0.770	0.000***	0.273	−1.460	0.000***	0.137
TSD	−1.604	0.000***	0.149	−1.912	0.000***	0.110
FB	−0.816	0.001***	0.274	−1.772	0.000***	0.105
SHP	−0.099	0.679^{ns}	0.444	- 0.959	0.003***	0.154
WF	−0.119	0.547 ^{ns}	0.400	−1.101	0.000***	0.150
STF	−1.556	0.000***	0.169	−3.202	0.000***	0.033
Intercept	2.218	0.000***		3.709	0.000***	

Cox and Snell rho-squared (ρ^2): 0.577
Nagelkerke rho-squared (ρ^2): 0.749
McFadden rho-squared (ρ^2): 0.585
Number of observations: 2278
- 2 log-likelihood: 553.031***

Model 2 (with control variables)

	Passives (pass)			Promoters (prom)		
	Coefficient	Sig.	$P_{(pass)}$	Coefficient	Sig.	$P_{(prom)}$
QT	−1.106	0.000***	0.235	−2.536	0.000***	0.056
TCL	−1.104	0.000***	0.225	−1.950	0.000***	0.097
TS	−0.729	0.000***	0.281	−1.449	0.000***	0.137
TSD	−1.640	0.000***	0.145	−1.947	0.000***	0.107
FB	−0.832	0.001***	0.272	−1.794	0.000***	0.104
SHP	0.062	0.802^{ns}	0.437	−0.996	0.003***	0.152
WF	−0.146	0.463^{ns}	0.397	−1.171	0.000***	0.143
STF	−1.583	0.000***	0.165	−3.207	0.000***	0.032
Purpose of travel[a]						
-Leisure	0.423	0.070*	0.381	0.393	0.194^{ns}	0.370
Trip type[b]						
-Transit	−0.081	0.807^{ns}	0.267	0.426	0.307^{ns}	0.443
Homeland airport[c]						
-Yes	−0.153	0.444^{ns}	0.300	−0.001	0.997^{ns}	0.350
Airport location[d]						
-Africa	−0.552	0.482^{ns}	0.201	0.251	0.816^{ns}	0.449
-Asia-Pacific	0.355	0.133^{ns}	0.392	0.192	0.539^{ns}	0.333
-North America	0.298	0.322^{ns}	0.406	−0.033	0.940^{ns}	0.292
-L.Am/Carib.	−1.428	0.080**	0.128	−0.459	0.610^{ns}	0.338
-Middle East	0.057	0.887^{ns}	0.351	−0.039	0.938^{ns}	0.318
Airport size[e]						
-Medium	−0.463	0.122^{ns}	0.297	−0.717	0.081*	0.231
-Large	−0.473	0.114^{ns}	0.278	−0.487	0.226^{ns}	0.275
Intercept	2.261	0.000***		3.851	0.000***	

Cox and Snell rho-squared (ρ^2): 0.581
Nagelkerke rho-squared (ρ^2): 0.753
McFadden rho-squared (ρ^2): 0.590
Number of observations: 2278
- 2 log-likelihood: 1152.744***

For all eight service attributes, results show a relative increase in the probability of the passenger being passive versus promoting, but the probabilities remain significantly low. The values of P (prom) are plotted in Figure 2 to illustrate the relative importance of the cyber security service attributes. It is clear that airport cyber security services and KLIA staff have the highest impact on turning passengers into promoters followed by queueing times. The other attributes have more or less the same impact.

