*International Journal on Recent and Innovation Trends in Computing and Communication*
*ISSN: 2321-8169 Volume: 11 Issue: 9*
***Article Received:*** *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

# IoT Safeguarding in Saudi Tourism Sector: Crafting a Preliminary Security Model for Enhancing Cyber Resilience

**Sarah Alghamdi**
Information Technology Department
Saudi Electronic Universit
Riyadh, Saudi Arabia
Abuabid27@hotmail.com

**Ali Abuabid (corresponding author)**
Information Technology Department
Saudi Electronic Universit
Riyadh, Saudi Arabia
a.abuabid@seu.edu.sa

**Abstract**— Incorporating the Internet of Things (IoT) has transformed technological landscapes, facilitating seamless communication across diverse devices and systems. However, this increased connectivity exposes critical sectors, including government and tourism, to elevated cybersecurity risks. There is a lack of knowledge regarding how organizations within the Saudi tourism sector address the cybersecurity risks associated with IoT systems. While much of the existing IoT literature concentrates on adopting IoT systems, a better understanding can be attained by proposing a preliminary research model encompassing the most significant factors influencing IoT security and related cybersecurity attacks. Despite limited empirical research on IoT security adoption in the Saudi tourism sector, this study seeks to address this gap. Motivated by this concern, this research investigates IoT security among Saudi organizations in the government tourism sector by developing a research model. inspired by the Technology Acceptance Model (TAM) literature. The model incorporates a total of eight factors (privacy, confidentiality, data integrity, access control, availability, trust, IoT standards and policies, and IoT Awareness) and seven cybersecurity attacks (denial of service (DoS & DDoS), replay attack, eavesdropping attack, man-in-the-middle (MiTM) attack, spoofing attack, Sybil attack, and physical attack) identified from various literature sources. The proposed research model is a valuable tool for understanding IoT security in Saudi tourism, offering guidelines for organizations considering introducing IoT security measures. These guidelines highlight specific factors that tourism organizations should consider, enhancing the likelihood of successful IoT security adoption in the tourism context. Additionally, this study encourages IoT researchers to replicate the research in another industry sector within Saudi Arabia or other countries, particularly within the Arabian Gulf region.

**Keywords**- IoT Security; Factors; IoT Attacks; Saudi; Tourism; Model

## I. INTRODUCTION

### A. Significance of IoT in Enhancing Tourism Services in Saudi Arabia

The widespread incorporation of technology and automation has emerged as a defining characteristic across various industries, yielding efficiency, productivity, and scalability enhancements while concurrently reducing costs and labor demands. Notably, the central focus in recent years has been on the burgeoning domain of the Internet of Things (IoT), A technological framework that enables the linking of common devices to the Internet [1]. This connectivity empowers remote control and monitoring from virtually any location globally. Within the expansive spectrum of IoT, devices range from simple sensors monitoring temperature and humidity to sophisticated machines capable of detecting and responding to environmental changes. The applications of IoT extend across numerous sectors, including smart homes, industrial automation, healthcare monitoring, transportation systems, and beyond [2].

Recognizing the transformative potential of IoT, the Saudi government has ardently championed its adoption

*International Journal on Recent and Innovation Trends in Computing and Communication*
*ISSN: 2321-8169 Volume: 11 Issue: 9*
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

through multifaceted initiatives and programs. This is particularly evident in endeavors to develop smart cities, enhance infrastructure, and augment overall quality of life [1]. Aligned with the national trajectory outlined in the Saudi Vision 2030, a comprehensive long-term development plan, there is a strategic emphasis on digital transformation and integrating emerging technologies, notably IoT systems, within the vibrant tapestry of the tourism sector.

According to [2], the symbiotic relationship between IoT adoption and the realization of Vision 2030 in the tourism sector is underscored by its contributions:

- Economic Diversification: Serving as a pivotal source of revenue diversification, the tourism sector offers an alternative to the longstanding reliance on the oil industry.
- Job Creation: As a significant contributor to employment in Saudi Arabia, the tourism industry is positioned to create numerous job prospects in sectors like hospitality, transportation, and entertainment.
- Foreign Investment: The flourishing tourism sector has attracted substantial foreign investment, contributing significantly to economic growth.
- Cultural Exchange: Tourism serves as a conduit for cultural exchange between Saudi Arabia and other nations.
- Infrastructure Development: To fortify the burgeoning tourism sector, considerable infrastructure development, encompassing airports, hotels, resorts, theme parks, and various attractions, is imperative. This benefits tourists and enhances the overall quality of life for residents.

The Saudi government's unwavering commitment to IoT is evident in many projects to bolster tourism. Table 1 delineates the IoT contributions to prominent development projects, ranging from infrastructure management to facilitating e-visa applications and using augmented reality (AR) and virtual reality (VR) to enrich the tourist experience [3]

TABLE l. IoT CONTRIBUTIONS TO PROMINENT DEVELOPMENT PROJECTS IN SAUDI TOURISM SECTOR (Source, [3])

| IoT Contribution | Project Description | Project Name |
|---|---|---|
| IoT is used to monitor and manage the infrastructure, such as using sensors to detect traffic congestion and adjust traffic signals accordingly or using smart building systems to optimize energy usage in hotels. | The government has invested heavily in developing infrastructure such as airports, roads, and hotels to support tourism. | Investment in infrastructure |
| IoT is used to streamline the e-visa application process by using biometric authentication for identity verification or Blockchain technology for secure data storage. | The implementation of an electronic visa system has simplified the process for tourists to acquire visas and travel to Saudi Arabia. | E-visa system |
| IoT is Used to enhance the tourist expectation about Saudi Arabia's augmented reality (AR) or virtual reality (VR) to provide immersive tours of cultural and natural attractions. | The government has also introduced tourist visas for the first time, allowing visitors worldwide to explore the country's cultural and natural attractions. | Tourist visas |
| IoT targets specific demographics with personalized marketing messages, such as using social media analytics to identify potential tourists and tailor ads accordingly. | The Saudi Commission for Tourism and National Heritage (SCTH) has launched various marketing campaigns to promote tourism in the country. | Marketing campaigns |
| IoT enhances the cultural event experience, such as using AR or VR to provide interactive exhibits or implementing smart crowd management systems for safety and security. | The government has organized various cultural events such as festivals, concerts, and exhibitions to attract tourists. | Cultural events |

