Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

Cybersecurity Risk Assessment of Smart Home IoT Ecosystems in the MENA Region

Hameed Almubark

Hameed.almubarak@brunel.ac.uk

Brunel University London

Hamed Al-Raweshidy

Brunel University London

Jenan Moosa Hasan

Ahlia University

Ahmed Jedidi

Applied Science University

Case Report

Keywords: Internet of Things, smart homes, IoT security, privacy, MENA region, blockchain, edge computing

Posted Date: June 29th, 2026

DOI: https://doi.org/10.21203/rs.3.rs-9783987/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: No competing interests reported.

Version of Record: A version of this preprint was published at Discover Internet of Things on November 3rd, 2026. See the published version at https://doi.org/10.1007/s43926-026-00539-9.

Cybersecurity Risk Assessment of Smart Home IoT Ecosystems in the MENA Region

Hameed Almubark, Member, IEEE, Dept. of Computer Science [Hameed.almubarak@brunel.ac.uk], Hamed Al-Raweshidy, Senior Member, IEEE, Dept. of Electronic and Electrical Engineering College of Engineering, Brunel University of London [hamed.al-raweshidy@brunel.ac.uk] and Jenan Moosa Hasan, College of Information Technology, Ahlia University [jhasan@ahlia.edu.bh], Ahmed Jedidi, College of Arts and Science Applied Science University,[Ahmed.jedidi@asu.edu.bh]

Abstract

The Internet of Things (IoT) is increasingly embedded in smart homes, industrial systems and healthcare environments, creating new requirements for low latency, bandwidth efficiency and robust security. However, many IoT devices remain difficult to secure because of limited processing capability, storage capacity, energy resources and fragmented communication protocols. This study investigates security and privacy concerns associated with IoT adoption in smart-home and related environments, with a particular focus on users in the MENA region. An online questionnaire was distributed to Arabic-speaking participants, resulting in 164 valid responses from 12 countries. The results show that users are highly concerned about privacy invasion, data theft, device hacking and unauthorized access, while their protection practices remain inconsistent. More than half of the respondents reported a need for additional support to secure existing IoT devices rather than replacing them. The findings also show that commonly used protection mechanisms include strong passwords, two-factor authentication, firmware updates, antivirus software, firewalls and VPNs, although users still require clearer guidance, checklists and professional support. Based on the survey results and related literature, the paper discusses practical recommendations for strengthening IoT security through user awareness, network protection, device-level controls, edge computing and blockchain-enabled approaches.

Keywords: Internet of Things; smart homes; IoT security; privacy; MENA region; blockchain; edge computing

1 Introduction

The Internet of Things (IoT) has quickly become a key technology for reducing costs, saving time and supporting automation in everyday tasks. Furthermore, the

architecture of IoT networks is evolving rapidly, enabling widespread adoption across multiple industries [1]. For example, in industries such as "the Internet-of-Vehicles (IoV)" [2] and smart homes [3], [4], [5], [6]. Thus, the authors Park et al. [7] anticipated that by 2025, IoT devices would generate enormous volumes of data—more than 79. 4 zettabytes (ZB). Despite numerous obstacles, the number of IoT devices continues to rise, and they are becoming increasingly important across a variety of industries. By 2030, there will be more than 10 billion connected devices, or three times as many, according to Statista [8]. Nonetheless, there are other obstacles, including security and privacy [7], [1], [9], [10], [11], decentralization [7], [11], [12], data authentication [7], [13], and bandwidth of the network [14], [15], [16]. The shortcomings of IoT devices include limited storage capacity, poor energy efficiency [13], [6], [17], and an inability to protect data [1], [12], [18]. To protect their data, individuals and businesses that use IoT devices or applications increasingly rely on security tools, programs and protocols. Additionally, they are more aware of the need to protect networks against malicious IoT devices. This has enabled a range of solutions to emerge, including firewalls, antivirus software, security software tailored to the Internet of Things, and blockchain technology (BC). Moreover, one of the main characteristics of blockchain is the implementation of consensus protocols, which enable the resolution of security [14] and tampering concerns as well as the tracking of action origins [13]. For instance, blockchain roles: integration of BC-based Internet of Edge model (BloE) [21], ECBCM [20], Edge-of-Things and BC (BEoT) [22], and a Novel BC-based key management scheme for MEC [23]. Therefore, the goal of these applications and technologies is to prevent unforeseen errors and the introduction of harmful IoT devices into the network. Although Edge Computing (EC) offers several advantages, including reduced network bandwidth, lower data transfer latency, enhanced user privacy, and reduced cloud energy consumption, EC still faces security challenges [15]. However, privacy and security issues remain due to heterogeneity across smart edge devices. Decentralized deep learning (DDL) [24], which can effectively process large volumes of data, is the optimal solution in these circumstances. Additionally, it incorporates state-of-the-art technologies to ensure reliable and effective communication, according to [6]. Therefore, several surveys and papers attempted to demonstrate the use of methods and protocols in the Internet of Things environment for data protection, or the application of blockchain in addressing the security of the IoT, for example, “Survey on Security Protocols for IoT” [3]. Accordingly, this study aims to identify the fears that individuals and organizations have regarding the use of IoT applications and devices. In addition, the study assesses how individuals and organizations protect their IoT devices and applications. The primary objective is to understand their approaches and compare them with other proposed methodologies. The study also identifies the extent to

