Journal of Information Systems Engineering and Management
2025, 10(9s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Privacy Challenges and Solutions in IoT Deployments: Insights from Saudi Arabia

Fawaz A. Mereani
Department of Computer and Applied Science, Applied College, Umm Al-Qura University, Mecca, Saudi Arabia
famereani@uqu.edu.sa

ARTICLE INFO

Received: 29 Oct 2024
Revised: 20 Dec 2024
Accepted: 30 Dec 2024

ABSTRACT

When firms implement the Internet of Things (IoT), they face many privacy issues. The literature identifies many issues related to the different layers of IoT. However, empirical studies on firms implementing IoT are rare. This study aimed to address this gap. An online survey using Survey Monkey obtained 199 valid responses. All ethical aspects were fully complied with. These responses were analysed for their frequencies. The results were presented and discussed. From the results and discussions of this study, large Saudi firms face many IoT privacy issues. However, most of these firms solve these problems by implementing effective solutions. Other firms that have not implemented effective solutions can learn from the firms that have effectively implemented solutions. The best practices derivable from the results are: (1) Perform a detailed analysis of IoT privacy issues in the organisation, identifying the threat to each layer; (2) Rate the privacy threats according to their frequency, probability and impact rather than through guesswork. This can be achieved by regular monitoring of IoT risks, (3) Implementing solutions based on the type of issue and the vulnerable IoT layer using the rating results, and (4) Regularly monitoring, reviewing and improving the implemented solutions to IoT privacy issues. Some limitations of this study and the scope for future research have been mentioned at the end of this paper.

Keywords: IoT, Privacy challenges, Solutions to IoT challenges, Saudi firms

Introduction

Noting that IoT systems of large firms are susceptible to major surface attacks due to the incapabilities of these systems to fully protect them from cyberattacks, Sadeghi, Wachsmann, and Waidner (2015) stressed the need for further research to develop and design appropriate IoT security mechanisms along with resilient novel isolation primitives to run-time attacks, minimal trust anchors for cyber-physical systems, and scalable security protocols.

Many privacy challenges to IoT deployment and their solutions have been reported. Tawalbeh, Muheidat, Tawalbeh, and Quwaider (2020) listed improper device updates, lack of efficient and robust security protocols, user unawareness, and active device monitoring as the challenges. The authors introduced a new generic layered model for IoT that incorporated components for privacy and security and identifying layers. Security measures were integrated before the deployment of IoT devices to guarantee a secure environment for communication and data sharing. The lowest layer consists of IoT nodes created using Amazon Web Services (AWS), which function as virtual machines. The middle layer, or edge, was constructed using a Raspberry Pi 4 hardware kit utilising the Greengrass Edge Environment in AWS. The top layer, referred to as the cloud, was established using the cloud-enabled IoT environment within AWS. Security protocols and essential management sessions were put in place between these layers to protect users' information privacy. Security certificates were implemented to facilitate data transfer among the layers of the proposed cloud/edge-enabled IoT model. The IoT framework was executed and assessed with two IoT-enabled devices communicating through the edge. Not only does the proposed system model address potential security vulnerabilities, but it can also be utilised alongside top security techniques to counter the cybersecurity threats encountered at each of the layers: cloud, edge, and IoT. The proposed IoT framework is shown in Fig 1.

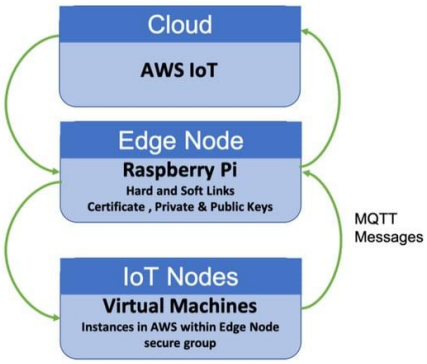

Figure 1 The IoT framework proposed by Tawalbeh, Muheidat, Tawalbeh, and Quwaider (2020)