*International Journal on Recent and Innovation Trends in Computing and Communication*
*ISSN: 2321-8169 Volume: 11 Issue: 9*
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

| | | |
|---|---|---|
| IoT is used for heritage site conservation efforts, such as using drones for aerial surveys or implementing smart irrigation systems for sustainable landscaping. | The government is also investing in preserving heritage sites such as Al-Ula and Mada'in Saleh, major tourist attractions. | Heritage sites preservation |

This confluence of technological innovation and economic diversification, witnessed firsthand as a citizen of Saudi Arabia, reflects a transformative journey toward a diversified economic landscape. The evolution of the tourism sector, leveraging the nation's geographical splendor, rich cultural heritage, and visionary projects, is a testament to Saudi Arabia's commitment to reshaping its economic narrative beyond the traditional reliance on oil and gas [1].

### B. Research Problem Statement

The security landscape of IoT adoption in Saudi Arabia is contingent on several factors, encompassing the nature of employed IoT devices, the efficacy of security measures implemented by governmental bodies and individuals, and the potential threats and vulnerabilities inherent in IoT technology. Like other nations, Saudi Arabia confronts cybersecurity challenges linked to IoT devices, including but not limited to data breaches, hacking endeavors, and unauthorized access. Consequently, it becomes imperative to institute robust security protocols such as encryption methodologies, firewalls, and consistent software updates, thereby safeguarding the integrity and privacy of IoT systems within the Kingdom of Saudi Arabia (KSA).

Security concerns are a central focus among the critical obstacles that impede the widespread adoption of IoT technology in Saudi organizations. It is crucial to comprehensively understand all factors contributing to these challenges within the Saudi context. By distinctly identifying and mitigating the influence of each factor, there is potential to enhance the adoption rate of IoT technology, thereby cultivating a more secure and resilient IoT ecosystem in the Kingdom.

### C. Research Goal and Questions

The primary objective of this research paper is to develop a preliminary research model to examine the factors influencing IoT security within the Saudi governmental tourism sector and the most frequent cybersecurity attacks targeting this sector. This overarching goal is articulated through the following specific research questions:

Q1: What are the cybersecurity factors that influence the adoption of IoT systems in the Saudi government tourism sector?

Q2: What are the most cybersecurity attacks targeting IoT systems in the Saudi government tourism sector?

### D. Organization of the Research

This research is structured into several sections, each contributing to the comprehensive exploration of IoT security factors in the Saudi governmental tourism sector. The introduction outlines the researcher's interests and motivations regarding security factors and attacks influencing IoT security in the tourism sector. Following this, the literature review explores existing research in IoT security factors and attacks, conducting an in-depth analysis of current challenges and factors hindering the development of IoT security in the Saudi governmental tourism sector. This chapter also elucidates each factor, delineating its positive and negative impacts. Finally, the paper's conclusion summarizes the essential findings and the research contributions to IoT security implementation in the Saudi tourism sector. It also outlines potential avenues for future researchers.

## II. LITERATURE REVIEW

### A. IoT security in the Saudi Governmental tourism sector

IoT is a rapidly growing field that is changing how people interact with the environment, significantly transforming many aspects of modern life. The definitions of IoT systems are many and varied. According to [4], the term "IoT" is characterized as a system in which the Internet is linked to the tangible world through pervasive sensors, encompassing RFID (Radio-frequency identification). Meanwhile, [5] has published a clear and concise definition of IoT as "a cyber-physical ecosystem of interconnected sensors and actuators, which enable decision-making." It is also defined as the extensive network of connected devices on the Internet that encompasses smartphones, tablets, and virtually anything equipped with sensors, such as cars, machinery in production plants, jet engines, oil drills, wearable devices, and various other items [6]. For this research paper, 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 [7].

IoT security protects IoT devices and systems from unauthorized access, misuse, and exploitation [6]. IoT systems' security is crucial because these Ensuring the security of IoT systems is paramount as these devices frequently gather and transmit sensitive data, including personal, health, and financial information [7]. A security breach can significantly harm individuals and organizations, including loss of privacy, financial loss, and damage to reputation [8].

Numerous countries globally recognize the significance of IoT systems and have cautiously begun incorporating such technologies across various industry sectors, acknowledging the accompanying risks. For instance, the United States stands out as one of the principal markets for Internet of Things (IoT) devices. Nevertheless, the extensive integration

*International Journal on Recent and Innovation Trends in Computing and Communication*
*ISSN: 2321-8169 Volume: 11 Issue: 9*
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

of IoT devices has introduced novel security challenges that necessitate attention. A primary obstacle in securing IoT devices in the U.S. lies in the abundance and diversity of available devices [9]. Many of these devices are developed and produced by small startups, which may lack the resources or expertise to incorporate robust security features, rendering them susceptible to cyberattacks [9]

Similarly, China is recognized as one of the largest markets for IoT devices [10]. Among the significant challenges in securing IoT devices in China is the absence of standardized norms and regulations for IoT security. Although some regulations are in place for cybersecurity and data protection, specific regulations addressing IoT security are currently lacking [11]. This dearth of regulatory frameworks can complicate the assurance of IoT device security, as manufacturers may not clearly understand the requisite security features [8].