which IoT users report privacy and security concerns. These findings motivate the search for practical methods to protect individual and organizational IoT assets.

The remainder of this paper is organized as follows. Section 2 reviews related work on IoT security. Section 3 presents the IoT ecosystem architecture. Section 4 describes the survey design and data collection. Section 4. 1 presents the survey results and analysis. Section 5 provides recommendations for enhancing IoT security, and Section 6 concludes the paper and identifies future research directions.

2 Related work

In order to improve data security for the Internet of Things environment, we review a number of studies that employ new, innovative, or integration approaches between two or three technologies, such as IoT, edge computing, Blockchain, protocols, or any other strategies. To achieve security and privacy, these programs and technologies can be used in a variety of industries, such as healthcare, manufacturing, smart cities, and smart homes [4], [19], [25], [26]. Here, we highlight research that has addressed data protection challenges by utilizing effective strategies that can be implemented to improve overall performance and data security. Additionally, these employed the survey to demonstrate the beneficial effects of either the survey alone or their approaches.

In an effort to improve patient data security and privacy in the healthcare industry, this study [27] used blockchain technology and found that BC had a beneficial impact on patient data protection. Additionally, the survey was distributed to administrators and healthcare professionals who employed blockchain technology in their individual businesses as part of the study. As a result, it attempted to find and demonstrate BC's beneficial influence during the survey. However, because this experiment cannot be applied to other fields, it may be constrained by the tiny dataset used. Ultimately, the security issue remains.

The purpose of the survey [3] was to highlight the importance of robust security protocols for the Internet of Things (IoT) ecosystem. For instance, in fields like smart cities, healthcare, and industry. Additionally, it demonstrated weaknesses across several IoT protocol tiers in addressing the problem. Therefore, the study focused on describing security flaws and the defenses provided by IoT protocols, which can achieve numerous crucial security and privacy goals, such as authorization, data integrity, and authentication. Nonetheless, the study operated at two levels: the network layer and the perception layer. The initial level collected data and sought to identify connected devices. Data transfer from the first level via current communication networks (edge and cloud service provider levels) was the primary

focus of the second level. Additionally, the study outlined protocols, including Public Key Infrastructure (PKI), Constrained Application Protocol over Datagram Transport Layer Security (CoAPs), and Open Authorization (OAuth), which are primarily used to protect data. Unfortunately, security is challenging, complex, and resource-intensive due to the restricted resources of IoT devices. Due to the low processing and storage capability of the perception layer (IoT devices).

This study [28] explores the security challenges faced by the Internet of Things (IoT) due to its integration in areas like smart cities and homes, emphasizing the vulnerability of IoT devices to cyber threats. It reviews algorithms and authentication techniques to enhance IoT network security and safeguard data. One key contribution is an authentication method that uses device fingerprints, incorporating physical state and location characteristics, verified through the Infinite Gaussian Mixture Model (IGMM) to ensure device authenticity. The document also categorizes diverse attack types, including physical, side-channel, environmental, cryptanalysis, and software attacks. Additionally, Zhang et al. [29] developed an algorithm to prevent Denial-of-Service (DoS) attacks by segmenting the network into working nodes, legitimate user nodes, attacker nodes, and monitoring nodes. Furthermore, the study highlights the development of a lightweight authentication protocol called PAuthKey, designed for distributed IoT systems. This protocol enables direct, efficient authentication between users and sensors, making it suitable for resource-constrained IoT devices. Overall, the study demonstrates improved authentication performance compared to traditional methods and offers practical solutions to bolster IoT security. Researchers at the University of South Carolina Aiken [30] examined IoT security by conducting a printer penetration test using the PRET tool in Kali Linux, following the RUB-NDS guide on GitHub. They also conducted a survey on IoT in the workplace, examining the balance between IoT benefits and security risks. Students emphasized the need to address security gaps to maximize the benefits of IoT, particularly in large organizations, while acknowledging the daily importance of IoT devices. Wireshark analysis of network traffic recorded over 80, 000 entries and 900 unique MAC addresses, revealing a diverse range of devices on campus. The researchers highlighted limitations in their data collection using basic tools and stressed the need for stronger network infrastructure. Ultimately, they concluded that secure IoT integration is essential to enhance learning experiences and prevent network issues, data breaches, and operational disruptions.