Abiodun, Abiodun, Alawida, Alkhawaldeh, and Arshad (2021) Reviewed 104 papers to show that stored, used, and in-transition data are vulnerable to security risks. IoT security requirements involve availability, integrity, confidentiality, authentication, authorisation, and access control. These requirements should not be limited to data but need to include the "Things", sensing objects, network communications, and applications of IoT. Some recent security challenges include botnet attacks, increasing numbers of IoT devices and data volumes, lack of data encryption, outdated inter-connected legacy systems, weak default passwords, unreliable threat detection systems, small-scale attacks on IoT, phishing, inability to predict attacks, delayed software updates, IoT financial breaches, users' privacy and heterogeneity of connected devices and environment. The possible solutions are trust management, authentication, privacy solutions, policy environment, fault tolerance, secure communications, secure routing, protection from distributed denial of services (DDoS) threats, spam prevention, IoT architecture and regulatory solutions. Some research gaps are swarm attestation, secure IoT management, identifying sensitive data, data security and sharing in clouds, audit of cloud security, composite survey responsibilities, the impact of cloud decentralisation, certification of cloud providers, protection from malicious things, WSN security and legal frameworks. The authors have given a classification of IoT attacks, as shown in Fig 2.

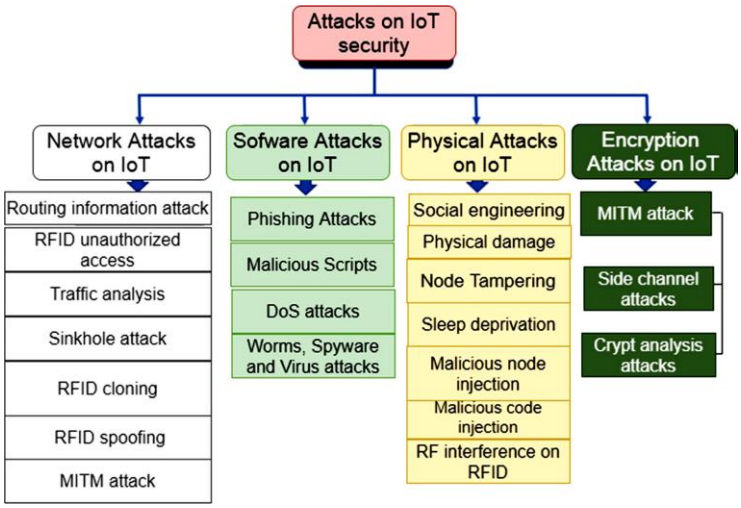

Figure 2 A classification of IoT attacks (Abiodun, Abiodun, Alawida, Alkhawaldeh, & Arshad, 2021).

Cloud of Things (CoT) is an integration of Cloud Computing and the Internet of Things (IoT). CoT applications are used in many areas. CoT faces security issues due to users' remote sharing of computing and networking resources. Preservation of data privacy is also a critical issue in this environment. Many challenges and solutions were reviewed by Abba Ari, et al. (2024).

In a detailed review, Babun, Denney, Celik, McDaniel, and Uluagac (2021) performed an in-depth analysis of the most popular IoT platforms from different application domains. They assessed OpenHAB, Samsung SmartThings, Apple HomeKit, Windows IoT Core, Microsoft FarmBeats, Amazon AWS IoT, ThingWorx, and Watson IoT Platform. The authors found a further need for fine-grained access control and authentication for all entities (users,

devices) with individual permissions and identities at every layer of an IoT solution for improved privacy and security.

The common vulnerabilities notable in IoT include security, privacy and data protection concerns. To address these issues, Lee and Ahmed (2021) developed a new IoT model. On evaluation, the proposed model outperformed a few current models. The authors defined security as threats in IoT security, privacy as confidentiality of IoT users and data protection as the protection of the data for IoT users. The authors selected five firms from different sectors. These firms were compared for their privacy, security and data protection. An efficiency value was computed by combining all three variables. The efficiency values obtained for the IoT generic layered model, the IoT stretched Model, and The Layered Cloud-Edge were 82%, 91% and 94%, respectively. Thus, the layered cloud-edge model proposed by the authors proved to be superior. In this paper, instead of comparing the firms, the authors compared three models. It is not clear whether all the three models were tested in all the three firms.