The Seybold REPORT
ISSN 1533-9211

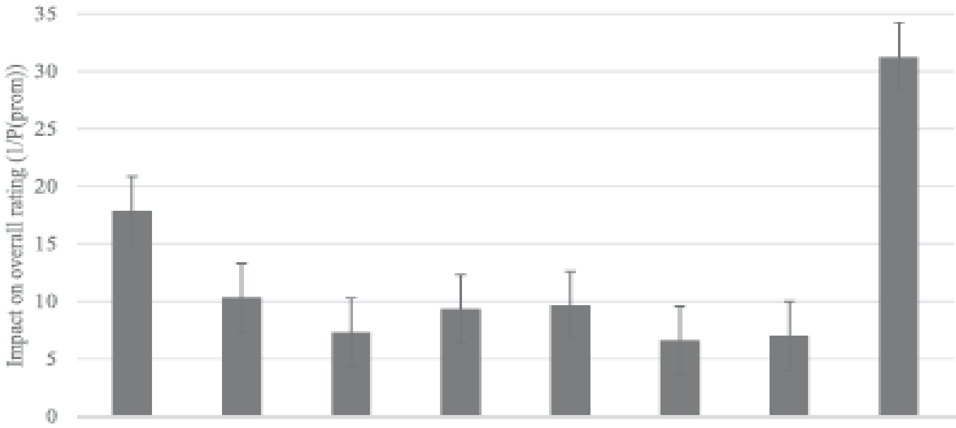

Figure 2: Relative Magnitude of the Impact of Service Attributes on Turning Passengers into Promoters

Results for the model with control variables show that leisure passengers are more likely to be passives compared to business passengers, however, when it comes to promoters, there is no significant difference between them. Purpose of travel and homeland airport do not have significant effects. Differences between all other airport regions and Europe are not significant, and there is no significant difference between regions regarding the probability of a passenger being a promoter. Passengers at medium-sized airports are less likely to be promoters compared to passengers at small airports, and there is no significant difference between passenger's at large airports and those at small airports in Malaysia. Despite the noted effects, and results of the Likelihood Ratio test, Table 5 shows that, in general, the control variables do not add a significant explanation to whether a passenger is passive or a promoter versus a detractor.

Table 5: Likelihood Ratio Tests

	Model fitting criteria	Likelihood Ratio tests		
Effect	−2 log likelihood of reduced model	Chi-square	df	Sig.
Intercept	1152.744	0.000	0	
QT	1225.448	72.704	2	0.000***
TCL	1183.507	30.762	2	0.000***
TS	1175.982	23.238	2	0.000***
TSD	1213.345	60.600	2	0.000***
FB	1183.308	30.564	2	0.000***
SHP	1167.051	14.307	2	0.001***
WF	1172.662	19.918	2	0.000***
STF	1259.022	106.278	2	0.000***
Trip type	1156.163	3.418	2	0.181^{ns}
Purpose of travel	1154.989	2.244	2	0.326^{ns}
Homeland airport	1153.628	0.884	2	0.643^{ns}
Airport location	1161.749	9.005	10	0.532^{ns}
Airport size	1156.993	4.249	4	0.373^{ns}

V. DISCUSSION

Cyber security services at KLIA are essential to ensure the safety and security of passengers, employees, and airport infrastructure. With the increasing use of technology and digitalization in the aviation industry, the risk of cyber threats and attacks has also increased. Cyber security services help to prevent and mitigate these threats, which can have serious consequences such as flight delays, cancellations, and even safety risks. In terms of passenger and customer satisfaction, the effectiveness of cyber security services at airports can have a significant impact. Passengers expect to feel safe and secure when traveling, and any perceived weakness in cyber security can undermine their confidence in the airport and the aviation industry as a whole. On the other hand, effective cyber security measures can enhance customer satisfaction by demonstrating the airport's commitment to safety and security. Overall, cyber security services are crucial for the smooth and safe operation of airports, and their impact on passenger and customer satisfaction should not be underestimated.

The Airport Operations Centre, also known as APOC, is an extremely vital facility. Even if the APOC is only offline for two hours, passengers can expect flight delays or even cancellations; the consequences of such disruptions can, of course, have a significant impact. Collaborative Decision Making (also known as CDM) and the Airport Operations Plan (also known as AOP) are at the core of APOC; consequently, anything that affects CDM and AOP falls under the purview of the guidance and recommendations contained in this report. If the availability and integrity of data and/or systems can be compromised, the APOC is very vulnerable to losing its credibility.