This survey [31] discusses various security problems that occur at each level of an IoT system, including the IoT layer, network layer, middleware layer, and gateways. It also identifies new approaches to addressing these security issues, thereby improving privacy and safety in IoT systems. These solutions include blockchain,

fog computing, edge computing, and machine learning. The study examines the current state of IoT security and explains the risks associated with each component of the system. When they discussed blockchain, they said it helps keep data safe by using a shared, decentralized record [31]. This survey paper [32] examines how Blockchain technology can integrate with the Internet of Things (IoT) to address challenges in device connectivity and data security. It examines how Blockchain can enhance the integration and security of IoT systems and provides examples of how this is achieved. For instance, Zhao et al. [34] created a wireless monitoring system that used a LoRaWAN gateway to send information to the cloud. They used different Blockchain methods like Bitcoin-based integration with digital signatures, Ethereum-based integration with smart contracts and crypto accounts, Hyperledger-based integration to improve tracking, and adhoc integration.Big data management plays a crucial role in sectors such as finance, healthcare, and education, where secure data storage and controlled information sharing are essential. However, this survey concentrates specifically on how blockchain technology can mitigate integration and security challenges within IoT environments. It further examines blockchain consensus mechanisms that safeguard against data manipulation, strengthen system security, and enable traceability of transactional activities.

The paper also explores how Blockchain is used in IoT contexts, demonstrating how it can enhance security and integration. In the end, the survey shows how widely Blockchain can be used in IoT environments.

All of these studies addressed and focused on methods. So, Table 1 shows that the studies shared the same issue, which is security and privacy, but they selected different methods, as shown in Fig. 1. We select a survey to help us discover people’s techniques, because users and businesses should tell us what they feel about IoT security and how they protect their IoT devices. Our survey aims to address these questions and identify which technique is most useful to users.