In Saudi Arabia, as in other countries, the government has recognized the importance of IoT systems and has promoted its adoption through various initiatives and programs [12]. For instance, the National Cybersecurity Authority (NCA) has issued guidelines for securing IoT devices and systems [13], and the Saudi Standards, Metrology, and Quality Organization (SASO) has developed standards for IoT security [14]. Additionally, these entities have implemented various initiatives to enhance cybersecurity awareness and fortify the protection of IoT systems against cyber threats. This involves the development of centralized regulations and standards for IoT security, the establishment of a national cybersecurity center, and investments in cybersecurity research and development [12]. One of the principal challenges in securing IoT devices in Saudi Arabia is the lack of awareness among consumers and businesses [15]. Many individuals are unaware of the security risks associated with IoT devices and may not implement appropriate measures to secure their devices. This renders them susceptible to hackers who can exploit the devices to access sensitive information or launch attacks on other systems [15].

Various government sectors oversee distinct governance and public service areas within the Saudi Arabian governance framework. These sectors may vary based on definitions and classifications, but commonly recognized entities include agencies, councils, commissions, authorities, and ministries [16]. These sectors are organized into three categories according to their functions and responsibilities. The executive branch comprises ministries, authorities, and agencies tasked with executing government policies and providing public services. An illustrative instance, such as the Tourism sector, serves as a central focus within this research paper. The legislative branch includes the Shura Council, an advisory body reviewing and proposing new laws and regulations, and the Council of Ministers, which possesses the authority to approve laws and policies. The judicial branch comprises the courts and other legal institutions tasked with upholding the law and ensuring justice [17].

The tourism sector is pivotal in realizing Vision 2030 in Saudi Arabia, serving as a critical driver of economic growth, diversification, job creation, and foreign investment [18]. As per the World Travel and Tourism Council (WTTC), the direct economic contribution of the travel and tourism sector to Saudi Arabia's GDP amounted to SAR 97.9 billion (USD 26.1 billion) in 2019, with a projected annual growth rate of 5.4%, reaching SAR 158.2 billion (USD 42.2 billion) by 2029 (Travel & Tourism Economic Impact [19]. The Saudi government has committed substantial investments to enhance tourism infrastructure and promote the country as a premier tourist destination, aiming to attract 100 million visitors annually by 2030 [20]. This strategic focus on tourism is anticipated to impact the country's GDP in the coming years significantly. The travel and tourism sector emerged as critical in realizing Vision 2030 by contributing to economic diversification, job creation, foreign investment, cultural exchange, and infrastructure development [2]. Consequently, continuing investment in this sector is essential for Saudi Arabia's long-term goals.

### B. Crafting a Preliminary IoT Security Model in the Saudi Tourism Sector

Integrating IoT systems has become integral to contemporary lifestyles, exerting a pervasive influence across diverse sectors in Saudi Arabia. While these systems offer numerous advantages, they concurrently introduce security considerations and challenges that necessitate careful attention. Through a comprehensive review of the literature about factors influencing IoT systems adoption, it has been identified that IoT is primarily influenced by two categories: security factors and attacks. The literature reveals that researchers have reported 25 factors and 36 attacks, emphasizing their direct impact on IoT security systems. In the context of this study, a systematic shortlisting approach has been developed to identify the most pertinent factors. The devised **shortlisting approach** is outlined as follows:

a. Inclusion of the most frequently mentioned factors and attacks in the literature.

b. Inclusion of factors that appear four times or more in the literature.

c. Inclusion of attacks that occur five times or more in the literature.

d. Inclusion of factors and attacks specifically relevant to the Saudi context.

After applying the above shortlisting approach, **eight** factors out of **25** and **seven** attacks out of 36 have been determined to directly impact the IoT systems security in the Saudi tourism sector. Table 2 summarizes selected studies conducted on security factors influencing IoT systems.

TABLE 2. SELECTED LITERATURE SOURCES OF IOT SECURITY

| Literature Sources | Research Methodology | IoT Applications | Industry Sector | Country |
|---|---|---|---|---|

| | | | | |
|---|---|---|---|---|
| [1] | Qualitative analysis using open-ended interviews | Health care services | Hospitals and Medical Cities | Saudi Arabia |
| [12] | Quantitative research method | Cloud Computing | Smart homes IOT-based devices | Saudi Arabia |
| [21] | Quantitative research method | Blockchain | Decentralize, reliable, and secure environment | Saudi Arabia |
| [22] | Literature Review | IoT and machine-to-machine(M2M) | Developing country | Saudi Arabia |
| [8] | Quantitative Survey | Systems in IoT professional's devices | IoT device manufacturers | USA |
| [23] | Qualitative approach | Social Internet of Things (SIoT) | Technology/Information Technology Organizations | Europe |
| [24] | Qualitative observations in IoT component interaction | Distributed ledger-based Blockchain (DL-BC) | Common operating picture for Wireless sensor network devices | Malaysia |

Moreover, Table 3 illustrates the finalization of the shortlisting procedure for gathered factors, with the retention of only eight selected factors.

TABLE 3. 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 |

Subsequently, Table 4 furnishes comprehensive descriptions and items pertaining to each selected factor.