A detailed analysis of IoT risks and solutions was provided by Deep, et al. (2022). The general IoT architecture consists of a perception layer of physical devices and sensors, a network layer of interconnection and communication protocols, a middle layer of intelligent computing, storing and analysing data and an application layer of specific services to users as a user interface. Three layers are stacked one above another in the sequence given. The security risks and parameters that determine them for each layer are given in the table shown in Fig 3. The challenges in securing IoT include bandwidth, power consumption, complexity, sensing and lightweight computing. The security requirements of IoT are confidentiality, availability and integrity. The authors identified 17 security issues and reviewed the solutions for each layer offered in the literature.

IoT Layers	Security Issues/ attacks	Security Parameters
Application Layer	Data access and security authentication issues, Data Protection and Recovery problems, spear-phishing attack, Software Vulnerabilities, Attacks on Reliability and Clone attack?	Data privacy, Access Control
Middleware Layer	making intelligent decision processing huge data, malicious-code attacks, multi-party authentication, handling suspicious information?	Integrity, Confidentiality
Network Layer	Cluster security problems, DoS attacks, Spoofed, Altered or Replayed routing Information? ? ? ?	Authentication, Integrity
Perception Layer	Node capture, Fake node, Mass node authentication, Cryptographic Algorithm and Key Management Mechanism?	Integrity, Authentication, Confidentiality

Figure 3 Security risks and their parameters (Deep, et al., 2022).

In the above short review, the papers dealt with only the general aspects of IoT, threats and some solutions. None of them dealt with the IoT privacy issues of specific firms or firms in different sectors. This paper aimed to deal with this gap using a survey of large Saudi firms in different sectors.

Literature Review

With the rapidly growing demand for medical IoT (MioT), concerns about privacy and security have arisen. This is due to ignoring the security and privacy aspects of its technologies, which are interconnected and heterogeneous. Such issues lead to unauthorised access to healthcare data by cyberattacks. If MIoT is attacked, it can cause 43% data leakage and information losses, 28% service outages, 15% job losses, 9% population loss, and 3% productivity loss. In the MioT architecture, data flows from the perception layer to the network layer and then to the application layer. About 88% of security threats are accounted for by web and application intrusion (31%), credential theft (24%), malware (12%), DDOS (9%), insider threat (6%) and others (6%). The attacks targeting each layer are given in Fig 4. The authors (Elhoseny, et al., 2021) discussed countermeasures against these attacks. They include access control, data encryption, data auditing, IoT healthcare policies, data search, data minimisation, data anonymisation, inventory services, network segmentation, following the best practices, wider awareness, continuous monitoring and reporting. Challenges of limited resources and heterogeneous resources affect the

perception layer. The network layer is challenged by insecure networks, resource limitations, zero-day vulnerabilities and security patches, high mobility, dynamic network topology and trust management. The application layer is challenged by insecure networks, resource limitations, zero-day vulnerabilities and security patches, trust management and social engineering.

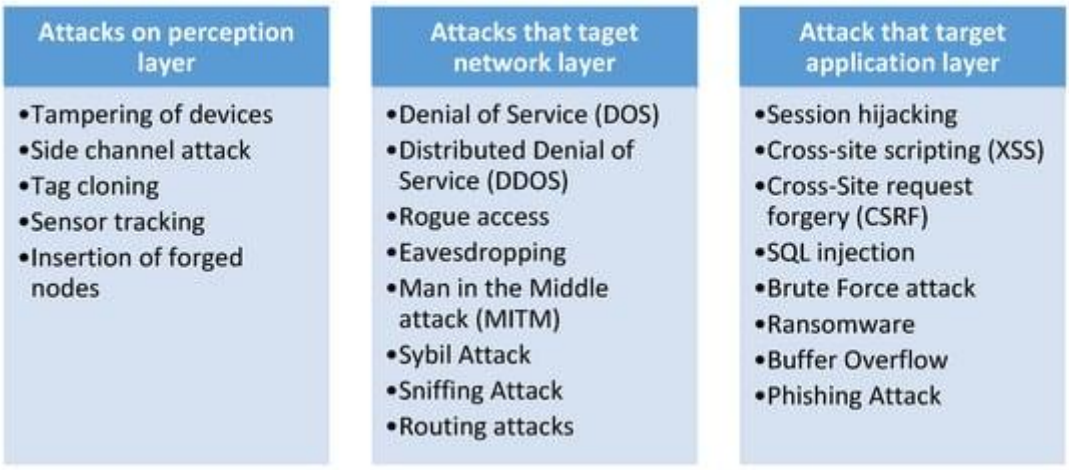

Figure 4 Attack classification based on MIoT architecture (Elhoseny, et al., 2021).