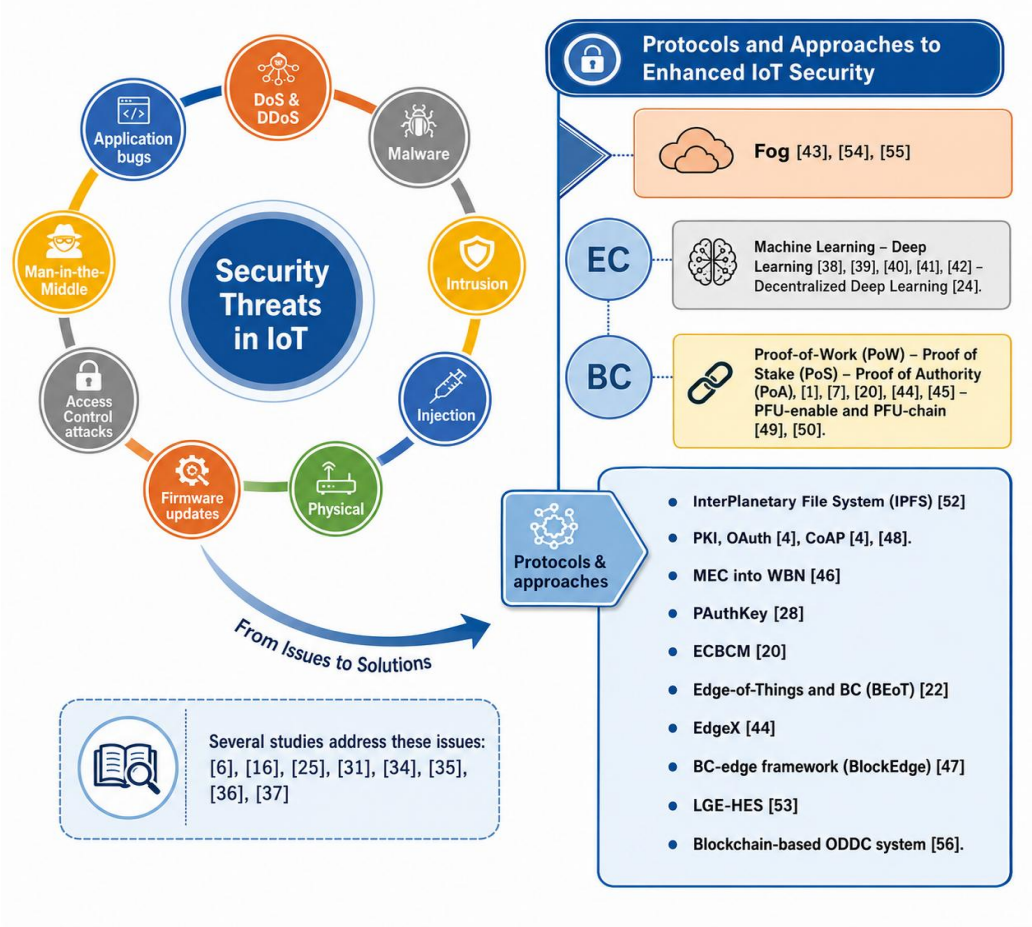


Fig. 1 Security risks in IoT systems and potential solution approaches

Table 1 Studies related to IoT security and privacy

No.	Studies	Issues	Suggested possible solution	Main aim
1	A Survey of User Perspectives on Security and Privacy in a Home Networking Environment [10]	IoT security; security and privacy; security	Further studies to secure data	Secure data
2	A Comprehensive Survey of Threat Detection and Mitigation in Layered IoT Security Frameworks [6]	IoT security and privacy	Reinforcement learning	Intrusion detection methods in IoT environments
3	A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures [31]	IoT security and privacy	BC, fog, EC and ML	High security
4	A Survey on Security, Privacy, Trust, and Architectural Challenges in IoT Systems [34]	IoT security, privacy and trust	ML, DL, BC and SDN	High performance
5	Lightweight Authentication Methods in IoT: Survey [37]	IoT authentication and security	IOTA blockchain, MEC and several protocols	Lightweight authentication
6	Multi-Access Edge Computing Architecture, Data Security and Privacy: A Review [57]	Data security and privacy	Multi-Access Edge Computing (MEC)	Reliable and high-speed communication
7	Exposed by Default: A Security Analysis of Home Router Default Settings and Beyond [36]	Default device and router vulnerabilities	Transport Layer Security (TLS)	Data protection
8	Enhancing Security and Privacy of Patient Data in Healthcare: A SmartPLS Analysis of Blockchain Technology Implementation [27]	Patient data security and privacy	BC	Scalability and interoperability
9	PUFchain: Hardware-Assisted Blockchain for Sustainable Simultaneous Device and Data Security in the Internet of Everything (IoE) [51]	Device and data security	BC, PUF-enabled mechanisms and PUFchain	Scalability and energy efficiency
10	This survey investigates security concerns and protection practices among IoT users	IoT security and privacy in user environments	BC, MEC and PUFchain	Scalability, low latency and energy efficiency

The protocols and methodological approaches summarized in Table 2 are designed to reduce security vulnerabilities in IoT environments characterized by multiple addressing schemes. They also aim to reduce resource consumption, improve scalability, maintain performance and lower latency. The comparison highlights the inherent tension between security and energy efficiency and emphasizes the need for continued development of secure, scalable and efficient IoT mechanisms.

Table 2 Comparison of techniques based on significant aspects in the IoT environment

Type	Security	Energy cost	Scalability	Performance	Low latency
Secure Edge Mobility Protocol (SEMP)	Yes	Yes	Yes	Yes	Yes
Blockchain (PoW) [61]	Yes	Yes	No	No	Yes
PUFchain [51]	Yes	No	Yes	Yes	Yes
BC-edge framework (BlockEdge) [47]	Yes	No	Yes	No	No
MEC (Blockchain/PoW) [59]	Yes	No	Yes	No	No
Edge-of-Things and BC (BEoT) [22]	Yes	No	No	Yes	No
Proof of PUF-Enabled [50]	Yes	No	No	Yes	No
Collaborative DNN-based IDPS [58]	Yes	No	No	Yes	Yes
BC-edge framework [47]	Yes	No	No	No	Yes
DAG-based blockchain (IOTA) [26]	Yes	No	Yes	No	Yes
Multi-Access Edge Computing (MEC) [57]	Yes	No	No	Yes	Yes
OIDC based on the Ethereum Blockchain [56]	Yes	No	No	Yes	No

However, numerous studies focus on IoT security and privacy across different sectors. Only a limited number address the threats faced by individuals and compare these with the risks encountered by businesses. As a result, we acquire valuable insights into how both individuals and businesses navigate security challenges in the IoT domain. This will also deepen understanding of how people use and protect IoT applications and devices in domestic settings, professional environments, and across various industries.