- Given the current legacy systems and services, airports may very well build APOC and CDM on top of untrustworthy, unauthenticated data sources and insecure networks. This is one of the particular cyber-problems facing the APOC. If the APOC is built on such a foundation, it will be impossible to establish trust in the organisation. For this reason, it is essential to provide an explanation of how the risks associated with these legacy systems will be reduced in the near future. It is necessary, for the medium term, to create a road map that explains how insecure legacy systems will be replaced with newer, more modern ones.
- System integration more frequently results in extended supply chains, in which each stakeholder relies on services provided by their partners, but which may be delivered by companies that are not directly affiliated with the original partners. When the supply chain is extended, more people will have access to the core infrastructures, which increases the possibility of security breaches. While it is possible to outsource certain services, this cannot be done with regard to the risk of cyberattacks.
- Even if the systems that make up airport control can be adequately protected, the assurance process still needs to be expanded to include all of the data's sources. It is necessary to have faith in the endpoints of connections; in the event that these cannot be trusted, problems will emerge. The scenario in which a communication service is used to inject false data, which then affects the entire aviation community, has been identified as the most dangerous possible outcome. Even though it is possible to "unplug" the affected service, this will still

be a solution that will reduce the capability of stakeholders to exchange data with the airport APOC as well as other APOCs located throughout Europe (since the • Network Operations Plan (NOP) will not be updated from the airport AOP).

If the issues of today are not resolved, we will be forced to confront a "dystopian future" that is fraught with high cyber risk and an inability to fully take advantage of the modernization and benefits that SESAR promises. The worst-case scenario is that assailants continue to improve their level of expertise, airports are frequently disrupted, and as a result, the travelling public suffers the consequences.

It is possible to find solutions to these issues and work towards a more utopian future in which advances in technology and data drive improvements in performance for everyone. As is the case more generally with SESAR research and development, there is an opportunity to address cyber-security in a methodical and coordinated manner that enables (but does not guarantee) the security functionality, assurance, and operating environment. For SESAR solutions, this most directly entails incorporating appropriate security requirements from the very beginning of the development process. Additionally, improvement in industrialization and deployment will result from improved work and coordination on standardised and unified security architectures.

1. Key Technical Controls required for an APOC Include Intrusion

Prevention and detection, data diodes (to protect read-only data, such as that relating to passengers), logging and auditing capabilities, device and service authentication, and data validation tools (which will also support general robustness for airports) are some of the features that should be implemented. Zoning and network separation will be limited because of the APOC's position as the "nerve centre," and because there will only be a single logical platform and data repository. However, they should be applied wherever possible. One approach that shows promise is the combination of organisational cyber-maturity assessments with more detailed metrics for the CyberSA of key APOC stakeholders, both on an individual and a team level. To accurately measure CyberSA on both an individual and a collective scale, Key Performance Indicators (KPIs) that are both detailed and dynamic are required.

In the end, trust is made possible thanks to security assurance, which results from the activities of developers, implementers, and assessors of security functionality; in particular, this occurs through structured design processes, documentation, and testing. Due to the high level of business criticality associated with APOCs, a high level of assurance is required, and as a result, the process, system, and environment aspects need to be addressed. Technical competence, openness and transparency to external assessment and criticism, self-awareness, and honesty are some of the practical-level characteristics that foster trust.

The legal and regulatory requirements that are in place now and those that are planned for the future do not define security assurance methods or a level of assurance for APOCs in a stringent manner. On the other hand, upcoming modifications to ECAC Doc 30 should introduce a set of auditable requirements (including an audit scheme) for cyber-security. These requirements should eventually provide a strong mandate for airports, including APOCs, to adequately address the majority of cyber risks. In order to combat threats posed by nation states, also known as highly capable and tenacious attackers, additional support from national authorities is required.