Two focus groups were conducted by Anawar et al. (2022), with five in the first and three in the second. The minimum requirements of participants were five years of experience in cybersecurity, three years in the telecommunication industry, two years in a managerial position and one year in a big data or cloud computing project. Based on the analysis of responses, four themes of technological challenges, two themes of organisational challenges, three environmental challenges and five mitigation challenges to threats related to the Malaysian telecommunication industry were identified. The sample size of five for focus groups may not be adequate for the validity of the findings.

In the case of the construction industry, IoT can be applied for asset/equipment tracking (25%), site condition monitoring (20%), fleet telematics (15%), supply chain tracking (10%), robotics and automation (5%), predictive maintenance (5%), wearables and safety gear (5%) and others (15%).

Using a PRISMA review and a survey of 54 senior construction officials, Musarat, Alaloul, Khan, Ayub, and Jousseaume (2024) observed that most participants supported IoT use as it has the potential to transform the construction sector into a more networked, safer and more productive environment than it is at present. However, privacy, security issues and the lack of standardised protocols need solutions. The sample size of 54 may be inadequate for valid results.

Based on a survey of 66 SME retailers in the UK, Argyropoulou, Garcia, Nemati, and Spanaki (2024) concluded that IoT capability positively impacts these firms through its mediating effect on supply chain integration and supply chain capabilities. The previous studies evaluated the impact of IoT on firm performance through the sequential mediating role of supply chain integration and capabilities. In this study, the impact of IoT capability on firm performance through sequential mediation of supply chain integration and supply chain capability was evaluated. However, the sample size of 66 is quite low to validate the results.

From a review, 25 significant factors were identified, and a survey of 120 building experts was conducted by Solanki and Sarkar (2024) in Gujarat, India. Building experts' opinions were used as inputs into a consistent fuzzy preference (CFPR) method. From CFPR, priority weights and ratings for probable outcomes were obtained to forecast success and failure. The most important factors were the affordable system, ease of use, battery life, and sensor size. The less important factors were poor collaboration between IoT and cloud developer community and building sector and suitable location. Suitable locations had a high probability of success based on forecasting. On the other hand, factors such as loss of jobs and data governance had a high probability of failure. The sample size of 120 may not be adequate for valid results.

To evaluate the stakeholder perceptions on the right to data portability (RtDP), Turner and Tanczer (2024) conducted semi-structured interviews with 28 consumer IoT users, 11 academic/industry experts and eight policymakers due to the contradictions in this respect between Art 20 and a proposed Data Act. The results showed a discrepancy between the purpose and the feasibility of RtDP, which led to inherent uncertainty about its significance and ultimate benefits. Many organisations face difficulties in IoT data transfer. A lack of guidance for data controllers and consumers has created an atmosphere of uncertainty which urgently needs to be addressed.

Analysis of data from 38 Dubai-based automobile firms by Ahmad, et al. (2024) showed that e-supply chain management methods in the automotive industry improved with IoT integration. The low sample size may limit the validity of this study.

Case studies on three startups providing IoT-based smart farming solutions for Vietnamese farmers and farming businesses by Thai and Miyazaki (2024) showed three characteristics of frugal innovations of connected products. They include substantial cost reduction, focused functionality, and optimal performance levels of these farmers and farming businesses. Many enablers and barriers to the deployment of IoT-based frugal innovations were also observed.

Wu and Yun (2024) studied the relationships between IoT-based technologies (IoTs) and organisational competitive performance (OCP) with the moderation of ethical compliance (EthC), drawing on the technology acceptance model (TAM) and utilitarianism theory. The authors surveyed 739 Chinese organisations. The results showed IoT technologies (IoT sensors, smart operational solutions, predictive maintenance, machine learning, blockchain, robotics, edge computing, IoT-enabled communication, augmented reality, and quality control sensors) to be positively related to OCP. EthC positively moderated the relationship between IoT and competitive performance.

