Journal of Multidisciplinary Engineering Science and Technology (JMEST)
ISSN: 2458-9403
Vol. 11 Issue 3, March - 2024

Iot SECURITY FACTORS AND ATTACKS IN THE SAUDI GOVERNMENTAL TOURISM SECTOR

SARAH ALGHAMDI[1]
Information Technology Department, Saudi Electronic University
Riyadh, Saudi Arabia

ALI ABUABID[2*]
Information Technology Department, Saudi Electronic University
Abha, Saudi Arabia
a.abuabid@seu.edu.sa
* Corresponding Author

Abstract: **Integrating the Internet of Things (IoT) has reshaped technological landscapes, fostering seamless communication across devices and systems. However, this increased connectivity exposes critical sectors, such as government and tourism, to heightened security risks. This research project delves into the security dynamics and prevalent cyber threats targeting Saudi Arabia's governmental tourism sector. By identifying and analyzing the most frequent security factors and attacks associated with IoT, the study aims to underscore the urgency of proactive measures. Through a meticulous investigation of historical cases and emerging threats, this research establishes a foundation for understanding the tactics employed by cyber adversaries. A pivotal component of the study involves a survey designed to gauge the awareness and preparedness of stakeholders within the Saudi governmental tourism sector. The survey aims to assess the current security measures, perceived vulnerabilities, and experiences with cyber incidents. The findings underscore the importance of prioritizing IoT security in safeguarding national security and economic stability, particularly in Saudi Arabia's vibrant tourism industry. The paper concludes by emphasizing the necessity of proactive measures and recommends future work in a comprehensive security framework tailored to the specific challenges faced by the Saudi Arabian governmental tourism sector. By implementing such measures, Saudi Arabia can fortify its tourism industry against potential cyber threats, ensuring the continued attraction of visitors worldwide while minimizing the risks associated with IoT integration in critical sectors.**

Keywords—IoT Security, Factors, IoT Attacks, Saudi, Tourism

I. INTRODUCTION

Recently, significant attention has been directed toward the rapidly expanding Internet of Things (IoT) realm. This technological infrastructure facilitates the connection of everyday devices to the Internet [1]. This connectivity provides the capability for remote control and monitoring from virtually any location worldwide. Within the broad spectrum of IoT, devices vary from basic sensors that monitor temperature and humidity to advanced machines capable of recognizing and reacting to environmental changes. The utilization of IoT spans various sectors, including smart homes, industrial automation, healthcare monitoring, transportation systems, and more [2].

Acknowledging the considerable transformative possibilities presented by the IoT, the Saudi government has fervently supported its integration through diverse initiatives and programs. This commitment is especially apparent in initiatives targeting the establishment of smart cities, improvements in infrastructure, and the overall enhancement of quality of life [1] Aligned with the overarching goals of the Saudi Vision 2030, a comprehensive and long-term development plan, there is a strategic focus on digital transformation and the incorporation of emerging technologies, with a particular emphasis on integrating IoT systems into the dynamic landscape of the tourism sector.

The interconnection between the implementation of IoT and the realization of Vision 2030 in the Saudi Arabian tourism sector is emphasized by its diverse contributions, encompassing economic diversification, job creation, foreign investment, cultural exchange, and infrastructure development, including airports, hotels, resorts, theme parks, and various attractions. These contributions not only enhance the experience for tourists but also improve residents' overall quality of life [2].

The security scenario associated with the adoption of IoT in Saudi Arabia depends on various factors. These include the types of IoT devices in use, the effectiveness of security measures implemented by governmental bodies and individuals, and the potential threats and vulnerabilities inherent in IoT technology. Like other countries, Saudi Arabia faces cybersecurity challenges related to IoT devices, such as data breaches, hacking attempts, and unauthorized access [3]. Therefore, it is crucial to establish strong security protocols, including encryption methods, firewalls, and regular software updates, to protect the integrity and privacy of IoT systems within the Saudi context.

Security issues stand out as one of the primary hurdles hindering the extensive integration of IoT technology in Saudi organizations. It is essential to thoroughly grasp the various elements contributing to these challenges within the Saudi context. Through clear identification and effective mitigation of each factor's impact, there is an opportunity to boost the adoption of IoT technology, fostering a more secure and robust IoT ecosystem in the Kingdom.

The main aim of this study is to conduct empirical tests on the factors that impact IoT security within the Saudi governmental tourism sector, as extensively discussed in[3]. This overarching objective is outlined through the following specific research questions:

Q1: What are the principal factors influencing the implementation of IoT security measures in the Saudi tourism sector?

Q2: What are the primary cybersecurity threats impacting IoT systems in the Saudi tourism sector?

This study is divided into six sections, each contributing to thoroughly examining IoT security factors within the Saudi governmental tourism sector. The introduction outlines the researcher's interests and motivations concerning the security factors that impact IoT adoption in the tourism sector. Subsequently, the literature review delves into existing research on IoT security factors, conducting a detailed analysis of current challenges and factors that impede the advancement of IoT adoption in the Saudi governmental tourism sector. The research methods employed in this paper were utilized to gather the necessary information and data to investigate the market. This section provides a detailed description of the methodology components and their implementation. Following this, the results and discussion section analyzes the final research results, engaging in a discussion aligned with the research objectives. Finally, the paper's conclusion summarizes the key findings and the research contributions to IoT security implementation in the Saudi tourism sector. It also addresses research limitations and outlines potential avenues for future researchers.

II. LITERATURE REVIEW

IoT is promptly expanding, altering how people engage with their surroundings and inducing significant changes in various facets of modern life. The definitions of IoT systems are manifold. The term "IoT" describes a system wherein the Internet is intricately linked to the tangible world through pervasive sensors, incorporating RFID (radio-frequency identification) [4]. Conversely, [5] defines IoT as "a cyber-physical ecosystem of interconnected sensors and actuators that enable decision-making." It is also characterized as an extensive network of connected devices on the Internet, encompassing smartphones, tablets, and virtually anything equipped with sensors, ranging from cars, machinery in production plants, jet engines, oil drills, and wearable devices to various other items [6]. For this study, A broader IoT definition has been accepted as a network comprising tangible devices, vehicles, structures, and other objects integrated with sensors, software, and network connectivity. These devices can collect and exchange data with each other and other systems over the internet. The IoT-collected data can be analyzed to develop insights and make decisions that enable automation and efficiency in various industries or sectors [5].

On the other hand, IoT security pertains to safeguarding IoT devices and systems against unauthorized access, misuse, and exploitation [6]. The security of IoT systems is vital because these devices regularly collect and transmit sensitive data, encompassing personal, health, and financial information [7] Ensuring the security of IoT systems is of utmost importance, as a security breach can have substantial consequences for individuals and organizations, leading to the loss of privacy, financial setbacks, and harm to reputation [8].

Numerous countries globally have embraced IoT systems in diverse industry sectors, with the USA being recognized as a pivotal market for IoT devices. However, the widespread adoption of IoT devices has brought about new security challenges that demand careful consideration. A significant challenge in securing IoT devices in the U.S. stems from the abundance and diversity of available devices [5]. Small startups create and manufacture a considerable portion of these devices, which might lack the resources or expertise to integrate robust security features, leaving them vulnerable to cyberattacks [5].