TABLE 4. FACTORS AFFECTING IOT SECURITY IN THE TOURISM SECTOR AND THEIR ITEMS

| Factors | Description | Items |
|---|---|---|
| Privacy | 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<br>2. Transparency<br>3. Consent management<br>4. Privacy policies |
| Confidentiality | 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)<br>2. Encryption<br>3. Authentication |
| Data integrity | Data integrity refers to the assurance that information is trustworthy, accurate, complete, and | 1. Data validation<br>2. Error detection and correction<br>3. Audit trails<br>4. Redundancy |

| | | |
|---|---|---|
| | consistent using IoT technologies helps in the safety of data from unauthorized changes. | |
| Access control | 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<br>2. Authorization<br>3. Intrusion detection/prevention systems (IDS/IPS): |
| Availability | 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 how easily businesses and individuals can access and use these technologies. | 1. Device uptime<br>2. Response time<br>3. Mean Time Between Failures (MTBF<br>4. Mean Time to Repair (MTTR) |
| Trust | 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<br>2. User engagement |
| IoT standards and policies | 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<br>2. Availability of IoT policy |
| IoT Awareness | 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<br>2. Availability of periodical training |

*Factor 1: Privacy*

Privacy is a significant concern regarding IoT implementation in the world. One of the main privacy concerns with IoT systems in Saudi Arabia is the collection of personal data [12]. With the increased usage of smart devices, individuals share personal information without realizing its privacy impact. IoT devices such as fitness trackers, smartwatches, and other wearables collect health data, location information, and other personal data, which could be misused if they fall into the wrong hands [25]. Also, there is a lack of transparency regarding data collection and usage by IoT systems. Most IoT devices collect data without users' knowledge, and how it is used is often unclear. Users need to have control over their data, and organizations must be transparent about how they are collecting and using personal information [12]

In contrast, there are positive impacts of privacy in the process of adopting IoT, including customized user experience based on their data, preferences, and behaviors. This allows for a more efficient and personalized experience,

*International Journal on Recent and Innovation Trends in Computing and Communication*
*ISSN: 2321-8169 Volume: 11 Issue: 9*
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

improving customer satisfaction. Also, IoT devices can help automate processes, reducing the workload on individuals and increasing productivity. This can lead to higher efficiency and lower costs for organizations. However, these advantages are accompanied by a negative impact, such as needing more control over personal data. IoT devices collect a vast amount of personal data, and users may have little control over how this data is collected, stored, and used [8]. Therefore, this study suggests that privacy should positively influence IoT security adoption by the Saudi tourism sector. Hence, the following hypothesis is suggested.

**H1: Privacy positively influences the Saudi tourism sector to adopt IoT security measures.**

*Factor 2: Confidentiality*

Confidentiality within the context of IoT pertains to safeguarding sensitive data against unauthorized access, disclosure, or utilization. This sensitive information encompasses personal data, financial details, trade secrets, and other exploitable data by cybercriminals. Since IoT systems depend on the aggregation and transmission of data from diverse devices and sensors, maintaining the confidentiality and security of this data is paramount. An inherent challenge in ensuring confidentiality in IoT lies in the substantial volume of data generated by these systems [23]

While confidentiality guarantees the safeguarding of sensitive information, enhances trust, and ensures compliance with regulations, it results in limitations on data sharing, heightened system complexity, and diminished usability of IoT systems and devices. Implementing confidentiality measures necessitates significant resources and technical expertise [26]. Additionally, effective implementation of confidentiality measures can incur substantial costs, particularly for small businesses or organizations with limited resources. Therefore, this study suggests that confidentiality should positively influence IoT security adoption by the Saudi tourism sector. Hence, the following hypothesis is suggested.

**H2: A high level of confidentiality positively influences the Saudi tourism sector to adopt IoT security measures.**

*Factor 3: Data integrity*

Data integrity, within the context of IoT, pertains to safeguarding data against unauthorized alterations, ensuring its accuracy and reliability. In the realm of IoT, data integrity faces potential compromise through various means, including data tampering, manipulation, or loss, presenting significant challenges, especially in critical industries like healthcare, energy, and transportation [27]

Several noteworthy challenges associated with data integrity in IoT encompass complexities and cybersecurity threats. IoT systems often exhibit intricacies involving many devices, sensors, and data streams, making the assurance of data integrity across these components a formidable task. Additionally, cybersecurity threats, such as data breaches or hacks, pose risks to data integrity. The evolving landscape of IoT technology introduces new threats, necessitating continual monitoring and adaptation of data integrity measures [23]. Therefore, this study suggests that data integrity should positively influence IoT security adoption by the Saudi tourism sector. Hence, the following hypothesis is suggested.

**H3: Data Integrity positively influences the Saudi tourism sector to adopt IoT security measures.**

*Factor 4: Access control*

Access control is a crucial facet of IoT technology in Saudi Arabia, involving regulating access to IoT devices and data exclusively for authorized personnel [28]. Access control measures aim to forestall unauthorized access, a potential threat that could compromise the security and privacy of both IoT systems and their associated data.

Prominent challenges associated with access control significantly impact the successful implementation of IoT in the tourism sector. Issues of scalability and cost pose noteworthy hindrances [28]. The expansive growth potential of IoT systems necessitates scalable access control measures capable of adapting to evolving requirements. Moreover, implementing effective access control measures can incur substantial costs, particularly for smaller businesses or organizations with limited resources. Therefore, this study suggests that access control positively influences IoT security adoption by the Saudi tourism sector. Hence, the following hypothesis is suggested.

**H4: Access Control positively influences the Saudi tourism sector to adopt IoT security measures.**

*Factor 5: Availability*

Availability is a critical aspect of IoT security, and it refers to the ability of IoT devices and systems to function and remain accessible in the event of disruptions, such as power outages, network failures, or cyberattacks [29]. The availability of IoT systems is critical to their adoption, particularly in industries where uptime is essential, such as healthcare, transportation, and manufacturing, and it significantly impacts the efficiency, productivity, and safety of these industries.