2. Framework for Aviation Cyber Security

The following framework has been drafted to address the expansive topic of cybersecurity for aviation:

- Develop common cyber standards for aviation systems Organisations such as the National Institute of Standards and Technology (NIST), the International Organisation for Standardisation (ISO), and others are collaborating with providers of critical infrastructure to develop information security and cyber protection standards for critical infrastructure. Participation in these activities in a constructive manner is essential if one is to ensure that the specific requirements of aviation are taken into consideration during the process of standardisation.
- Ensure a cybersecurity culture: The same discipline that was used to achieve aviation's high safety standard must also be applied to the process of developing a common vision, common strategy, goals, and definitions, as well as a common framework and roadmap for addressing the evolving threats. This is necessary in order to ensure that cybersecurity is taken seriously.
- Have a good understanding of the danger: In order to effectively plan our defences, the aviation community needs to have a common understanding of the actors, as well as their motivations and intentions. Our adversaries are planning their cyberattacks in creative and unconventional ways, and we need to do the same if we want to stop them.
- Gain an understanding of the risk: It is essential for the aviation industry to determine the components of the aviation system that require protection in order to successfully manage the cyber risk. The aviation system is a large and complicated international entity, and there are many different stakeholders. Understanding the interactions of the system is going to be a slow and methodical process that will require some time.
- Communicate the threats and ensure situational awareness: It is important that the government and industry share threat and mitigation data in order to increase the speed at which threats are mitigated across the aviation system.
- Communicate the threats and ensure situational awareness. The Critical Infrastructure Partnership Advisory Council, also known as CIPAC, is a forum where industry stakeholders and the United States government can discuss sensitive matters pertaining to aviation security. Cyberthreats to the aviation industry are also global in scope and have implications on a global scale. As a result, there is a necessity for the establishment of systems that allow for the exchange of data with the international aviation community.
- Respond to incidents and have an understanding of the timeliness requirements for doing so The aviation community needs to have an understanding of the timeliness requirements for responding to threats. Different events dictate different response times. A change to the

The Seybold Report
ISSN 1533-9211

software of an aircraft, for instance, requires a great deal more testing, certification, and approvals than a change to the software of a ticketing system does, which means that the latter can be implemented more quickly. Within the context of the response framework, these limitations need to be taken into consideration. In order to respond appropriately to an attack in a timely manner, processes, methods, and standards need to differentiate the requirements of each aviation subsystem.

- Work to improve the defensive structure by: Additionally, the industry is responsible for implementing systems and standards that will safeguard the components that make up the aviation system. In order to accomplish this, the interfaces between the major subsystems as well as the subsystem itself need to be protected.
- Specify design principles The design principles that guided the development of the Internet opened the door for potential adversaries to exploit those vulnerabilities. Aviation needs to define design principles for its networks and control systems that take into account the ever-evolving cybersecurity threat and make sure there are no silent failures. This is necessary because the cyber domain is continuing to expand. This would include the identification of architectures and design principles that protect critical systems and platforms against known attack methods. Additionally, this would include making certain that aviation systems are secure by default and are resilient against unknown threat scenarios.
- Specify the operational principles: These guidelines concentrate on the operational facets of the systems that are put into action in the field. This would ensure that our systems and platforms are resilient by having a robust cyber culture, operational standards, and best practises that mitigate threats to our systems and platforms.
- Conduct the necessary research and development: The aviation community needs to focus its resources on researching and developing appropriate design and perational principles, such as: o creating secure and resilient system architectures, including methods for maintaining secure data transfer, isolating critical data, and effectively recovering from attacks; o improving attack detection; and o ensuring forensic readiness.
- Ensure that government and industry work together: The aviation community needs to make sure that both the government and the private sector collaborate on this issue. In order to coordinate the national aviation cybersecurity strategies, policies, and plans, a framework should be established that includes both the government and industry. This would involve things like: o establishing policy for near-term and long-term developments in cybersecurity; o defining internationally accepted rules of behaviour; o enforcing consequences for inappropriate behaviour; and o positioning cybersecurity as a high priority on the diplomatic agenda.