Most papers have been reviews on various aspects related to IoT design, architecture, applications and challenges. Only very limited empirical studies were observed. The scanty research in this area justifies this study. In the next section, Methodology, the methods used for data collection and analysis are described. This is followed by a description of the results, discussions of the results and conclusions. Some limitations of this research and the scope for future research are also outlined.

Methodology

This study aimed to explore the privacy challenges and solutions in Internet of Things (IoT) deployments in large organisations in Saudi Arabia. To achieve this objective, 199 senior IT personnel from a sample of large Saudi organisations were surveyed.

This section outlines the survey creation, distribution, data collection, and analysis to ensure a comprehensive understanding of the current landscape of IoT privacy issues and the strategies employed to counter them in Saudi Arabia.

Survey Design and Distribution

A structured survey was set up on the online survey platform Survey Monkey, known for its ease of use, reliability, and capability to handle a considerable volume of respondents. The survey items were divided into four sections: Demographic Information, IoT Deployment Landscape, Privacy Challenges, and Solutions and Best Practices. Each section sought to capture specific insights related to the participants' organisational context and their practices concerning IoT deployment and privacy.

Survey invitations were sent via email to a targeted list of senior IT personnel from large Saudi companies. The email list was procured through corporate partnerships and professional networks, ensuring relevance and engagement from respondents who possess firsthand experience and oversight in IoT strategies and implementations within their organisations.

Ethical Considerations and Informed Consent

To comply with ethical research guidelines, potential respondents were provided with a comprehensive overview of the study, including its purpose and the importance of their participation. An informed consent statement was embedded at the beginning of the survey, assuring participants of confidentiality and the optional nature of their

contribution. They were also informed of their right to withdraw from the survey at any time without the need for any explanation. Only those participants who voluntarily agreed to the terms proceeded to complete the survey.

Data Collection and Response Rate

The data collection phase was actively monitored to ensure a robust and representative sample. The survey remained open until 250 responses had been collected. This number was deemed sufficient for achieving statistical significance, allowing for meaningful analysis and generalisation of findings across the participating organisations. However, many of them did not meet the qualifying criteria. Only 199 valid responses were obtained.

Data Analysis

The collected data was subjected to descriptive statistical analysis using frequency counts. This method was chosen to highlight the distribution of responses across the different questions, thereby providing an overview of the prevalent challenges and solutions related to IoT privacy. By examining the frequencies, patterns, and trends within the data, the study was able to identify critical insights and implications, which are detailed in the results and discussion sections.

Results

The results obtained using the above methodology are described below.

Demographic Information

Demographic Information of the survey participants is given in Table 1.

Table 1 Demographics of survey respondents

Survey question	Response options	Frequency	Per cent
What is your job title?	CIO/CTO	37	18.6
	IT Director	43	21.6
	IT Manager	38	19.1
	Senior IT Specialist	41	20.6
	Other	40	20.1
	Total	199	100.0
How many employees are there in your organisation?	Less than 500	46	23.1
	500-1,000	46	23.1
	1,001-5,000	54	27.1
	More than 5,000	53	26.6
	Total	199	100.0
Which industry does your organisation belong to?	Finance	32	16.1
	Government	27	13.6
	Healthcare	33	16.6
	Manufacturing	28	14.1
	Retail	20	10.1
	Telecommunications	31	15.6
	Other	28	14.1
	Total	199	100.0

Those dealing with information and technology were about 80% (n=159). Others were 20% (n=40). Out of 199, 92 (46%) had 1000 or less employees. The remaining 107 (54%) had above 1000 employees. About 16% of each of the 199 organisations dealt with finance, healthcare and telecommunications. About 14% each of them were related to government services, manufacturing and others. Only 20 (10%) were in the retail sector. These trends demonstrate ample diversity among the survey respondents.

IoT Deployment Landscape

The types of IOT devices used and their purpose were enquired in the survey. Their responses are provided in Table 2.