IoT devices from different manufacturers may not work together seamlessly, creating interoperability issues and challenging ensuring availability across different systems. Also, availability can be compromised by cybersecurity threats such as denial of service attacks, data breaches, or hacks [29]. As IoT technology evolves, new threats may emerge, requiring constant monitoring and adaptation of availability measures. Therefore, this study suggests that availability positively influences IoT security adoption by the Saudi tourism sector. Hence, the following hypothesis is suggested.

**H5: Availability positively influences the Saudi tourism sector to adopt IoT security measures.**

*Factor 6: Trust*

*International Journal on Recent and Innovation Trends in Computing and Communication*
*ISSN: 2321-8169 Volume: 11 Issue: 9*
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

Trust, within the context of IoT systems and devices, encompasses the confidence that these entities will function as intended, provide accurate data, and safeguard the privacy and security of users. The absence of trust may lead to user reluctance to adopt IoT devices, limiting these technologies' potential advantages [30]. The establishment of trust necessitates a holistic approach that encompasses aspects of security, reliability, privacy, and transparency. Organizations must ensure that their IoT devices exhibit robust security measures, reliability, and data collection and utilization transparency. Adherence to relevant regulations and industry standards further builds trust among users.

Challenges affecting IoT's trustworthiness include privacy and data integrity concerns. Users may harbor apprehensions regarding the privacy implications of IoT devices, especially when these devices gather sensitive data such as health or financial information [30]. Therefore, this study suggests that trust positively influences IoT security adoption by the Saudi tourism sector. Hence, the following hypothesis is suggested.

**H6: Trust positively influences the Saudi tourism sector to adopt IoT security measures.**

*Factor 7: IoT standards and policies*

The availability of cybersecurity standards and policies plays a crucial role in ensuring the security and effective implementation of IoT in Saudi Arabia. However, vulnerabilities in these standards and policies can considerably impact IoT adoption. Some weaknesses in the standards and policies pertaining to IoT in Saudi Arabia include a lack of standardization and inadequate testing and certification processes [31]. The absence of universal standards for IoT devices and systems may result in interoperability issues, making it challenging for users to assess different devices' security, reliability, and privacy. This can contribute to a lack of trust in IoT, impeding its adoption. Inadequate testing and certification processes for IoT devices can undermine confidence in the quality, reliability, and security of these devices, resulting in reduced adoption rates and limiting the potential benefits of IoT.

The impact of weak standards and policies on IoT adoption is substantial. Users are less inclined to adopt IoT devices and systems perceived as insecure, unreliable, or non-compliant with regulations [31]. This reluctance can lead to slower adoption rates, decreased market penetration, and missed opportunities for innovation and growth. Therefore, this study suggests that IoT standards and policies positively influence IoT security adoption by the Saudi tourism sector. Hence, the following hypothesis is suggested.

**H7: IoT Standards and Policies positively influence the Saudi tourism sector to adopt IoT security measures.**

*Factor 8: IoT Awareness*

Insufficient knowledge of IoT technology constitutes a noteworthy challenge that hinders its adoption. This lack of awareness and understanding stems from various factors, such as a limited comprehension of the potential benefits offered by IoT and a restricted understanding of the associated security and privacy implications [32]

Efforts to enhance awareness about IoT involve elucidating how IoT devices operate and underscoring the advantages of their usage. Additionally, collaboration with experts in the field of information technology can contribute to raising awareness and disseminating knowledge about IoT. According to [32], heightened IoT awareness positively correlates with users' understanding of IoT privacy and security. Therefore, this study suggests that IoT Awareness positively influences IoT security adoption by the Saudi tourism sector. Hence, the following hypothesis is suggested.

**H8: IoT Awareness positively influences the Saudi tourism sector to adopt IoT security measures.**

C. Cyber security attacks targeting IoT systems in the Saudi Tourism Sector

Cybersecurity attacks encompass any malicious activities directed at a computer system, network, or device intending to cause damage, disruption, theft, or compromise of data or information [15]. These attacks can be perpetrated by individuals or organized groups, targeting entities such as individuals, businesses, governments, or other organizations. The escalating prevalence of connected devices across various sectors has led to a rise in cybersecurity attacks specifically targeting IoT systems in recent years.

A comprehensive analysis was undertaken after conducting a thorough literature review on IoT security, as depicted in Table 5. All mentioned attacks were cataloged, and their frequencies were calculated, identifying 36 attacks. From this pool, **seven** attacks were shortlisted based on a frequency threshold of 5 or more. However, discerning the specific types of attacks from this shortlist that have been experimentally explored within the Saudi context remains undisclosed.

TABLE 5. HIGHEST FREQUENT ATTACKS TARGETING IOT SECURITY IN THE TOURISM SECTOR

| Attacks | Frequency |
|---|---|
| 1. Denial Of Service (DoS & DDoS) attack | 13 |
| 2. Replay Attack | 8 |
| 3. Eavesdropping Attack | 7 |
| 4. Man-in-The-Middle (MiTM) Attack | 7 |
| 5. Spoofing Attack | 6 |
| 6. Sybil attack | 6 |
| 7. Physical attacks | 5 |

*International Journal on Recent and Innovation Trends in Computing and Communication*
*ISSN: 2321-8169 Volume: 11 Issue: 9*
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

*Attack 1: Denial of Service (DoS & DDoS) attack*

In recent years, the propagation of IoT devices has made DoS and DDoS attacks increasingly attractive targets for these types of attacks. A Denial of Service (DoS) attack is 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 [33].

DoS and DDoS attacks overwhelm a network or system with traffic, rendering it unusable. In a DoS attack, the attacker uses a single device or computer to send a large volume of traffic to a target server or website, effectively causing it to crash or become unavailable. In a DDoS attack, the attacker uses a network of compromised devices, known as a botnet, to launch the attack. This makes it more difficult to stop the attack as the traffic comes from multiple sources [33].