VI. CONCLUSION AND RECOMMENDATIONS

The relentless pursuit of innovation in commercial aviation has resulted in a level of reliability and safety that has never been seen before, as well as a world that is confident in the robustness, vigilance, efficiency, and resiliency of the global aviation system. Nevertheless, the system of

The Seybold Report
ISSN 1533-9211

global aviation is currently at a crossroads. The increased use of information and communication technology across the aviation industry creates a more interconnected global aviation system. To maintain consumers' faith in the aviation industry, it is necessary to have a comprehensive understanding of the implications brought about by the increased connectivity and dependence on information and communication technologies (ICT).

The aviation community is in a one-of-a-kind position to effectively manage risks to its individual operations and assets, as well as to identify effective strategies to make those things more secure and resilient. Nevertheless, there is not yet a standardized road map or an international policy regarding cybersecurity in the commercial aviation industry. It is imperative that the aviation community develop a common framework for governing the various components of the aviation system in order to keep this high degree of confidence at a consistent level. Additionally, a partnership between the government and the industry is required in order to proactively thwart threats to the aviation industry and to strengthen the aviation system's resilience against attacks.

Recommendations

In light of the constantly shifting nature of cyber risks, the aviation community is obligated to pursue the following course of action:

- Increase the cooperation and focus within the aviation community, with the active participation of all major industry players;
- Leverage, extend, and apply the existing industry best practises, the response team, and the research and education efforts that are under way;
- Implement a common cybersecurity vision, strategy, goals, and framework to address evolving threats.
- Include the relevant government agencies in the conversation;
- Commence the Construction of a Roadmap by Identifying Near-Term, Mid-Term, and Long-Term Actions; and
- Establish a Framework for Government and Industry to Coordinate National Aviation Cybersecurity Strategies, Policies, and Plans.

References

1) ACI (Airports Council International). (2020b). ASQ survey – methodology. Available at: https://aci.aero/customer-experience-asq/services/asq-departure-survey/meth odology/ (accessed 5 June 2020).

2) ACI (Airports Council International). (2020c). ACI introduces new Airport Service Quality questions related to COVID-19. Available at: https://aci.aero/news/2020/ 07/14/aci-introduces-new-airport-service-quality-questions-related-to-covid-19/ (accessed 20 April 2020).

3) Akama, J. S., & Kieti, D. M. (2003). Measuring tourist satisfaction with Kenya’s wildlife safari: A case study of Tsavo west National Park. Tourism Management, 24(1), 73–81. https://doi.org/10.1016/S0261-5177(02)00044-4.

4) Brito, J., & Castillo, A. (2019). Bitcoin: A Primer for Policymakers. Mercatus Research, Mercatus Center at George Mason University.

5) Y. M. A. Tarshany, Y. Al Moaiad and Y. A. Baker El-Ebiary, "Legal Maxims Artificial Intelligence Application for Sustainable Architecture And Interior Design to Achieve the Maqasid of Preserving the Life and Money," 2022 Engineering and Technology for Sustainable Architectural and Interior Design Environments (ETSAIDE), 2022, pp. 1-4, doi: 10.1109/ETSAIDE53569.2022.9906357.

6) W. A. H. M. Ghanem et al., "Cyber Intrusion Detection System Based on a Multiobjective Binary Bat Algorithm for Feature Selection and Enhanced Bat Algorithm for Parameter Optimization in Neural Networks," in IEEE Access, vol. 10, pp. 76318-76339, 2022, doi: 10.1109/ACCESS.2022.3192472.

7) Y. A. Baker El-Ebiary et al., "Blockchain as a decentralized communication tool for sustainable development," 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE), 2021, pp. 127-133, doi: 10.1109/ICSCEE50312.2021.9497910.

8) Y. A. Baker El-Ebiary et al., "Track Home Maintenance Business Centers with GPS Technology in the IR 4.0 Era," 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE), 2021, pp. 134-138, doi: 10.1109/ICSCEE50312.2021.9498070.

9) S. I. Ahmad Saany et al., "Exploitation of a Technique in Arranging an Islamic Funeral," 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE), 2021, pp. 1-8, doi: 10.1109/ICSCEE50312.2021.9498224.

10) J. A. Jusoh et al., "Track Student Attendance at a Time of the COVID-19 Pandemic Using Location-Finding Technology," 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE), 2021, pp. 147-152, doi: 10.1109/ICSCEE50312.2021.9498043.