In Saudi Arabia, like other nations, the government has acknowledged the significance of IoT systems and actively encouraged their adoption through diverse initiatives and programs [9]. Notably, the National Cybersecurity Authority (NCA) has issued guidelines for ensuring the security of IoT devices and systems [10] At the same time, the Saudi Standards, Metrology, and Quality Organization (SASO) have formulated standards for IoT security [11]. Furthermore, these entities have undertaken various initiatives to bolster cybersecurity awareness and strengthen the safeguarding of IoT systems against cyber threats. These initiatives encompass establishing centralized regulations and standards for IoT security, creating a national cybersecurity center, and investing in cybersecurity research and development [9]. One of the primary challenges in securing IoT devices in Saudi Arabia is insufficient awareness among consumers and businesses [12]. Many individuals are unaware of the security risks associated with IoT devices and may not implement appropriate measures to protect their devices. This leaves them vulnerable to hackers who can exploit the devices to access sensitive information or launch attacks on other systems [12].

Different government entities oversee distinct governance and public service areas within the Saudi Arabian governance framework. These entities may

be categorized differently based on definitions, but commonly recognized ones include agencies, councils, commissions, authorities, and ministries [13]. These entities are organized into three categories based on their functions and responsibilities. The executive branch encompasses ministries, authorities, and agencies responsible for executing government policies and delivering public services. The Tourism sector, a focal point in this research paper, serves as an illustrative example within this branch. The legislative branch includes the Shura Council, an advisory body reviewing and proposing new laws and regulations, and the Council of Ministers, which has the authority to approve laws and policies. The judicial branch consists of the courts and other legal institutions entrusted with upholding the law and ensuring justice [14].

The tourism sector plays a central role in achieving Vision 2030 in Saudi Arabia, acting as a crucial catalyst for economic growth, diversification, job creation, and foreign investment [15]. According to the World Travel and Tourism Council (WTTC), the direct economic contribution of the travel and tourism sector to Saudi Arabia's GDP was SAR 97.9 billion (USD 26.1 billion) in 2019, with an anticipated annual growth rate of 5.4%, reaching SAR 158.2 billion (USD 42.2 billion) by 2029 (Travel & Tourism Economic Impact [16]). The Saudi government has made substantial investments to enhance tourism infrastructure and position the country as a leading tourist destination, with the goal of attracting 100 million visitors annually by 2030 [17]. This strategic emphasis on tourism is expected to impact the country's GDP in the coming years significantly. The travel and tourism sector has emerged as a critical contributor to realizing Vision 2030 by fostering economic diversification, job creation, foreign investment, cultural exchange, and infrastructure development [2]. Consequently, ongoing investment in this sector is imperative for fulfilling Saudi Arabia's long-term goals.

A. Determinants Impacting IoT Security in the Saudi Tourism Sector

As previously stated, a comprehensive exploration of the theoretical landscape regarding the primary factors influencing IoT security in the Saudi tourism sector is detailed in [3]. We are reiterating these factors here to facilitate understanding for the readers of this paper. Table 1 presents the factors influencing IoT security in the Saudi government tourism sector, as identified and associated with their frequency in the relevant literature.

TABLE 1. HIGHEST FREQUENT FACTORS AFFECTING IOT SECURITY IN THE TOURISM SECTOR

Factors	Frequency
1. Privacy	15
2. Confidentiality	11
3. Data integrity	9
4. Access control	7
5. Availability	7
6. Trust	5
7. IoT standards and policies	4
8. IoT Awareness	4

Following that, Table 2 illuminates the identified factors connected with the comprehensive definition and the criteria that will be employed to assess the significance of these factors in relation to IoT security in the Saudi tourism sector.

TABLE 2. FACTORS AFFECTING IOT SECURITY IN THE TOURISM SECTOR AND THEIR ITEMS.

Factors	Literature Sources	Description	Items
Privacy	[18] [9] [8]	Privacy refers to the user's ability to control when, how, and to what extent personal information is collected, used, and shared. It involves protecting sensitive information from unauthorized access, use, or disclosure.	1. Data minimization 2. Transparency 3. Consent management 4. Privacy policies
Confidentiality	[19] [20]	Confidentiality refers to how authorized users' identifiable private information will be handled, managed, and disseminated. It is the practice of keeping sensitive information secure and protected from unauthorized access or disclosure. It involves ensuring that only authorized individuals have access to confidential information.	1. Access control list (ACLs) 2. Encryption 3. Authentication
Data integrity	[21] [19]	Data integrity refers to the assurance that information is trustworthy, accurate, complete, and consistent. Using IoT technologies helps protect data from unauthorized changes.	1. Data validation 2. Error detection and correction 3. Audit trails 4. Redundancy
Access control	[22]	Access control refers to the controls that manage the interaction and communication between users and systems in IoT, making it a challenge for the developer and consumer to trust IoT adoption.	1. Firewall 2. Authorization 3. Intrusion detection/prevention systems (IDS/IPS):
Availability	[23]	Availability refers to the accessibility and presence of IoT devices and services in a particular market or region. It is an essential factor for adopting and implementing IoT solutions as it determines the ease with which businesses and individuals can access and use these technologies.	1. Device uptime 2. Response time 3. Mean Time Between Failures (MTBF Mean Time to Repair (MTTR)

TABLE 2. FACTORS AFFECTING IOT SECURITY IN THE TOURISM SECTOR AND THEIR ITEMS(CONT.)

Factors	Literature Sources	Description	1. Items
Trust	[24]	Trust is a critical factor in the success of IoT solutions as it involves the security, privacy, and reliability of data collected and transmitted by these devices. Trust is built through robust security measures, transparent data-handling practices, and adherence to industry standards.	1. Presence of trust in IoT 2. User engagement
IoT standards and policies	[4]	IoT standards and policies refer to the guidelines, regulations, and protocols that govern the development, deployment, and operation of IoT devices and services. These standards ensure interoperability between different devices, promote data privacy and security and establish best practices for IoT implementation.	1. Availability of IoT 2. Availability of IoT policy
IoT Awareness	[25] [12]	IoT awareness refers to the level of knowledge and understanding that individuals, businesses, and governments have about the potential benefits and risks associated with IoT technologies. Increased awareness can lead to greater adoption of these technologies while also promoting responsible use through informed decision-making.	1. Existence of awareness programs 2. Availability of periodical training

B. Cybersecurity assaults aimed at IoT systems within the Saudi Tourism Sector

As previously stated, a comprehensive exploration of the theoretical landscape regarding the primary cybersecurity attacks targeting IoT security in the Saudi tourism sector is detailed in [3]. We are reiterating these attacks here to facilitate understanding for the readers of this paper. Cybersecurity attacks include any malicious activities directed at a computer system, network, or device intending to cause damage, disruption, theft, or compromise of data or information [12]. Cybersecurity offenders may operate as individuals or as part of organized groups, directing their efforts toward entities like individuals, businesses, governments, or other organizations. The growing ubiquity of connected devices across diverse sectors has led to a notable increase in cybersecurity attacks that specifically target IoT systems in recent years.