Some of the challenges related to DoS and DDoS attacks in IoT adoption include limited processing power, whereby many IoT devices have limited processing power and memory, which makes them more vulnerable to overload from a flood of traffic. This can make them attractive targets for attackers looking to launch DoS and DDoS [23]. Also, there is a challenge of scalability whereby as the number of IoT devices continues to grow, the potential attack surface for DoS and DDoS attacks also increases. This challenges network administrators, who must ensure that all devices are properly secured and updated [23]

As with any other organization, the KSA government sector may be vulnerable to DoS and DDoS attacks that target their IoT systems. Attackers may specifically target IoT devices used by government agencies, such as sensors, surveillance cameras, and other networked devices used for various functions [33]. Attorneys may target IoT systems in the KSA government sector through botnets. Botnets are networks of compromised devices that a central attacker or group of attackers controls. Attackers can use botnets to launch massive DDoS attacks against a target system or network, causing it to become overwhelmed and unavailable [17].

*Attack 2: Replay Attack*

Within the scope of IoT, replay attacks denote 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. Subsequently, the attacker replays the captured message to assume the identity of the original sender, doing so without the knowledge or consent of the intended recipient.

In nations characterized by a pronounced cybersecurity threat landscape, such as Russia and China, replay attacks emerge as a particularly pressing concern [34]). These countries are noted for being involved in state-sponsored cyberattacks and possessing advanced capabilities in this domain. Consequently, IoT devices and networks within these regions face an elevated risk of being targeted by replay attacks and other cyber threats.

Replay attacks pose a substantial threat to IoT systems within the governmental sector of Saudi Arabia due to the extensive integration of IoT devices and networks in this domain. The Saudi government has invested substantially in developing and deploying IoT systems to bolster smart city initiatives, enhance public services, and fortify national security [35]. These systems find application in diverse contexts, including transportation, energy management, and public safety. In the KSA government sector, replay attacks could yield severe consequences, including compromising sensitive information, disrupting critical services, and national security breaches. For instance, an attacker could execute a replay attack on an IoT device utilized for surveillance, potentially circumventing security measures and gaining unauthorized access to secure locations or obtaining sensitive information [35]

Replay attacks introduce several challenges to the adoption of IoT devices and networks. A primary challenge lies in the intricacy of IoT systems, often involving multiple devices and networks that necessitate secure communication with each other [36]). This complexity can pose difficulties in identifying and mitigating vulnerabilities susceptible to exploitation in a replay attack.

*Attack 3: Eavesdropping Attack*

An eavesdropping attack is 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[37]. This type of attack is particularly concerning in the IoT environment because many IoT devices are designed to continuously transmit data over the internet, making it easier for an attacker to intercept and analyze the data for sensitive information. For example, an attacker may be able to obtain login credentials or personal information, such as credit card numbers or medical data, by intercepting traffic between an IoT device and a server.

In the US, eavesdropping attacks have targeted various entities, including government agencies, businesses, and individuals. One notable example is the NSA's PRISM program, which was revealed by Edward Snowden in 2013[9]. The program collected data from various tech companies, including Google, Facebook, and Apple, which raised concerns about privacy violations.

It is possible for eavesdropping attacks to target IoT systems in the Saudi government's tourism sector, just like in any other country. IoT devices, such as sensors, cameras, and other network-connected devices, are becoming increasingly popular in government organizations and can provide valuable insights and data. However, these devices can also pose security risks if not properly secured, especially if they are connected to the internet without appropriate security measures in place [37].

Eavesdropping attacks can pose significant challenges to adopting IoT technology, particularly in areas where security is a primary concern, such as the government sector. Some of the challenges related to eavesdropping attacks in IoT adoption include security concerns, trust issues, legal

*International Journal on Recent and Innovation Trends in Computing and Communication*
*ISSN: 2321-8169 Volume: 11 Issue: 9*
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

implications, and complexity in regard to securing IoT systems.

*Attack 4: Man-in-The-Middle (MiTM) Attack*

The MiTM attack is a type of cyber-attack in which a malicious actor intercepts and alters communications between two parties who believe they are communicating directly [7]. In the context of the IoT, MiTM attacks are particularly concerning because many IoT devices are connected to the internet and can be vulnerable to this type of attack.

The United States has experienced several high-profile MiTM attacks, particularly in the financial sector. In 2013, target Corporation experienced a breach due to a MiTM attack that resulted in the theft of millions of customers' credit card information[7]. In 2017, Equifax, one of the largest credit bureaus in the United States, experienced a MiTM attack that resulted in the theft of the sensitive personal data of millions of people [7].

While there is limited public information available on the specific incidents of MiTM attacks targeting IoT systems in the Saudi Arabian government sector, it is safe to assume that such attacks could significantly impact the country's infrastructure and sensitive government operations. As a global oil and gas industry leader, Saudi Arabia has invested heavily in IoT systems to optimize its production and operational efficiency [21]. These IoT systems are often interconnected with other critical infrastructure systems such as transportation, power grids, and telecommunications. A MiTM attack on an IoT system in the Saudi Arabian government tourism sector could allow an attacker to intercept and alter communication between devices, potentially leading to the theft of sensitive data, unauthorized access to government networks, and even control of critical infrastructure systems[21]. This could result in significant financial losses, operational disruptions, and damage to the country's reputation.

*Attack 5: Spoofing Attack*

A spoofing attack is a type of cyber-attack in which an attacker impersonates a legitimate device or system to gain unauthorized access or manipulate data [38]. These attacks can take different forms, such as MAC address spoofing, IP address spoofing, or DNS spoofing. Spoofing attacks have heavily affected India, particularly in the financial industry [24]. One of India's most significant spoofing attacks was the 2018 Punjab National Bank scam, in which hackers used spoofed SWIFT messages to steal over $2 billion from the bank. The Indian government has implemented various measures to combat spoofing attacks, such as mandating the use of Blockchain technology in stock trading to prevent spoofing of trade orders[24].