11) Y. A. Baker El-Ebiary et al., "E-Government and E-Commerce Issues in Malaysia," 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE), 2021, pp. 153-158, doi: 10.1109/ICSCEE50312.2021.9498092.

12) Y. A. B. El-Ebiary et al., "Determinants of Customer Purchase Intention Using Zalora Mobile Commerce Application," 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE), 2021, pp. 159-163, doi: 10.1109/ICSCEE50312.2021.9497995.

13) S. Bamansoor et al., "Efficient Online Shopping Platforms in Southeast Asia," 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE), 2021, pp. 164-168, doi: 10.1109/ICSCEE50312.2021.9497901.

14) S. Bamansoor et al., "Evaluation of Chinese Electronic Enterprise from Business and Customers Perspectives," 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE), 2021, pp. 169-174, doi: 10.1109/ICSCEE50312.2021.9498093.

15) A. Altrad et al., "Amazon in Business to Customers and Overcoming Obstacles," 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE), 2021, pp. 175-179, doi: 10.1109/ICSCEE50312.2021.9498129.

16) Y. A. Baker El-Ebiary et al., "Mobile Commerce and its Apps - Opportunities and Threats in Malaysia," 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE), 2021, pp. 180-185, doi: 10.1109/ICSCEE50312.2021.9498228.

17) M. B. Mohamad et al., "Enterprise Problems and Proposed Solutions Using the Concept of E-Commerce," 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE), 2021, pp. 186-192, doi: 10.1109/ICSCEE50312.2021.9498197. IEEE Explore, Scopus

18) P. R. Pathmanathan et al., "The Benefit and Impact of E-Commerce in Tourism Enterprises," 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE), 2021, pp. 193-198, doi: 10.1109/ICSCEE50312.2021.9497947.

19) K. Aseh et al., "The Future of E-Commerce in the Publishing Industry," 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE), 2021, pp. 199-205, doi: 10.1109/ICSCEE50312.2021.9498175.

20) S. M. S. Hilles et al., "Latent Fingerprint Enhancement and Segmentation Technique Based on Hybrid Edge Adaptive DTV Model," 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE), 2021, pp. 8-13, doi: 10.1109/ICSCEE50312.2021.9498025.

21) S. M. S. Hilles et al., "Adaptive Latent Fingerprint Image Segmentation and Matching using Chan-Vese Technique Based on EDTV Model," 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE), 2021, pp. 2-7, doi: 10.1109/ICSCEE50312.2021.9497996.

22) S. T. Meraj et al., "A Diamond Shaped Multilevel Inverter with Dual Mode of Operation," in IEEE Access, vol. 9, pp. 59873-59887, 2021, doi: 10.1109/ACCESS.2021.3067139.

23) Mohammad Kamrul Hasan, Muhammad Shafiq, Shayla Islam, Bishwajeet Pandey, Yousef A. Baker El-Ebiary, Nazmus Shaker Nafi, R. Ciro Rodriguez, Doris Esenarro Vargas, "Lightweight Cryptographic Algorithms for Guessing Attack Protection in Complex Internet of Things Applications", Complexity, vol. 2021, Article ID 5540296, 13 pages, 2021. https://doi.org/10.1155/2021/5540296.

24) Y. A. B. El-Ebiary, S. Almandeel, W. A. H. M. Ghanem, W. Abu-Ulbeh, M. M. M. Al-Dubai and S. Bamansoor, "Security Issues and Threats Facing the Electronic Enterprise Leadership," 2020 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS), 2020, pp. 24-28, doi:10.1109/ICIMCIS51567.2020.9354330.

25) Available online: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/ european-agenda-security/20180613_swd-2018-331-commission-staff-working-document_en.pdf (accessed on 12 October 2018).

26) IATA, Fact Sheet Cyber Security. Available online: https://www.iata.org/pressroom/facts_figures/fact_ sheets/Documents/fact-sheet-cyber-security.pdf (accessed on 12 October 2018).