Following a thorough literature review on IoT security, a detailed analysis was undertaken, illustrated in Table 3. All documented attacks were systematically recorded, and their frequencies were computed, identifying 36 attacks in total. Subsequently, 7 attacks were selected based on a frequency threshold of 5 or more. However, the specific types of attacks from this shortlist that have been empirically investigated within the Saudi context remain undisclosed.

TABLE 3. HIGHEST FREQUENT ATTACKS TARGETING IOT SECURITY IN THE TOURISM SECTOR

Attacks	Literature Sources	Description	Frequency
1. Denial Of Service (DoS & DDoS) attack	[26] [19] [27]	A type of cyber-attack that is designed to disrupt access to a particular system or network by flooding it with traffic or overwhelming it with requests	13
2. Replay Attack	[28] [29] [30]	a security threat wherein an assailant intercepts and records a transmitted message or command between two IoT devices or between an IoT device and a network or server	8
3. Eavesdropping Attack	[31] [5]	A security breach in which a third party gains unauthorized access to sensitive information by intercepting and monitoring the communication between IoT devices, sensors, or other network-connected devices	7
4. Man-in-The-Middle (MiTM) Attack	[7] [32]	A type of cyber-attack in which a malicious actor intercepts and alters communications between two parties who believe they are communicating directly	7
5. Spoofing Attack	[33] [34]	A type of cyber-attack in which an attacker impersonates a legitimate device or system to gain unauthorized access or manipulate data	6
6. Sybil attack	[5] [35] [36]	It constitutes a security threat characterized by a malevolent actor creating numerous counterfeit identities with the intention of gaining control or manipulating a given system	6
7. Physical attacks	[37] [38] [39]	It denotes a cyber-attack wherein an individual or a group with malicious intent gains physical access to or tampers with a device or network infrastructure component	5

III. RESEARCH METHODOLOGY

This study employed an online survey approach to gain insights into the perceptions of governmental organizations within the Saudi tourism sector regarding the factors influencing IoT systems and the cybersecurity attacks associated with adopting IoT technologies. The selection of an online survey was driven by its expeditious access to participants, enhanced outreach to challenging contacts, and the efficiency of automated data collection, thereby minimizing researcher time and effort [40]. Additionally, online surveys contribute to cost savings through electronic data collection [41].

Aligned with the positivist research tradition, the study unfolded through five distinct stages: a thorough literature analysis to formulate theoretical concepts, the development of a survey instrument, evaluation of the instrument by domain experts, survey administration, and empirical data analysis. The literature analysis identified a comprehensive set of IoT security factors and cybersecurity attacks, laying the groundwork for an initial survey instrument categorized into four sections: profiles of participating managers, organizational characteristics, factors influencing IoT security adoption, and cybersecurity attacks targeting IoT devices within the Saudi tourism sector. The instrument underwent scrutiny by four domain experts, comprising three IoT academics and one senior IT manager from a government organization. Their feedback, totaling 18 items, focused on enhancing instrument clarity and readability (13 items), introducing new factor-related items (4 items), and removing a redundant item (1 item).

The survey targeted 80 governmental tourism organizations in Saudi Arabia, specifically reaching out to top management and senior personnel in IT or cybersecurity departments. A total of 25 tourism organizations, representing a 31.25% response rate, responded to the survey questionnaires distributed via email. The Director of Public Relations at the Saudi Ministry of Tourism facilitated access to these organizations.

IV. RESULTS

The research findings were examined utilizing the well-established statistical software SPSS version 25. Descriptive statistics, including frequencies, percentages, mean, and standard deviations, were employed to characterize the cybersecurity factors impacting IoT systems within the government tourism sector of Saudi Arabia and the associated attacks. The sample size warranted the use of non-parametric tests, specifically the Mann-Whitney U test and the Kruskal-Wallis test, to evaluate the distribution of mean rank scores for IoT security factors concerning sociodemographic information. The analyses considered a significance level of less than 0.05 ($P < 0.05$) statistically significant.

A. The Socio-Demographic Information

Table 4 summarizes the primary characteristics of the participating respondents. A slight prevalence of male respondents is noted, and the distribution of participating managers with respect to their work experience within their respective businesses is well-represented across all groups.

TABLE 4. THE SOCIO-DEMOGRAPHIC INFORMATION

Managers	Frequency	Percent
Gender	14	56.0
• Male		
• Female	11	44.0
Job role	9	36.0
• Manager	6	24.0
• Director		
• Senior	10	40.0
Years with the organization	2	8.0
• < One year	9	36.0
• 1-5 years	4	16.0
• 6-10 years		
• 10 years	10	40.0
Organization type	7	28.0
• Ministry	5	20.0
• Authority	8	32.0
• Company	5	20.0
• Program		
Number of employees	7	28.0
• < 200	5	20.0
• 200 - 500		
• 500	13	52.0

B. The Internal Consistency Method

It was employed to assess the scale's validity, confirming that the designed items measure the same underlying factor. This involved testing the high correlation of these items using Pearson correlation, with Cronbach's alpha (α) being a commonly utilized method. Internal consistency estimates with an alpha (α) magnitude of ≥ 0.70 were deemed acceptable. As depicted in Table 5, all 24 items exhibited highly significant and positive correlations with the overall scale score, ranging from (r=0.727, p<0.01) to (r=0.413, p<0.05). The Cronbach's alpha for the total scale score was (α=0.93), indicating a high level of internal consistency. Therefore, the findings confirm the scale's validity and reliability.

TABLE 5. THE INTERNAL CONSISTENCY METHOD OF THE IOT SECURITY FACTORS SCALE

No.	R	No.	R	No.	R	No.	R
1	0.521**	7	0.663**	13	0.570**	19	0.741**
2	0.747**	8	0.730**	14	0.598**	20	0.737**
3	0.496*	9	0.692**	15	0.703**	21	0.728**
4	0.807**	10	0.413*	16	0.434*	22	0.544**
5	0.610**	11	0.587**	17	0.716**	23	0.568**
6	0.442*	12	0.437*	18	0.727**	24	0.553**
*r ≤ 0.05; ** r ≤ 0.01; ns = Not significant							

C. Descriptive Information on the IoT Security Factors

IoT security is affected by 8 factors using 24 items, utilizing a 5-point Likert scale ranging from (5=strongly agree) to (1=strongly disagree). As depicted in Table 6, ***Privacy*** was evaluated with four items, yielding a total mean score of (M=3.26 and SD=0.92, indicating a high level). Notably, the item "We collect only the necessary data and avoid the unnecessary collection of personal information" attained the highest mean score (M=3.60; SD=1.08, signifying a high level), while the item "We have clear and comprehensive privacy policies that outline how personal data is collected, used, and shared" obtained the lowest mean score (M=3.04; SD=1.10, indicating a moderate level).