3 IoT ecosystem architecture

A wide range of industries are currently adopting the Internet of Things (IoT), which interconnects everyday services through an extensive, integrated network. IoT links people and gadgets to collect data through sensors, as those in a patient's monitoring system, webcams, and home plant watering systems, as shown in Fig. 2. The Perception Layer, which collects data, the Network Layer, which is in the middle of the structure and includes devices like routers, and the Application Layer, which processes and stores the data and includes devices like the cloud, are the three primary components of the Internet of Things. Additionally, it is used in several

important industries, including healthcare, the military, and finance. Because IoT devices lack standardized protocols [16], attacks at the Things layer can target them to obtain or fabricate data [13]. This enables any device to connect to them [3]. The amount of data produced by these IoT devices is expected to exceed 79. 4 zettabytes (ZB) by 2025 [7], [14]. By then, Huawei predicts that there will be approximately 100 billion IoT devices, with more than a million sensors being added every hour [64]. This results in a large volume of data, which poses significant security and privacy risks. For example, given the limitations of security measures and the wide range of IoT devices, security and privacy are crucial for detecting distributed denial-of-service (DDoS) attacks [7]. Furthermore, due to their limited computing capacity and energy consumption, IoT devices are generally weak and unable to defend against security threats [15]. While the Internet of Things (IoT) enhances daily life [12] by streamlining tasks and increasing efficiency, it simultaneously introduces significant security and privacy challenges. Consequently, the integration of edge computing with IoT presents substantial potential to enhance operational efficiency, minimize energy usage [13], [64], reduce latency [15], [24], and strengthen privacy protections [15], [13], [63]. Despite the persistent security concerns associated with edge computing [15], [38], blockchain technology is widely regarded as a viable solution for addressing vulnerabilities within IoT ecosystems [14], [20], [54].

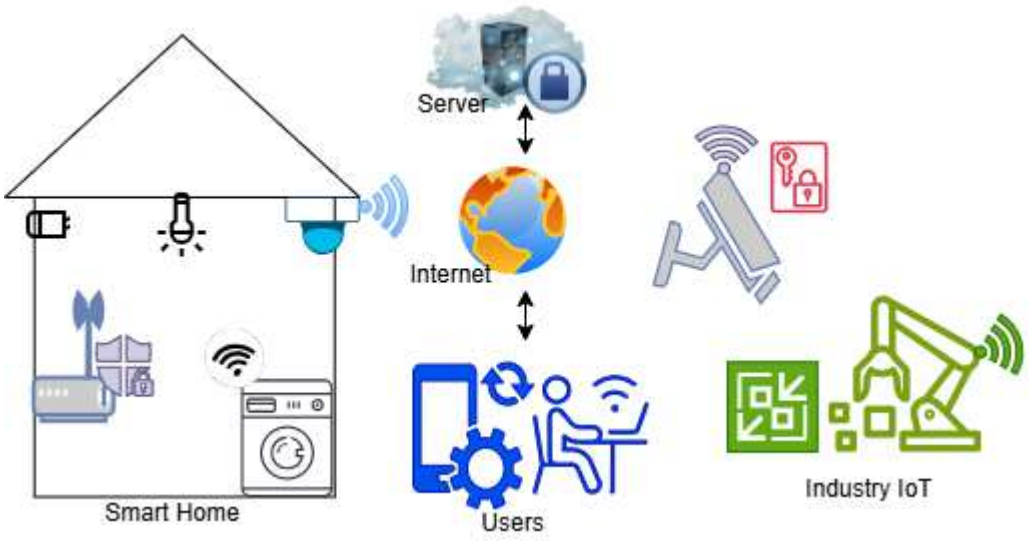


Fig. 2 IoT ecosystem architecture and common application domains

4 Survey design and data collection

Initially, we designed the online questionnaires using SurveyMonkey. The survey comprised three sections: the first gathers general participant information, including location, age, and IoT technology familiarity. The second section, Security Practices, explores how participants manage their IoT devices—covering updates, password types, and security configurations. The final section, Tools and Programs, Concerns and Awareness, prompts participants to share how they protect their IoT devices and which tools they employ. We analyzed the survey data with SurveyMonkey and validated our findings using SPSS, a software suited for data collection, analysis, interpretation, presentation, and organization through statistical and mathematical methods.

The survey was designed primarily for individual users. Business-level data collection would require formal approval letters, institutional ethical clearance and consent from organizations in each participating country. Therefore, this study also draws on prior surveys and studies involving companies and organizations, particularly studies that examine how organizations use and protect IoT devices in workplace and industry settings.

The survey was distributed to the general public, with a focus on Arabic-speaking individuals. The online survey was completed by 164 respondents from 12 countries, including Saudi Arabia, Egypt, Tunisia, Kuwait, Qatar, Bahrain, Oman, Iraq, Algeria, the United Kingdom, Australia and Turkey. The focus on Arabic speakers was selected to address the limited representation of the MENA region in prior IoT security survey research.