Table 2 IoT deployment landscape of survey participant firms

Survey question	Response options	Frequency	Per cent
What types of IoT devices are mainly used in your organisation?	Asset tracking devices	34	17.1
	Cameras	30	15.1
	Sensors	33	16.6
	Smart appliances	26	13.1
	Wearables	40	20.1
	Other	36	18.1
	Total	199	100.0
What is the primary objective for IoT deployment in your organisation?	Cost reduction	41	20.6
	Enhanced customer experience	37	18.6
	Improved security	30	15.1
	New business models	33	16.6
	Operational efficiency	28	14.1
	Other	30	15.1
	Total	199	100.0

Although there may be sectoral differences for IoT devices, the responses to the questions did not differentiate them. While 20% (n=40) used wearables, 30 to 36 firms used asset-tracking devices, cameras, sensors and others. Smart appliances were used by 28 (13%)

These IoT devices were used for cost reduction by 41 (20.6%) firms, enhanced customer experience by 37 (18.6%) firms, new business models by 33 (16.6%) firms, improved security by of the firm30 (15.1%) firms and operational efficiency by 28 (14.1%) firms.

Thus, the firms of the survey respondents used different types of IoT devices for different purposes.

Privacy Challenges

This study aimed to evaluate the privacy challenges and solutions to them for large Saudi organisations. The data collected for the first part dealing with challenges is provided in Table 3. The primary challenges, their rating and the firm's monitoring of these challenges are included in Table 3.

Table 3 Privacy challenges to IoT use by the participant firms

		Frequency	Percent
How would you rate the privacy challenges your organisation faces due to IoT deployments?	Very Low	42	21.1
	Low	25	12.6
	Moderate	43	21.6
	High	45	22.6
	Very High	44	22.1
	Total	199	100.0
What is the primary privacy concerns related to IoT in your organisation?	Compliance with regulations	25	12.6
	Data breaches	28	14.1
	Data leaks	32	16.1
	Data ownership issues	26	13.1

	Lack of consumer consent	36	18.1
	Unauthorised data access	32	16.1
	Other	20	10.1
	Total	199	100.0
Does your organisation conduct regular privacy risk assessments for IoT deployments?	No	64	32.2
	Not sure	70	35.2
	Yes	65	32.7
	Total	199	100.0

Lack of consumer consent was the primary concern for 36 (18.1%) of the firms. Data leaks and unauthorised access were the primary concerns for 32% of firms (16.1%) of the firms. Data breaches were a problem for 28 (14.1%) of the firms. Data ownership issue was the problem for 26 (13.1%) of the firms. The difficulty in complying with regulations was the problem for 25 (12.6%) of the firms. The remaining 20 (10.1%) of the firms reported other problems.

The above privacy challenges were rated high to very high by 89 (44.7%) of the firms. They were rated very low to low by 67 (33.7%) of the firms. Only 43 (21.6%) of the firms rated these challenges as moderate. Thus, more surveyed firms faced high to very high IoT privacy challenges compared to firms facing very low to low challenges.

Despite the recognition of such levels of IoT privacy challenges, only 65 (32.7%) firms regularly assessed the privacy risk assessments for IoT deployments. Such assessments were not done by 64 (32.2%) firms. A significantly large number of 70 (35.2%) respondents were not sure whether their firms conducted any such assessments.

Solutions and Best Practices

The last part of this study is solutions to the identified IoT privacy challenges and from these solutions, designing best practices. Table 4 provides the solutions, their effectiveness and the existence of any specific guidelines or standards for privacy practices.

Table 4 Solutions, their effectiveness and the existence of specific guidelines or standards

Survey question	Response options	Frequency	Per cent
What primary measure does your organisation implement to address privacy challenges in IoT?	Access controls	29	14.6
	Compliance with regulations	24	12.1
	Data encryption	30	15.1
	Employee training	20	10.1
	Other	40	20.1
	Privacy by design principles	31	15.6
	Regular audits	25	12.6
	Total	199	100.0
How effective do you find your current solutions in mitigating privacy risks?	Effective	51	25.6
	Ineffective	37	18.6
	Neutral	34	17.1
	Very effective	41	20.6
	Very ineffective	36	18.1
	Total	199	100.0
Are there specific regulations or	No	94	47.2
	Yes	105	52.8

standards that guide your IoT privacy practices?	Total	199	100.0

Seven solutions to IoT privacy challenges were tried by the surveyed firms. Access control was implemented by 29 (14.6%) firms, regulatory compliance was implemented by 24 firms (this was a challenge for 25 firms in the previous table), 30 (15.1%) firms implemented data encryption, 20 (10.1%) firms trained their employees, 31 (15.6%) firms implemented privacy by design principles, 25 (12.6%) firms conducted a regular audit of their IoT challenges and 40 (20.1%) firms implemented other solutions.