27) ICAO. Assembly Resolution A39-19, September 2016. Available online: https://www.icao.int/Meetings/ a39/Documents/Resolutions/a39_res_prov_en.pdf (accessed on 12 October 2018).

28) Urban, J.A. Not Your Granddaddy's Aviation Industry: The Need to Implement Cybersecurity Standards and Best Practices within the International Aviation Industry. Alb. L. J. Sci. Tech. 2017, 27, 62–93.

29) Suarez-Alem´ an, A., & Jim´ ´enez, J. L. (2016). Quality assessment of airport performance from the passengers´perspective. Research in Transportation Business & Management, 20, 13–19. https://doi.org/10.1016/j.rtbm.2016.04.004.

30) Thelle, M. H., & Sonne, M. L. C. (2018). Airport competition in Europe. Journal of Air Transport Management, 67, 232–240. https://doi.org/10.1016/j.jairtraman.2017.03.005.

31) Tribe, J., & Snaith, T. (1998). From SERVQUAL to HOLSAT: Holiday satisfaction in Varadero, Cuba. Tourism Management, 19(1), 25–34. https://doi.org/10.1016/ S0261-5177(97)00094-0.

32) Trischler, J., & Lohmann, G. (2018). Monitoring quality of service at Australian airports: A critical analysis. Journal of Air Transport Management, 67, 63–71. https://doi.org/ 10.1016/j.jairtraman.2017.11.004.

33) Tsai, W., Hsu, W., & Chou, W. (2011). A gap analysis model for improving airport service quality. Total Quality Management and Business Excellence, 22(10), 1025–1040. https://doi.org/10.1080/14783363.2011.611326.

34) Urdang, B. S., & Howey, R. M. (2001). Assessing damages for non-performance of a travel professional – A suggested use of “SERVQUAL”. Tourism Management, 22(5), 533–538. https://doi.org/10.1016/S0261-5177(01)00008-5.

35) Van Vaerenbergh, Y., Varga, D., De Keyser, A., & Orsingher, C. (2019). The service recovery journey: Conceptualisation, integration, and directions for future research. Journal of Service Research, 22(2), 103–119. https://doi.org/10.1177/ 1094670518819852.

36) Wattanacharoensil, W., Schuckert, M., & Graham, A. (2016). An airport experience framework from a tourism perspective. Transport Reviews, 36(3), 318–340. https:// doi.org/10.1080/01441647.2015.1077287.

37) Wattanacharoensil, W., Schuckert, M., Graham, A., & Dean, A. (2017). An analysis of the airport experience from an air traveler perspective. Journal of Hospitality and Tourism Management, 32, 124–135. https://doi.org/10.1016/j.jhtm.2017.06.003.

38) Which?. (2018). Luton named worst UK airport for the third year running – long queues dismay passengers at Stansted and Manchester. Available at: https://www.which.co. uk/news/2018/08/luton-named-worst-uk-airport-for-the-third-year-running/.

39) Taviti Naidu Gongada, Amit Agnihotri, Kathari Santosh, Vijayalakshmi Ponnuswamy, Narendran S, Tripti Sharma and Yousef A.Baker El-Ebiary, “Leveraging Machine Learning for Enhanced Cyber Attack Detection and Defence in Big Data Management and Process Mining” International Journal of Advanced Computer Science and Applications(IJACSA), 15(2), 2024. http://dx.doi.org/10.14569/IJACSA.2024.0150266.

40) Franciskus Antonius Alijoyo, Taviti Naidu Gongada, Chamandeep Kaur, N. Mageswari, J.C. Sekhar, Janjhyam Venkata Naga Ramesh, Yousef A.Baker El-Ebiary, Zoirov Ulmas, Advanced hybrid CNN-Bi-LSTM model augmented with GA and FFO for enhanced cyclone intensity forecasting, Alexandria Engineering Journal, Volume 92, 2024, Pages 346-357, ISSN 1110-0168, https://doi.org/10.1016/j.aej.2024.02.062.