TABLE 6. DESCRIPTIVE INFORMATION ON PRIVACY

Statement	Strongly disagree		Disagree		Neutral		Agree		Strongly Agree		M	SD	Level
	N	%	N	%	N	%	N	%	N	%			
We have a list that specifies which users or devices are allowed or denied access to specific resources.	0	0	4	16	0	0	16	64	5	20	3.88	0.93	H
We use data encryption mechanisms so that only authorized parties can access them.	1	4	4	16	3	12	15	60	2	8	3.52	1.00	H
We verify the user's identity before allowing access to sensitive data using biometric authentication such as fingerprints, facial recognition, or iris scans or Two-factor authentication (2FA) such as a password and a security token.	1	4	2	8	1	4	16	64	5	20	3.88	0.97	H
Total mean score											**3.76**	**0.81**	**H**
Keys: *1.00-1.80= Very low (VL); 1.81-2.60=Low(L); 2.61-3.40=Moderate(M);3.41-4.20=High(H);4.21-5.00=Very high (VH).*													

As shown in Table 7, **Confidentiality** was assessed through three items, resulting in a total mean score of (M=3.76; SD=0.81). Notably, the item "We have a list that specifies which users or devices are allowed or denied access to specific resources" attained the highest mean score (M=3.88; SD=01.93), while the item "We use data encryption mechanisms in such a way that only authorized parties can access them" received the lowest mean score (M=3.52; SD=1.00).

TABLE 1 DESCRIPTIVE INFORMATION ON CONFIDENTIALITY

Statement	Strongly disagree		Disagree		Neutral		Agree		Strongly Agree		M	SD	Level
	N	%	N	%	N	%	N	%	N	%			
We have a list that specifies which users or devices are allowed or denied access to specific resources.	0	0	4	16	0	0	16	64	5	20	3.88	0.93	H
We use data encryption mechanisms so that only authorized parties can access them.	1	4	4	16	3	12	15	60	2	8	3.52	1.00	H
We verify the user's identity before allowing access to sensitive data using biometric authentication such as fingerprints, facial recognition, or iris scans or Two-factor authentication (2FA) such as a password and a security token.	1	4	2	8	1	4	16	64	5	20	3.88	0.97	H
Total mean score											**3.76**	**0.81**	**H**
Keys: *1.00-1.80= Very low (VL); 1.81-2.60=Low(L); 2.61-3.40=Moderate(M);3.41-4.20=High(H);4.21-5.00=Very high (VH).*													

Examining Table 8, ***Data Integrity*** was gauged using four items, resulting in a total mean score of (M=3.35; SD=0.67). Notably, the item "We have audit trails to maintain a record of all actions taken on the data, including who accessed it, when, and for what purpose" achieved the highest mean score (M=3.76; SD=0.78), while the item "We use RAID techniques that store multiple copies of the data in different locations to ensure that it is not lost or corrupted due to hardware failures or other issues" received the lowest mean score (M=3.08; SD=0.95).

TABLE 8: DESCRIPTIVE INFORMATION OF DATA INTEGRITY

STATEMENT	Strongly disagree		Disagree		Neutral		Agree		Strongly Agree		M	SD	Level
	N	%	N	%	N	%	N	%	N	%			
We validate the data's accuracy and completeness before it is transmitted or stored.	0	0	6	24.0	9	36.0	7	28.0	3	12.0	3.28	0.98	M
We identify errors in the data and correct them to ensure that they are accurate and consistent.	0	0	6	24.0	8	32.0	9	36.0	2	8.0	3.28	0.94	M
We have audit trails to record all actions taken on the data, including who accessed it, when, and for what purpose.	0	0	3	12.0	2	8.0	18	72.0	2	8.0	3.76	0.78	H
We use RAID techniques that store multiple copies of the data in different locations to ensure that it is not lost or corrupted due to hardware failures or other issues.	0	0	9	36.0	6	24.0	9	36.0	1	4.0	3.08	0.95	M
Total mean score											**3.35**	**0.67**	**M**
Keys: 1.00-1.80= Very low (VL); 1.81-2.60=Low(L); 2.61-3.40=Moderate(M);3.41-4.20=High(H);4.21-5.00=Very high(VH).													

As indicated in Table 9, ***Access Control*** was assessed through three items, resulting in a total mean score of (M=3.72; SD=0.62). Noteworthy is the item "We authorize users or devices to access specific resources with the ability to do certain actions," which obtained the highest mean score (M=3.84; SD=0.55), while the item "We use software that detects and prevents unauthorized access attempts by monitoring network traffic for suspicious activity" received the lowest mean score (M=3.56; SD=0.82).

TABLE 9. DESCRIPTIVE INFORMATION ON THE ACCESS CONTROL

Statement	Strongly disagree		Disagree		Neutral		Agree		Strongly Agree		M	SD	Level
	N	%	N	%	N	%	N	%	N	%			
We have a network security system that monitors and controls incoming and outgoing traffic based on predetermined security rules.	0	0	3	12	3	12	16	64	3	12	3.76	0.83	H
We authorize users or devices to access specific resources with the ability to do certain actions.		0	1	4	3	12	20	80	1	4	3.84	0.55	H
We use software that detects and prevents unauthorized access attempts by monitoring network traffic for suspicious activity.	0	0	4	16	4	16	16	64	1	4	3.56	0.82	H
Total mean score											**3.72**	**0.62**	**H**
Keys: *1.00-1.80= Very low (VL); 1.81-2.60=Low(L); 2.61-3.40=Moderate(M);3.41-4.20=High(H);4.21-5.00=Very high (VH).*													

Furthermore, Table 10 reveals that ***Trust*** was evaluated through two items, resulting in a total mean score of (M=3.42; SD=0.79). Specifically, the item "We believe that the usage rate and employee engagement of IoT technology will increase in the future" achieved the highest mean score (M=3.84; SD=1.07), while the item "We trust the security measures taken in the IoT adoption" obtained a lower mean score (M=3.00; SD=1.15).

TABLE 10. DESCRIPTIVE INFORMATION ON TRUST

Statement	Strongly disagree		Disagree		Neutral		Agree		Strongly Agree		M	SD	Level
	N	%	N	%	N	%	N	%	N	%			
We trust the security measures taken in the IoT adoption.	2	8.0	7	28.0	8	32	5	20	3	12	3.00	1.15	M
We believe that the usage rate and employee engagement of IoT technology will increase in the future.	1	4.0	2	8.0	4	16	11	44	7	28	3.84	1.07	H
Total mean score											**3.42**	**0.79**	**H**
Keys: *1.00-1.80= Very low (VL); 1.81-2.60=Low(L); 2.61-3.40=Moderate(M);3.41-4.20=High(H);4.21-5.00=Very high (VH).*													

As depicted in Table 11, ***Standards and policies*** were assessed through two items, resulting in a total mean score of (M=2.60 and SD=1.03, indicating a low level). Specifically, the item "We have a clear IoT policy and regulation" achieved the highest mean score (M=2.92; SD=1.08, indicating a moderate level), while the item "We have built our own standards to adopt IoT" received a lower mean score (M=2.28; SD=1.14, indicating a low level).