Another purpose of this survey was to focus on the Arabic-speaking region. Although the topic is global, we selected this area because the Middle East and North Africa (MENA) region includes a large Arabic-speaking population with diverse levels of IoT adoption and cybersecurity awareness. Extensive survey research has examined security and privacy issues, including [36], which focused on China and collected a total of 393 responses, comprising 322 from China and 71 from North America and Europe but none from MENA. Therefore, we chose the MENA region to redress this gap in the literature.

The survey focuses mainly on the security tools used by individuals and organizations to protect IoT devices, as well as the development of a practical protection framework supported by recommendations. In contrast, China-based studies often emphasize technical and device-level vulnerabilities, while global studies typically focus on conceptual frameworks, behavioral perspectives and systematic literature reviews, as shown in Table 3.

Table 3 Comparison between the MENA survey, China-based study, and global IoT security studies

Aspect	MENA region (this study)	China-based study [36]	Global studies [10]
Research type	Survey-based empirical study	Experimental and technical security analysis	Systematic literature reviews and surveys
Main focus	Security tools and protection practices used by users	Device configuration vulnerabilities and default settings	Security challenges, user perspectives and conceptual frameworks
Study environment	Smart homes and mixed IoT environments	Home routers and network infrastructure	General smart-home ecosystems
Data source	Survey responses from users and organizations	Analysis of commercial devices and configurations	Multiple academic studies and datasets
Security perspective	Practical deployment and protection practices	Technical threat modeling and vulnerability discovery	Behavioral and conceptual security analysis
Identified risks	Inconsistent protection practices and improper tool usage	Weak default configurations and insecure protocols	Heterogeneous device interaction risks
Security tools considered	Firewalls, antivirus, IoT protection software and network security tools	Router configuration, TLS implementation and firmware security	General security mechanisms and frameworks
Regional characteristics	Diverse security maturity levels across users	Device-centric security evaluation	Non-region-specific analysis
Main contribution	Protection framework and practical recommendations	Security evaluation framework for devices	Identification of research gaps and future research directions

4. 1 Survey results and analysis

The survey findings show how participants perceive IoT security, which tools they use, and where further support is needed. The analysis also clarifies users' awareness of privacy, authentication, firmware updates, network protection and device-level security controls in smart-home and related IoT environments.

The questionnaire was created using SurveyMonkey and distributed to the general public, with a focus on Arabic-speaking participants. A total of 164 valid responses were collected from 12 countries, including Saudi Arabia, Egypt, Tunisia, Kuwait, Qatar, Bahrain, Oman, Iraq, Algeria, the United Kingdom, Australia and Turkey, as shown in Fig. 3.

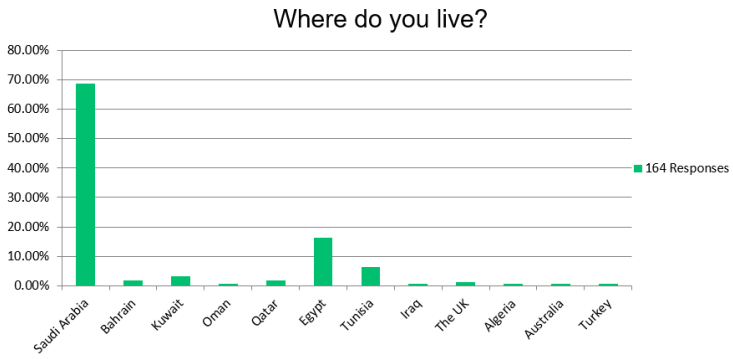


Fig. 3 Countries represented in the survey responses

Saudi Arabia, Egypt and Tunisia accounted for the largest shares of responses, with approximately 67. 07%, 15. 85% and 6. 10%, respectively. Bahrain and Qatar each contributed three responses, while Oman, Iraq, Algeria, Australia and Turkey each contributed one response.