Out of 199, 92 (46.2%) firms found the solutions they implemented to be effective or very effective. On the other hand, 73 (36.7%) firms found the solutions they implemented to be ineffective or very ineffective. Out of 199, 34 (17.1%) participants gave a neutral response. Thus, the large Saudi firms surveyed in this study implemented effective to very effective solutions for high to very high levels of IoT privacy challenges.

Discussion & Conclusion

Discussion

This study aimed to evaluate the IoT privacy issues, solutions, and their effectiveness in the case of Saudi firms in different sectors. Overall, the results showed that a majority of the firms surveyed effectively or very effectively solved high-to-very-high IoT privacy challenges of various types despite fewer firms regularly monitoring them.

Most papers in the literature categorised the threats to privacy according to the layers in the IoT architecture (Deep et al. 2022; Elhoseny et al. (2021). If the survey participants were able to categorise privacy threats, it might have been more useful for them. The survey items did not cover this point. The need for efficient and robust protocols as a solution to IoT privacy issues was identified by Tawalbeh et al. (2020). This solution was not included in the survey items. Access control was suggested as a security requirement by Babun et al. (2021. In this study, this method was used by 29 (14.1%) firms only. Abiodun et al. (2021) also identified different types of security attacks on different parts of IoT. They suggested privacy and regulatory solutions. Privacy by design principles was used by 31 (15.6%) of the firms in this study. Compliance with regulations was implemented by 24 (12.1%) of the firms in this study. The lack of standardised protocols was mentioned by (Musarat et al., 2024) as a deficiency in the current systems of IoT. More than half of the surveyed participants agreed with this point. Asset tracking is normally used by construction firms. No construction firm participated in the survey. Right-to-data portability is an issue among stakeholders in IoT systems (Turner & Tanczer, 2024). In this study, the data ownership issue was mentioned as an IoT privacy threat by 26 (13.1) firms. Also, unauthorised data access was another privacy issue mentioned by 32 (16.1%) firms in this study.

Overall, it can be said that there is partial support for some of the aspects covered by this study. This is because very few papers matched the topics covered in the survey. Survey items in line with the literature would have been more useful.

Conclusion

From the results and discussions of this study, it can be concluded that large Saudi firms face many IoT privacy issues. However, most of these firms solve these problems by implementing effective solutions. Other firms that have not implemented effective solutions can learn from the firms that have effectively implemented solutions.

The best practices derivable from the results are-

1. Perform a detailed analysis of IoT privacy issues in the organisation, identifying the threat to each layer.
2. Rate the privacy threats according to their frequency, probability and impact rather than by guess. This can be achieved by regularly monitoring IoT risks.
3. Implement solutions based on the type of issue and the vulnerable IoT layer using the rating results.
4. Regularly monitor, review and improve the implemented solutions to IoT privacy issues.

In-depth interviews with a few of the survey participants could have added to the usefulness of this study. This is one of the limitations of this research.

As was pointed out at the end of the literature review, empirical studies on firms were rare. Hence, many more empirical studies are suggested.

Studies comparing IoT privacy issues in firms from different sectors will be useful. Identification of any predictor will be useful in anticipating IoT privacy threats and implementing proactive solutions.

From the results of this study, some best practices have been suggested. The claim that they are best practices needs to be verified by rigorous research.

References

[1] Abba Ari, A. A., Ngangmo, O. K., Titouna, C., Thiare, O., Mohamadou, A., & Gueroui, A. M. (2024). Enabling privacy and security in Cloud of Things: Architecture, applications, security & privacy challenges. *Applied Computing and Informatics, 20*(1/2), 119-141. doi:10.1016/j.aci.2019.11.005

[2] Abiodun, O. I., Abiodun, E. O., Alawida, M., Alkhawaldeh, R. S., & Arshad, H. (2021). A review on the security of the internet of things: Challenges and solutions. *Wireless Personal Communications, 119*, 2603-2637. doi:0.1007/s11277-021-08348-9