TABLE 2. DESCRIPTIVE INFORMATION ON THE STANDARDS AND POLICIES

Statement	Strongly disagree		Disagree		Neutral		Agree		Strongly Agree		M	SD	Level
	N	%	N	%	N	%	N	%	N	%			
We have built our standards to adopt IoT.	7	28	9	36	5	20	3	12	1	4	2.28	1.14	L
We have a clear IoT policy and regulation.	1	4	10	40	6	24	6	24	2	8	2.92	1.08	M
Total mean score											**2.60**	**1.03**	**L**
Keys: *1.00-1.80= Very low (VL); 1.81-2.60=Low(L); 2.61-3.40=Moderate(M);3.41-4.20=High(H);4.21-5.00=Very high (VH).*													

Moving to Table 12, ***Awareness*** was appraised through two items, resulting in a total mean score of (M=2.78; SD=1.01). Specifically, the item "We regularly conduct awareness programs" garnered the highest mean score (M=2.92; SD=1.12, indicating a moderate level), while the item "Training that increases knowledge about IoT systems is available at a periodic pace" received a slightly lower mean score (M=2.64; SD=1.08, also indicating a moderate level).

TABLE 3. DESCRIPTIVE INFORMATION ON THE AWARENESS

Statement	Strongly disagree		Disagree		Neutral		Agree		Strongly Agree		M	SD	Level
	N	%	N	%	N	%	N	%	N	%			
We regularly conduct awareness programs.	0	0.0	14	56	1	4.0	8	32.0	2	8.0	2.92	1.12	M
Training that increases knowledge about IoT systems is available at a periodic pace.	2	8.0	14	56	0	0.0	9	36.0	0	0.0	2.64	1.08	M
Total mean score											**2.78**	**1.01**	M
Keys: *1.00-1.80= Very low (VL); 1.81-2.60=Low(L); 2.61-3.40=Moderate(M);3.41-4.20=High(H);4.21-5.00=Very high (VH).*													

Finally, Table 13 reveals that ***Availability*** was assessed through four items, yielding a total mean score of (M=3.42; SD=0.76, denoting a high level). Specifically, the item "We have SLA that indicates the amount of time an IoT device is operational without any downtime or failure" achieved the highest mean score (M=3.52; SD=0.77, indicating a high level), while the item "We have SLA that indicates the average time between failures of an IoT device or system" obtained a slightly lower mean score (M=3.28; SD=0.91, indicating a moderate level).

TABLE 4: DESCRIPTIVE INFORMATION ON THE AVAILABILITY

Statement	Strongly disagree		Disagree		Neutral		Agree		Strongly Agree		M	SD	Level
	N	%	N	%	N	%	N	%	N	%			
We have an SLA that indicates the amount of time an IoT device is operational without any downtime or failure.	0	0.0	3	12	7	28	14	56	1	4.0	3.52	0.77	H
We have an SLA that indicates how quickly an IoT system responds to user requests or commands.	0	0.0	4	16	5	20	15	60	1	4.0	3.52	0.82	H
We have an SLA that indicates the average time between failures of an IoT device or system.	0	0.0	7	28	5	20	12	48	1	4.0	3.28	0.94	M
We have an SLA that indicates the average time it takes to repair a failed IoT device or system.	0	0.0	6	24	5	20	13	52	1	4.0	3.36	0.91	M
Total mean score											**3.42**	**0.76**	**H**
Keys: *1.00-1.80= Very low (VL); 1.81-2.60=Low(L); 2.61-3.40=Moderate(M);3.41-4.20=High(H);4.21-5.00=Very high (VH).*													

D. The Relationship between IoT Security Factors in the Saudi Governmental Tourism Sector

Table 14 illustrates the connections among identified IoT security factors. Most factors exhibit a positive relationship with each other, ranging from (r=0.802, p<0.01) to (r=0.403, p<0.01). While some relationships were deemed insignificant with values around 3.00, it is worth noting that, due to the sample size, these factors could still be highly related.

TABLE 5. THE RELATIONSHIP BETWEEN CYBER SECURITY FACTORS

Factors	Privacy	Confidentiality	Data Integrity	Access Control	Trust	Standards & Policies	Awareness	Availability
Privacy	1							
Confidentiality	0.439*	1						
Data integrity	0.579**	0.635**	1					
Access control	0.424*	0.612**	0.394	1				
Trust	0.484*	0.392	0.537**	0.478*	1			
IoT standards& policies	0.592**	0.237	0.533**	0.284	0.704**	1		
IoT Awareness	0.641**	0.330	0.623**	0.218	0.632**	0.802**	1	
Availability	0.314	0.338	0.403*	0.407*	0.416*	0.523**	0.512**	1
**p≤0.05; **p≤0.01; ***p≤0.001*								

E. Security threats encountered by the Saudi governmental tourism sector

In Table 15, the presentation of attack types is outlined. Denial of Service emerged as the predominant threat at 36.84%, succeeded by Physical attacks at 31.58%, Phishing at 21.05%, and finally, Eavesdropping and Man-in-The-Middle (MiTM) both accounted for 5.26% each.

TABLE 15. SECURITY THREATS IN THE SAUDI TOURISM SECTOR

Attack type	Frequency	Percent
Denial of Service (DoS)	7	36.84
Physical	6	31.58
Phishing	4	21.05
Eavesdropping	1	5.26
Man-in-The-Middle (MiTM)	1	5.26
Total	**19**	**100.0**

V. DISCUSSION

In the initial phase of the study, an extensive literature review was conducted on a global scale, revealing eight factors deemed most influential in IoT security. In descending order of significance, these factors include *privacy, confidentiality, data integrity, access control, availability, trust, IoT standards and policies*, and *IoT awareness*. However, analyzing responses specific to the Saudi governmental tourism sector depicted a shift in priorities. Figure (1) illustrates that *confidentiality* and *access control* have garnered the highest importance, while the remaining five factors hold moderate significance. The outcomes suggest a noteworthy emphasis within the Saudi tourism sector on IoT security factors, underscored by implementing robust tools and mechanisms. Notably, the sector places particular emphasis on data confidentiality and access control, emphasizing authentication and authorization, as opposed to aspects like awareness and establishing well-defined standards and policies.

FIGURE 1: THE TOTAL MEAN SCORES AND LEVELS OF THE CYBER SECURITY FACTORS

In Table 16, non-parametric tests, namely Mann-Whitney and Kruskal-Wallis, were utilized to assess the distribution of IoT security factors concerning socio-demographic factors. The findings reveal that the profile of the responding organizations significantly influences the results.

On the other hand, in the initial phase of the research, an extensive global literature review was conducted, revealing seven prominent attacks that target IoT security. In descending order of significance, these attacks include denial of service (DoS & DDoS) attacks, replay attacks, eavesdropping attacks, man-in-the-middle (MiTM) attacks, spoofing attacks, Sybil attacks, and physical attacks.