There have been reports of spoofing attacks targeting IoT systems in the Saudi Arabian government tourism sector. These attacks aim to exploit vulnerabilities in IoT devices and systems, which can lead to data breaches, malware infections, and other cyber threats [39]. Here are some ways in which spoofing attacks can target IoT systems in the Saudi Arabian government tourism sector, the impersonation of legitimate devices, DNS spoofing, and IP address spoofing.

*Attack 6: Sybil attack*

The Sybil attack constitutes a security threat characterized by a malevolent actor creating numerous counterfeit identities with the intention of gaining control or manipulating a given system. Within the Internet of Things (IoT) realm, a Sybil attack manifests when an assailant generates multiple spurious devices or nodes within a network, masquerading as authentic entities.

In technologically advanced nations with sophisticated IoT infrastructures, such as the United States, the impact of a Sybil attack could be significant. IoT devices are widely used in critical infrastructure systems such as healthcare, transportation, and energy, making them vulnerable to attack. However, the US government has taken steps to mitigate this threat by introducing legislation such as the IoT Cybersecurity Improvement Act, which sets security standards for IoT devices purchased by the government [9].

In Saudi Arabia, the threat of Sybil attacks on IoT devices and networks is a concern, as the country has a growing IoT infrastructure that is becoming increasingly integrated into critical infrastructure systems. One potential target for Sybil attacks in Saudi Arabia is the country's energy sector, which relies heavily on IoT devices to monitor and control operations. A successful Sybil attack on these devices could disrupt the energy supply, potentially causing significant economic and social consequences [22].

A critical challenge posed by the Sybil attack is data manipulation. Sybil attackers can manipulate data by flooding the network with fake data or manipulating the data received from legitimate devices [38]. This can cause inaccurate or inconsistent data, leading to incorrect decisions being made based on the data.

*Attack 7: Physical attacks*

In the sphere of the IoT, a physical attack 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 [40]. The objective of such an attack is typically to pilfer sensitive data, disrupt services, or induce physical damage.

Saudi Arabia has encountered a series of prominent cyber-attacks directed at its governmental institutions in recent years. Notably, in 2017, the Saudi Arabian Ministry of Foreign Affairs fell victim to a cyber-attack targeting over 6,000 accounts, resulting in a substantial data breach [41]). Subsequently, in 2018, another cyber-attack was launched on the Saudi Arabian government and financial sector. This attack employed the notorious Shamoon malware, leading to the destruction of data and the disruption of services [41].

IoT devices exhibit diverse forms, encompassing varying levels of computing power, connectivity, and security features [42]. The heterogeneity of IoT devices poses a challenge in implementing standardized security protocols that can be universally applicable across all devices. This

*International Journal on Recent and Innovation Trends in Computing and Communication*
*ISSN: 2321-8169 Volume: 11 Issue: 9*
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

presents a formidable obstacle in establishing comprehensive security measures for IoT ecosystems.

D. Architectural Model: Designing the IoT Security Blueprint

This paper has presented factors and cybersecurity attacks that aid or hinder implementing and adopting IoT security in the Saudi tourism sector. By synthesizing the factors and cybersecurity attacks outlined and discussed in Sections B and C, the research model is depicted in Figure 1. This model aims to comprehend the integration of security measures within the IoT framework. The objective is pursued by systematically identifying key factors influencing the adoption of IoT security, specifically within the governmental tourism sector in Saudi Arabia. Additionally, the model endeavors to discern the significance of cybersecurity attacks outlined in the literature that specifically target the aforementioned sector.

Following a filtering process (outlined in Section B) designed to condense the identified factors and attacks relevant to IoT security (as discussed in Section B and presented in Table 4), it was determined that 8 out of 25 factors hold particular significance in influencing IoT security in the Saudi tourism sector. Simultaneously, a total of 7 out of 36 cybersecurity attacks targeting IoT devices in the Saudi tourism sector (discussed in Section C and delineated in Table 5) were identified. In addition, a total of 8 hypotheses were derived (discussed in Section B and presented in Table 6).

TABLE 6. LIST OF DERIVED HYPOTHESES

| No. | Hypotheses Description |
|---|---|
| H1 | Privacy positively influences the Saudi tourism sector to adopt IoT security measures. |
| H2 | A high level of Confidentiality positively influences the Saudi tourism sector to adopt IoT security measures. |
| H3 | Data Integrity positively influences the Saudi tourism sector to adopt IoT security measures. |
| H4 | Access Control positively influences the Saudi tourism sector to adopt IoT security measures. |
| H5 | Availability positively influences the Saudi tourism sector to adopt IoT security measures. |
| H6 | Trust positively influences the Saudi tourism sector to adopt IoT security measures. |
| H7 | IoT Standards and Policies positively influence the Saudi tourism sector to adopt IoT security measures. |
| H8 | IoT Awareness positively influences the Saudi tourism sector to adopt IoT security measures. |