41) V Moses Jayakumar, R. Rajakumari, Kuppala Padmini, Sanjiv Rao Godla, Yousef A.Baker El-Ebiary and Vijayalakshmi Ponnuswamy, “Elevating Neuro-Linguistic Decoding: Deepening Neural-Device Interaction with RNN-GRU for Non-Invasive Language Decoding” International Journal of Advanced Computer Science and Applications(IJACSA), 15(2), 2024. http://dx.doi.org/10.14569/IJACSA.2024.0150233.

42) Mamta Kumari, Zoirov Ulmas, Suseendra R, Janjhyam Venkata Naga Ramesh and Yousef A. Baker El-Ebiary, “Utilizing Federated Learning for Enhanced Real-Time Traffic Prediction in Smart Urban Environments” International Journal of Advanced Computer Science and Applications(IJACSA), 15(2), 2024. http://dx.doi.org/10.14569/IJACSA.2024.0150267. Scopus, ISSN: 1992-8645

43) D. Anuradha, Gillala Chandra Sekhar, Annapurna Mishra, Puneet Thapar, Yousef A.Baker El-Ebiary and Maganti Syamala, “Efficient Compression for Remote Sensing: Multispectral Transform and Deep Recurrent Neural Networks for Lossless Hyper-Spectral Imagine” International Journal of Advanced Computer Science and Applications(IJACSA), 15(2), 2024. http://dx.doi.org/10.14569/IJACSA.2024.0150256.

44) Sushil Dohare, Deeba K, Laxmi Pamulaparthy, Shokhjakhon Abdufattokhov, Janjhyam Venkata Naga Ramesh, Yousef A.Baker El-Ebiary and E. Thenmozhi, “Enhancing Diabetes Management: A Hybrid Adaptive Machine Learning Approach for Intelligent Patient Monitoring in e-Health Systems” International Journal of Advanced Computer Science and Applications(IJACSA), 15(1), 2024. http://dx.doi.org/10.14569/IJACSA.2024.0150162.

ISSN 1533-9211

45) M Nagalakshmi, M. Balamurugan, B. Hemantha Kumar, Lakshmana Phaneendra Maguluri, Abdul Rahman Mohammed ALAnsari and Yousef A.Baker El-Ebiary, "Revolutionizing Magnetic Resonance Imaging Image Reconstruction: A Unified Approach Integrating Deep Residual Networks and Generative Adversarial Networks" International Journal of Advanced Computer Science and Applications(IJACSA), 15(1), 2024. http://dx.doi.org/10.14569/IJACSA.2024.0150139.

46) Sasikala P, Sushil Dohare, Mohammed Saleh Al Ansari, Janjhyam Venkata Naga Ramesh, Yousef A.Baker El-Ebiary and E. Thenmozhi, "A Hybrid GAN-BiGRU Model Enhanced by African Buffalo Optimization for Diabetic Retinopathy Detection" International Journal of Advanced Computer Science and Applications(IJACSA), 15(1), 2024. http://dx.doi.org/10.14569/IJACSA.2024.0150197.

47) Karimunnisa Shaik, Dyuti Banerjee, R. Sabin Begum, Narne Srikanth, Jonnadula Narasimharao, Yousef A.Baker El-Ebiary and E. Thenmozhi, "Dynamic Object Detection Revolution: Deep Learning with Attention, Semantic Understanding, and Instance Segmentation for Real-World Precision" International Journal of Advanced Computer Science and Applications(IJACSA), 15(1), 2024. http://dx.doi.org/10.14569/IJACSA.2024.0150141.

48) Asfar H. Siddiqui, Kathari Santosh, Dr. Mohammed Saleh Al Ansari, Badugu Suresh, Mrs. V. Sathiya, Prof. Ts. Dr. Yousef A. Baker El-Ebiary "Exploring the Dynamics Of Educational Feedback Networks With Graph Theory And Lstm-Based Modeling For Enhanced Learning Analytics And Feedback Mechanisms" Journal of Theoretical and Applied Information Technology, Vol. 101. No. 1 (2024).