TABLE 16. THE DISTRIBUTION OF IOT SECURITY FACTORS IN TERMS OF SOCIO-DEMOGRAPHIC INFORMATION

Factor	Privacy	Confidentiality	Data integrity	Access control	Trust	standards & policies	Awareness	Availability
Gender	13.21	13.14	13.36	13.46	11.79	11.54	12.39	12.14
• Male	12.73	12.82	12.55	12.41	14.55	14.86	13.77	14.09
• Female								
p-value	0.87	0.91	0.78	0.70	0.34	0.25	0.61	0.50
Job role	14.44	10.72	14.50	12.89	14.17	13.06	11.39	14.44
• Manager	13.83	12.92	13.50	11.42	12.25	14.83	15.25	13.83
• Director	11.20	15.10	11.35	14.05	12.40	11.85	13.10	11.20
• Senior								
p-value	0.60	0.42	0.63	0.75	0.83	0.69	0.59	0.60
Experience	13.00	9.25	12.25	9.25	15.75	10.75	11.25	13.00
• < 1 year	12.78	16.72	12.94	14.11	12.50	12.56	13.39	12.78
• 1-5 years	10.63	7.25	10.00	12.25	11.75	11.13	9.13	10.63
• 6-10 years	14.15	12.70	14.40	13.05	13.40	14.60	14.55	14.15
• 10 years								
p-value	0.88	0.14	0.78	0.83	0.92	0.77	0.62	0.88
Organization type	11.57	11.71	12.50	9.93	9.86	12.07	11.43	11.57
• Ministry	10.10	9.90	13.40	16.00	15.10	13.00	15.10	10.10
• Authority	14.56	14.25	14.88	10.06	17.94	16.94	13.25	14.56
• Company	15.40	15.90	10.30	19.00	7.40	8.00	12.70	15.40
• Program								
p-value	0.58	0.53	0.74	**0.05***	**0.03***	0.13	0.85	0.58
Number of employees	11.36	11.57	6.71	12.50	8.57	9.79	11.21	11.36
• < 200	11.60	11.30	14.90	13.80	17.30	15.40	15.60	11.60
• 200 - 500	14.42	14.42	15.65	12.96	13.73	13.81	12.96	14.42
• 500								
p-value	0.60	0.59	**0.03***	0.95	0.10	0.30	0.58	0.60
Statistic	**<0.001***	0.07	**<0.001*****	0.56	**0.03***	0.04	**<0.001*****	0.47

*p≤0.05; **p≤0.01; ***p≤0.001

Contrastingly, the analysis of responses specific to the Saudi governmental tourism sector, as depicted in Figure (2), reveals variations from the literature review findings. Denial of Service (DoS) attacks emerged as the predominant threat facing the tourism sector, followed by physical attacks, phishing attacks, eavesdropping attacks, and lastly, Man-in-The-Middle (MiTM) attacks.

Phishing, a type of cyber-attack where fraudulent emails or messages are sent to deceive individuals into divulging sensitive information, such as login credentials or credit card details, showed a notable contrast between the literature review and the sector's responses. Typically appearing as messages from legitimate sources, such as banks or social media platforms, these deceptive communications often include links to fake websites. Once victims enter their information on these fraudulent sites, attackers can exploit it for identity theft, financial fraud, or other malicious activities [12]. This type of attack tends to be more prevalent in organizations or sectors with limited knowledge about cybersecurity threats.

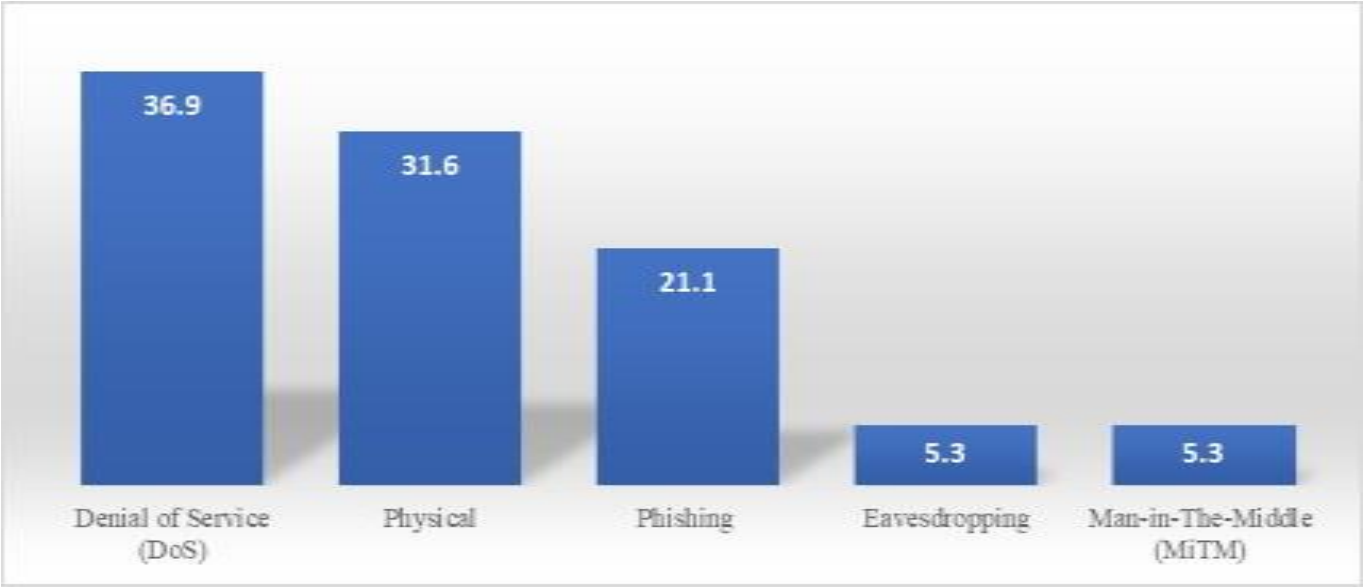

FIGURE 2: DISTRIBUTION OF ATTACK TYPES IN THE SAUDI TOURISM SECTOR BY PERCENTAGE

V.1 Recommendations To Overcome the Identified Weakness in IoT Security in the Saudi Government Tourism Sector

Based on these findings, the researchers propose several recommendations for enhancing IoT security in the Saudi tourism sector:

1. **Increase Awareness through Continuous Training:**

- Conduct ongoing IoT security awareness sessions and periodic training programs for employees and customers.
- Collaborate with reputable global cybersecurity organizations, such as SANS, to ensure comprehensive and up-to-date training.
- Develop a robust training program covering all facets of IoT security, including risk identification, threat awareness, and protection measures.
- Incorporate practical exercises simulating real-world scenarios to allow participants to apply their knowledge in a secure environment.