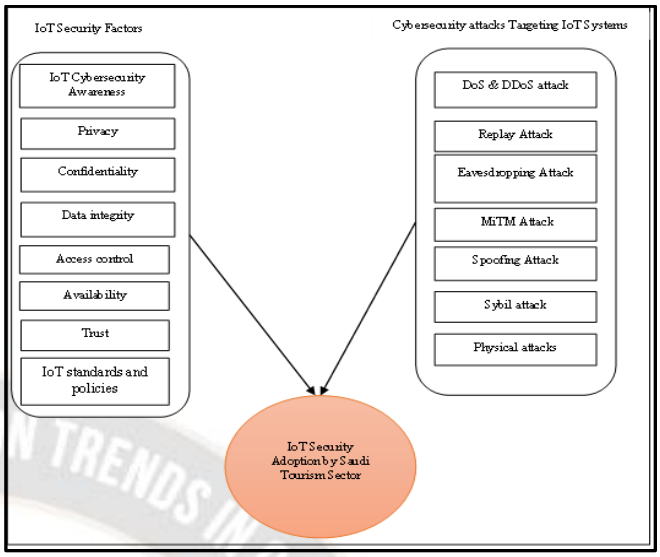


Figure 1: Proposed Research Model

E. CONCLUSION AND FUTURE WORK

In conclusion, the integration of the Internet of Things (IoT) has brought about a transformative shift in technological landscapes, fostering seamless communication across diverse devices and systems. However, this heightened connectivity has exposed critical sectors, notably government and tourism, to increased cybersecurity risks. The existing body of knowledge on how organizations in the Saudi tourism sector navigate these cybersecurity challenges associated with IoT systems is notably lacking. While much of the prevailing IoT literature predominantly focuses on the adoption of IoT systems, this study has aimed for a more comprehensive understanding by introducing a research model. This model encompasses the most influential factors affecting IoT security and the associated cybersecurity attacks. Despite the limited empirical research on IoT security implementation in the Saudi tourism sector, our study has sought to fill these gaps. Motivated by these concerns, our research has delved into the realm of IoT security within Saudi organizations operating in the government tourism sector. The research model incorporates a total of 8 factors (*privacy, confidentiality, data integrity, access control, availability, trust, IoT standards and policies, and IoT Awareness*) and 7 cybersecurity attacks (*denial of service (DoS & DDoS), replay attack, eavesdropping attack, man-in-the-middle (MiTM) attack, spoofing attack, Sybil attack, and physical attack*), all identified from various literature sources. This study contributes to a deeper understanding of IoT security considerations in the Saudi tourism sector, paving the way for enhanced cybersecurity strategies and resilience in the face of evolving technological landscapes.

The outcomes of this study are useful to IoT researchers and practitioners alike. For IoT researchers, the following contributions are made:

a. The study has introduced a research model that assists in understanding the IoT security process in the Saudi tourism sector.

b. It is the first known rigorous academic exercise on IoT security in the Saudi tourism context. It explains how various factors influence the adoption of IoT security measures. As such, the proposed research model of this study contributes to building a theoretical foundation for understanding IoT security in the Saudi tourism community.

For IoT security practitioners, this study makes the following contributions:

a. The 'IoT security model' developed in this study provides useful guidelines for the senior management of Saudi tourism organizations contemplating introducing IoT systems for the first time. These guidelines will suggest which particular factors management should care for during the IoT security measure introduced in their organizations. This will, in turn, facilitate the eventual successful implementation of IoT security for the Saudi tourism context.
b. Knowledge of the IoT cybersecurity attacks targeting the Saudi tourism sector can help them better manage their IoT systems projects, facilitate minimizing uncertainty associated with IoT adoption, and thus assist the tourism sector in avoiding IoT system introduction failures.

IoT researchers are encouraged to empirically test the proposed research model by conducting a large-scale survey undertaken in Saudi Arabia. They are also encouraged to apply the research model and hypothesis developed in this study to other industry sectors and countries from the Arabian Gulf region.

## 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] General Entertainment Authority, "GEA," https://www.gea.gov.sa/.
[4] B. Dorsemaine, J.-P. Gaulier, J.-P. Wary, N. Kheir, and P. Urien, "Internet of things: a definition & taxonomy," in 2015 9th International Conference on Next Generation Mobile Applications, Services and Technologies, IEEE, 2015, pp. 72–77.
[5] M. Remac, "The European Union Agency for Network and Information Security (ENISA)-Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA)," 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] T. Houston, "Mass surveillance and terrorism: does PRISM keep Americans safer?," University of Tennessee Honors Thesis Projects., 2017.
[10] N. Kshetri, "The evolution of the internet of things industry and market in China: An interplay of institutions, demands and supply," Telecomm Policy, vol. 41, no. 1, pp. 49–67, 2017.
[11] D. Lin, C. K. M. Lee, and K. Lin, "Research on effect factors evaluation of internet of things (IoT) adoption in Chinese agricultural supply chain," in 2016 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM), IEEE, 2016, pp. 612–615.
[12] 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.
[13] National Cybersecurity Authority (NCA), "Policy and Standards," https://nca.gov.sa/en. Accessed: Dec. 04, 2023. [Online]. Available: https://nca.gov.sa/en
[14] M. and Q. O. (SASO) Saudi Standards, "IoT security standard," https://www.saso.gov.sa/en/pages/default.aspx.
[15] 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.
[16] 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.
[17] 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.
[18] 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.
[19] 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/

[20] 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.
[21] 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.
[22] M. T. Quasim, "Challenges and applications of internet of things (IoT) in Saudi Arabia," 2021.
[23] 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.
[24] 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.
[25] 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.
[26] 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.
[27] 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.
[28] I. Ali, S. Sabir, and Z. Ullah, "Internet of things security, device authentication and access control: a review," arXiv preprint arXiv:1901.07309, 2019.
[29] 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.
[30] 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.
[31] 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.
[32] 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.
[33] 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.
[34] 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.
[35] 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.
[36] 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.
[37] 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.
[38] 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.
[39] 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.
[40] 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.
[41] 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.
[42] A. K. M. Haque and S. Tasmin, "Security Threats and Research Challenges of IoT-A Review," arXiv preprint arXiv:2101.03022, 2020.