Table 4 Percentage and number of survey participants by country

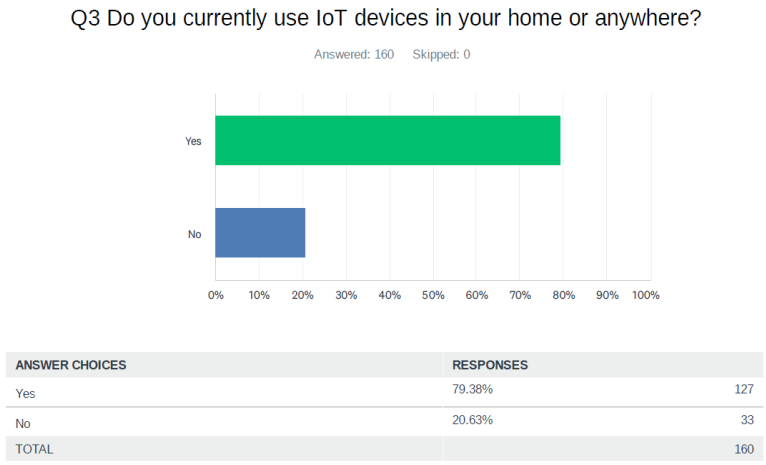
Country	Percentage	Number of participants
Saudi Arabia	67.07%	110
Bahrain	1.83%	3
Kuwait	3.05%	5
Oman	0.61%	1
Qatar	1.83%	3
Egypt	15.85%	26
Tunisia	6.10%	10
Iraq	0.61%	1
The United Kingdom	1.22%	2
Algeria	0.61%	1
Australia	0.61%	1
Turkey	0.61%	1
Total	100%	164

Question 2 shows a high level of participation among younger respondents, particularly those aged between 18 and 24, who represented more than half of the sample. This pattern is consistent with the rapid diffusion of IoT technologies among younger users

and students. Participation from older groups was lower, indicating that some demographic segments are still adapting to IoT technology, as illustrated in Fig. 4.

Fig. 4 Age distribution of survey participants

Most Arabic-speaking participants are familiar with IoT technology, and 127 participants also work with it. However, 33 participants do not use it at home or at work, representing less than 25% of all participants, as shown in Fig. 5.



ANSWER CHOICES	RESPONSES	
Yes	79.38%	127
No	20.63%	33
TOTAL		160

Fig. 5 Participants who use IoT technology

Question 4 shows that more than 50% of participants have between 1 and 3 IoT devices. However, for 7 devices or more and more than 10 devices, participation is less than 10%, indicating that IoT technology is increasing rapidly. Option B indicates that more than 30% of participants have between 4 and 6 devices. As shown in Fig. 6.

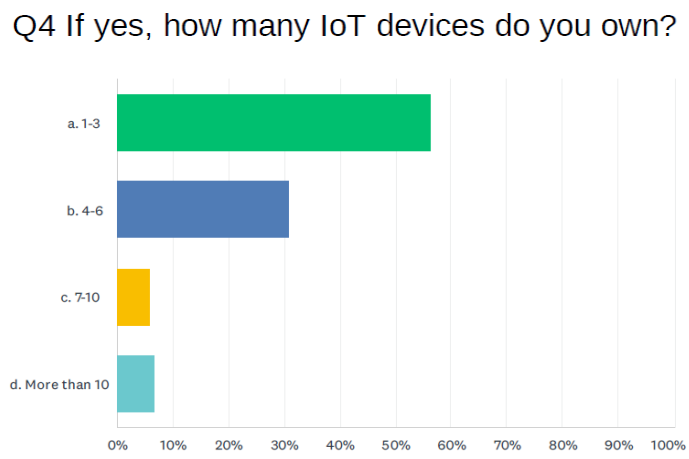


Fig. 6 Number of IoT devices used by participants

Here we demonstrate how users perceive privacy and security and why these are important to them. Privacy refers to protecting information for every IoT device and its users [4]. Security encompasses confidentiality, integrity, and access control [4], all of which ensure data availability when needed. Privacy and security represent central concerns within IoT systems, particularly due to threats such as distributed denial-of-service (DDoS) attacks [15]. Additional challenges include the limitations of existing security mechanisms [7], the heterogeneity of IoT devices [7], [15], constrained computational resources [28], and the energy costs associated with implementing security measures.,

Survey findings indicate that 38% of participants selected combined privacy and security factors as their primary means of protecting data. A further 35% emphasized security and privacy concerns, reflecting the strong cultural emphasis on privacy within Arab societies, where trust is a significant issue and religious values further reinforce the importance of personal privacy [66]. For analytical clarity, security and privacy were treated as separate categories. Security alone was selected by 10% of respondents, while privacy alone was chosen by 8%, as illustrated in Fig. 7. Although edge computing can help mitigate security and privacy risks [14], its capacity to handle large data volumes remains limited, reducing its overall effectiveness. In this context, blockchain technology offers a complementary solution by facilitating the development of secure, transparent, and trustworthy systems capable of addressing security and privacy challenges in edge computing environments [8], [14], [45]