2. **Establish a Security Culture:**

- Foster a culture of cybersecurity within the Saudi tourism organizations by instilling a sense of responsibility among employees and customers for safeguarding their data and devices.
- Regularly communicate the importance of IoT security through diverse channels such as emails, posters, newsletters, and internal forums.
- Provide accessible resources like online forums or help desks for employees and customers to seek advice or report suspicious activities related to IoT devices.
-

3. **Develop Customized Policies in Alignment with Regulatory Framework:**

- Formulate organization-specific policies in line with the nature of their operations and the directives of the Saudi Cyber Security Authority.
- Gain a comprehensive understanding of guidelines and regulations set by the Saudi Cyber Security Authority to align policies with the national cybersecurity framework.
- Perform thorough risk assessment to identify potential cybersecurity threats and vulnerabilities, enabling the development of policies addressing these risks and protecting assets from cyber-attacks.
- Establish concise policies and procedures for data protection, access control, incident response, and disaster recovery, ensuring effective communication with all employees and stakeholders.

6.0 CONCLUSIONS AND FUTURE WORK

The widespread integration of the Internet has elevated the prominence of IoT technologies, prompting global organizations, particularly those in the tourism sector, to delve into diverse IoT implementations. Despite the potential benefits, deriving advantages from these technologies proves challenging due to the myriad cybersecurity threats faced by IoT devices. While there is existing literature on IoT adoption, a noticeable gap exists in understanding the factors influencing IoT security within the Saudi tourism sector, with a lack of exploration into specific cybersecurity attacks targeting organizations in this field. To address this literature gap, we initiated this research paper to understand better Saudi tourism organizations' perceptions of IoT security adoption.

Our study has yielded several noteworthy findings, discussed in the context of existing literature. However, it is essential to approach the interpretation

of these findings with caution due to using a convenient and small sample. Despite this limitation, we believe our findings contribute valuable insights to both theory and practice. In terms of theory, this research illuminates success factors and key cybersecurity attacks of IoT security, focusing on the Saudi tourism sector—an area that has been overlooked in existing IoT security literature primarily concerned with the general adoption of IoT technologies. Concerning practice, our findings aim to heighten the awareness of management in tourism organizations regarding pivotal factors and cybersecurity attacks associated with IoT security adoption, enabling them to establish realistic expectations for their investments in IoT technology.

Several opportunities exist to extend our work. Increasing the sample size and conducting qualitative case studies would enhance the generalizability of our research findings. Further studies are warranted to explore the ripple effect of IoT technology investment on organizational processes. This research suggests that Saudi tourism organizations adopt a long-term perspective on utilizing IoT technologies, prompting the need for additional studies to explore this phenomenon in contexts beyond Saudi Arabia.

The widespread adoption of the Internet has heightened the visibility of IoT technologies, prompting organizations globally, especially those in the tourism sector, to invest in diverse IoT implementations. Despite the potential benefits, realizing advantages from these technologies proves challenging due to the multitude of cybersecurity threats IoT devices face. While there is existing literature on IoT adoption, there is a notable gap in understanding the factors influencing IoT security within the Saudi tourism sector and a lack of exploration into the specific cybersecurity attacks targeting organizations in this sector. To address this gap in the literature, this research paper was initiated to understand better Saudi tourism organizations' perceptions of IoT security adoption.

Several interesting findings have emerged from our study, which was discussed in light of the existing literature. However, our interpretation of the findings should be treated with caution due to the selection of a convenient and small sample. Despite this limitation, our findings are useful to theory and practice. For theory, this research highlights the success factors and key cybersecurity attacks of IoT security from the perspective of the Saudi tourism sector, which has not been specifically addressed in the existing IoT security literature. As the IoT literature is primarily concerned with adopting IoT technologies in general, this study helps reduce a gap in the literature. With regard to practice, the findings would help raise awareness of tourism organizations' management about the key factors and cybersecurity attacks associated with IoT security adoption and thus help set realistic expectations from their investment decisions in IoT technology.

There are several ways to extend our work. There is a clear need to increase the sample size and conduct qualitative case studies. Together, they would help us improve the generalization of the research findings. Further studies are needed to investigate the ripple effect of IoT technology investment on organizational processes. This research indicated that Saudi tourism organizations have a long-term view of utilizing IoT technologies. Further studies are required to explore this phenomenon in contexts other than Saudi Arabia.

REFERENCES

[1]M. N. Al Otaibi, “Internet of Things (IoT) Saudi Arabia healthcare systems: state-of-the-art, future opportunities and open challenges,” *J Health Inform Dev Ctries*, vol. 13, no. 1, 2019.

[2]B. E. Barakka, “Determinants of Tourism Competitiveness in Emerging Tourists’ Destinations in the Arab Region: the Case of Saudi Arabia.,” *International Journal of Hospitality & Tourism Studies (IJHTS)*, vol. 2, no. 2, 2021.

[3]Sarah Alghamdi and AbuAbid Ali, “IoT Safeguarding in Saudi Tourism Sector: Crafting a Preliminary Security Model for Enhancing Cyber Resilience,” *International Journal on Recent and Innovation Trends in Computing and Communication*, vol. 11, no. 9, pp. 3847–3859, 2023, doi: 10.17762/ijritcc.v11i9.9641.

[4]J. Saleem, M. Hammoudeh, U. Raza, B. Adebisi, and R. Ande, “IoT standardisation: Challenges, perspectives and solution,” in *Proceedings of the 2nd international conference on future networks and distributed systems*, 2018, pp. 1–9.

[5]T. Houston, “Mass surveillance and terrorism: does PRISM keep Americans safer?,” University of Tennessee Honors Thesis Projects., 2017.

[6]M. Muntjir, M. Rahul, and H. A. Alhumyani, “An analysis of Internet of Things (IoT): novel architectures, modern applications, security aspects and future scope with latest case studies,” *Int. J. Eng. Res. Technol*, vol. 6, no. 6, pp. 422–447, 2017.

[7]P. Williams, I. K. Dutta, H. Daoud, and M. Bayoumi, “A survey on security in internet of things with a focus on the impact of emerging technologies,” *Internet of Things*, vol. 19, p. 100564, 2022.

[8]S. Mohanty, K. Cormican, and C. Dhanapathi, “Analysis of critical success factors to mitigate privacy risks in IoT Devices,” *Procedia Comput Sci*, vol. 196, pp. 191–198, 2022.

[9]O. Almutairi and K. Almarhabi, “Investigation of Smart Home Security and privacy: Consumer perception in Saudi Arabia,” *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 4, 2021.

[10]National Cybersecurity Authority (NCA), “Policy and Standards,” https://nca.gov.sa/en. Accessed: Dec. 04, 2023. [Online]. Available: https://nca.gov.sa/en

[11]M. and Q. O. (SASO) Saudi Standards, “IoT security standard,” https://www.saso.gov.sa/en/pages/default.aspx.

[12]M. Almoaigel and A. Abuabid, “Implementation of Cybersecurity Situation Awareness Model in Saudi SMEs,” *Int J Adv Comput Sci Appl*, vol. 14, no. 11, pp. 1082–1092, Nov. 2023.

[13]A. Bukhatir, M. A. Al-Hawari, S. Aderibigbe, M. Omar, and E. Alotaibi, “Improving student retention in higher education institutions–Exploring the factors influencing employees extra-role behavior,” *Journal of Open Innovation: Technology, Market, and Complexity*, vol. 9, no. 3, p. 100128, 2023.