[3] Ahmad, A., Nuseir, M. T., Alzoubi, H. M., Al Kurdi, B., Alshurideh, M. T., & Al-Hamad, A. (2024). Impact of the Internet of Things (IoT) on the E-Supply Chain with the Mediating Role of Information Technology Capabilities: An Empirical Evidence from the UAE Automotive Manufacturing Industry. In H. M. Alzoubi, M. T. Alshurideh, & T. M. Ghazal (Eds.), *Cyber Security Impact on Digitalization and Business Intelligence: Big Cyber Security for Information Management: Opportunities and Challenges* (Vols. Studies in Big Data, vol 117, pp. 409-429). Cham: Springer International Publishing. doi:10.1007/978-3-031-31801-6_25

[4] Anawar, S., Othman, N. F., Selamat, S. R., Ayop, Z., Harum, N., & Rahim, F. A. (2022). Security and Privacy Challenges of Big Data Adoption: A Qualitative Study in Telecommunication Industry. *International Journal of Interactive Mobile Technologies, 16*(19), 81-97. doi:10.3991/ijim.v16i19.32093

[5] Argyropoulou, M., Garcia, E., Nemati, S., & Spanaki, K. (2024). The effect of IoT capability on supply chain integration and firm performance: an empirical study in the UK retail industry. *Journal of Enterprise Information Management, 37*(3), 875-902. doi:10.1108/JEIM-06-2022-0219

[6] Babun, L., Denney, K., Celik, Z. B., McDaniel, P., & Uluagac, A. S. (2021). A survey on IoT platforms: Communication, security, and privacy perspectives. *Computer Networks, 192*, 108040. doi:10.1016/j.comnet.2021.108040

[7] Deep, S., Zheng, X., Jolfaei, A., Yu, D., Ostovari, P., & Bashir, A. K. (2022). A survey of security and privacy issues in the Internet of Things from the layered context. *Transactions on Emerging Telecommunications Technologies, 33*(6), e3935. doi:10.1002/ett.3935

[8] Elhoseny, M., Thilakarathne, N. N., Alghamdi, M. I., Mahendran, R. K., Gardezi, A. A., Weerasinghe, H., & Welhenge, A. (2021). Security and privacy issues in medical internet of things: overview, countermeasures, challenges and future directions. *Sustainability, 13*(21), 11645. doi:10.3390/su132111645

[9] Lee, C., & Ahmed, G. (2021). Improving IoT privacy, data protection and security concerns. *International Journal of Technology, Innovation and Management, 1*(1), 18-33. doi:10.54489/ijtim.v1i1.12

[10] Musarat, M. A., Alaloul, W. S., Khan, A. M., Ayub, S., & Jousseaume, N. (2024). A survey-based approach of framework development for improving the application of internet of things in the construction industry of Malaysia. *Results in Engineering, 21*, 101823. doi:10.1016/j.rineng.2024.101823

[11] Sadeghi, A.-R., Wachsmann, C., & Waidner, M. (2015). Security and privacy challenges in industrial internet of things. *Proceedings of the 52nd annual design automation conference, 7-11 June, 2015, San Fransisco, USA* (pp. 1-6). ACM. doi:10.1145/2744769.2747942

[12] Solanki, A., & Sarkar, D. (2024). Forecasting the probability of successful deployment of internet of things and cloud computing in the building sector through consistent fuzzy preference relations method. *World Journal of Engineering*, Ahead of print. doi:10.1108/WJE-06-2023-0161

[13] Tawalbeh, L., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2020). IoT Privacy and security: Challenges and solutions. *Applied Sciences, 10*(12), 4102. doi:10.3390/app10124102

[14] Thai, L. M., & Miyazaki, K. (2024). Frugal innovation for smart connected products: a case study of IoT-based smart farming by Vietnamese startups. *Asian Journal of Technology Innovation*, 1-25. doi:10.1080/19761597.2024.2359035

[15] Turner, S., & Tanczer, L. M. (2024). In principle vs in practice: User, expert and policymaker attitudes towards the right to data portability in the internet of things. *Computer Law & Security Review, 52*, 105912. doi:10.1016/j.clsr.2023.105912

[16] Wu, X., & Yun, X. (2024). Navigating firm competitive performance through artificial intelligence: moderation of ethical compliance. *International Journal of Information Systems and Change Management,, 14*(1), 70-84. doi:10.1504/IJISCM.2024.138083