[14]S. M. Alholiby and Z. A. Almulhim, “From the Lack to the Requirement: The Public Consultation Reform in Saudi Arabia,” *UCLA Journal of Islamic and Near Eastern Law*, vol. 20, 2023.

[15]S. Dargaoui, M. Azrour, A. El Allaoui, A. Guezzaz, and S. Benkirane, “Authentication in Internet of Things: State of Art,” in *Proceedings of the 6th International Conference on Networking, Intelligent Systems & Security*, 2023, pp. 1–6.

[16]World Travel and Tourism Council (WTTC), “Contribution of travel and tourism to Saudi Arabia’s GDP.” Accessed: Dec. 04, 2023. [Online]. Available: https://wttc.org/

[17]Elsiddig Yousif Mohamed Musa, “The impact of tourism in the kingdom of Saudi Arabia on GDP, (2005 – 2017: An analytical approach),” *Global Journal of Economics and Business*, vol. 10, no. 2, pp. 458–462, 2021.

[18]P. M. Chanal and M. S. Kakkasageri, “Security and privacy in IoT: a survey,” *Wirel Pers Commun*, vol. 115, no. 2, pp. 1667–1693, 2020.

[19]M. Frustaci, P. Pace, G. Aloi, and G. Fortino, “Evaluating critical security issues of the IoT world: Present and future challenges,” *IEEE Internet Things J*, vol. 5, no. 4, pp. 2483–2495, 2017.

[20]K. Y. Najmi, M. A. AlZain, M. Masud, N. Z. Jhanjhi, J. Al-Amri, and M. Baz, “A survey on security threats and countermeasures in IoT to achieve users confidentiality and reliability,” *Mater Today Proc*, 2021.

[21]M. N. Aman, B. Sikdar, K. C. Chua, and A. Ali, “Low power data integrity in IoT systems,” *IEEE Internet Things J*, vol. 5, no. 4, pp. 3102–3113, 2018.

[22]I. Ali, S. Sabir, and Z. Ullah, “Internet of things security, device authentication and access control: a review,” *arXiv preprint arXiv:1901.07309*, 2019.

[23]M. Haghi, K. Thurow, and R. Stoll, “Wearable devices in medical internet of things: scientific research and commercially available devices,” *Healthc Inform Res*, vol. 23, no. 1, pp. 4–15, 2017.

[24]P. Shi, H. Wang, S. Yang, C. Chen, and W. Yang, “Blockchain-based trusted data sharing among trusted stakeholders in IoT,” *Softw Pract Exp*, vol. 51, no. 10, pp. 2051–2064, 2021.

[25]K. C. Ravikumar, P. Chiranjeevi, N. M. Devarajan, C. Kaur, and A. I. Taloba, “Challenges in internet of things towards the security using deep learning techniques,” *Measurement: Sensors*, vol. 24, p. 100473, 2022.

[26]U. Islam *et al.*, “Detection of distributed denial of service (DDoS) attacks in IOT based monitoring system of banking sector using machine learning models,” *Sustainability*, vol. 14, no. 14, p. 8374, 2022.

[27]A. Cheema, M. Tariq, A. Hafiz, M. M. Khan, F. Ahmad, and M. Anwar, “Prevention Techniques against Distributed Denial of Service Attacks in Heterogeneous Networks: A Systematic Review,” *Security and Communication Networks*, vol. 2022, pp. 1–15, 2022.

[28]M. A. Al-Shareeda, S. Manickam, S. A. Laghari, and A. Jaisan, “Replay-attack detection and prevention mechanism in industry 4.0 landscape for secure SECS/GEM communications,” *Sustainability*, vol. 14, no. 23, p. 15900, 2022.

[29]M. Nadeem, A. Arshad, S. Riaz, S. W. Zahra, A. K. Dutta, and S. Almotairi, “A Secure Architecture to Protect the Network from Replay Attacks during Client-to-Client Data Transmission,” *Applied Sciences*, vol. 12, no. 16, p. 8143, 2022.

[30]A. R. Sfar, E. Natalizio, Y. Challal, and Z. Chtourou, “A roadmap for security challenges in the Internet of Things,” *Digital Communications and Networks*, vol. 4, no. 2, pp. 118–137, 2018.

[31]S. Zaman *et al.*, “Security threats and artificial intelligence based countermeasures for internet of things networks: a comprehensive survey,” *Ieee Access*, vol. 9, pp. 94668–94690, 2021.

[32]E. A. Shammar, A. T. Zahary, and A. A. Al-Shargabi, “A survey of IoT and blockchain integration: Security perspective,” *IEEE Access*, vol. 9, pp. 156114–156150, 2021.

[33]N. M. Kumar and P. K. Mallick, “Blockchain technology for security issues and challenges in IoT,” *Procedia Comput Sci*, vol. 132, pp. 1815–1823, 2018.

[34]B. Elnaim and H. Al-Lami, “The current state of phishing attacks against Saudi Arabia university students,” *International Journal of Computer Applications Technology and Research*, vol. 6, no. 1, pp. 42–50, 2017.

[35]M. T. Quasim, “Challenges and applications of internet of things (IoT) in Saudi Arabia,” 2021.

[36]R. Parashar, A. Khan, and A. K. Neha, “A survey: The internet of things,” *International Journal of Technical Research and Applications*, vol. 4, no. 3, pp. 251–257, 2020.

[37]Y. Shah and S. Sengupta, “A survey on Classification of Cyber-attacks on IoT and IIoT devices,” in *2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, IEEE, 2020, pp. 406–413.

[38]R. A. Al-Mulhim, L. A. Al-Zamil, and F. M. Al-Dossary, “Cyber-attacks on Saudi Arabia environment,” *International Journal of Computer Networks and Communications Security*, vol. 8, no. 3, pp. 26–31, 2020.

[39]A. K. M. Haque and S. Tasmin, “Security Threats and Research Challenges of IoT-A Review,” *arXiv preprint arXiv:2101.03022*, 2020.

[40]K. B. Wright, “Researching Internet-based populations: Advantages and disadvantages of online survey research, online questionnaire authoring software packages, and web survey services,” *Journal of computer-mediated communication*, vol. 10, no. 3, p. JCMC1034, 2005.

[41]S. Almalki, “Integrating Quantitative and Qualitative Data in Mixed Methods Research--Challenges and Benefits.,” *Journal of education and learning*, vol. 5, no. 3, pp. 288–296, 2016.

Information about the authors:

Dr. Ali AbuAbid is an Assistant Professor of Information Technology at the College of Computing and Informatics, Saudi Electronic University. His academic journey led him to obtain a Ph.D. from Monash University, Melbourne, Australia, where he delved into cutting-edge research in the field of Information Technology. With a focus on bridging the gap between academia and industry, Dr. AbuAbid's research interests span across cybersecurity, Internet of Things (IoT), and the adoption of technological innovations by organizations. His commitment to advancing knowledge in these domains is reflected in a series of impactful publications and active participation in international conferences.