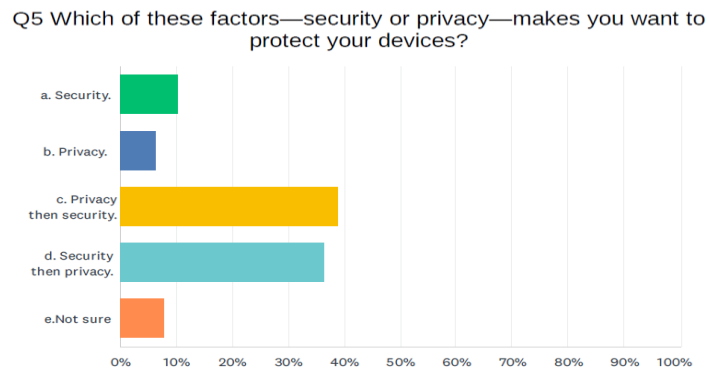


Fig. 7 Participants' perception of privacy and security

This question explores the frequency with which participants update IoT device firmware. While 20% of participants reported weekly updates and around 23% reported monthly updates, a large share update only every few months, rarely or never. This result suggests that many users are aware of IoT risks but still require clearer guidance on the importance of regular updates, as shown in Fig. 8.

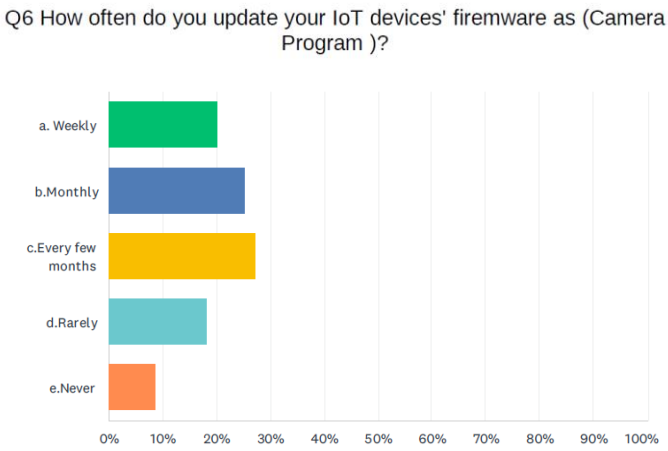


Fig. 8 Frequency of IoT firmware updates

This question assesses users' ability to select strong and unique passwords for IoT devices. Half of the participants reported that they always use strong passwords, while 30% do so sometimes. However, approximately 20% rarely or never use strong

passwords, indicating a continuing need for basic security awareness, as shown in Fig. 9.

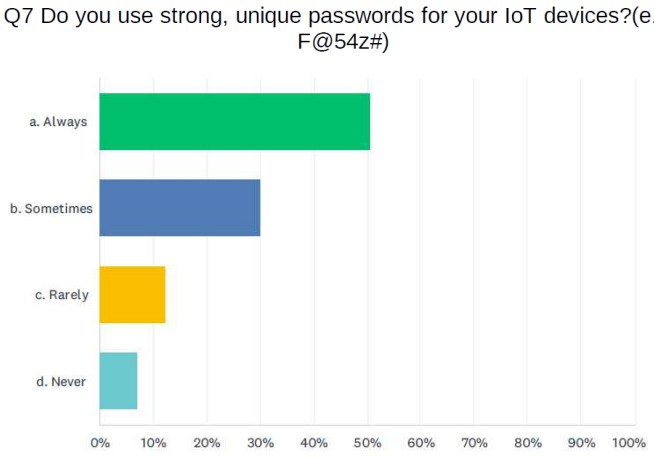


Fig. 9 Use of strong and unique passwords for IoT devices

This question examines the security methods that participants use for IoT devices and applications. Notably, over 45% of respondents selected option (a) Strong password, which relates to encryption types such as Symmetric Encryption (using one shared key) and Asymmetric Encryption (employing a public/private key pair). Common password encryption techniques include Rivest-Shamir-Adleman (RSA), Data Encryption Standard (DES), and Advanced Encryption Standard (AES), among others. In contrast, option (b) is regarded as more robust and secure than option (a), as it involves a two-step authentication process for accessing IoT devices or applications. Consequently, about 28% of participants chose (b), indicating that many still find it difficult to secure their IoT systems compared to organizations. Additionally, option (c) is an effective technique for protecting IoT devices, as it updates programs to identify new vulnerabilities or malware; however, less than 10% of respondents selected this option. Furthermore, around 5% of participants chose Network segmentation as a way to safeguard their IoT devices. The least popular choice is (e) None, which indicates a lack of awareness regarding IoT threats, posing a vulnerability. Approximately 7% of participants selected this option. In conclusion, while participants generally recognize the risks associated with IoT technology, they do not possess enough knowledge to determine the most effective methods to secure their IoT devices or applications. They are also aware of potential hazards linked to using IoT technology. As shown in Fig. 10.

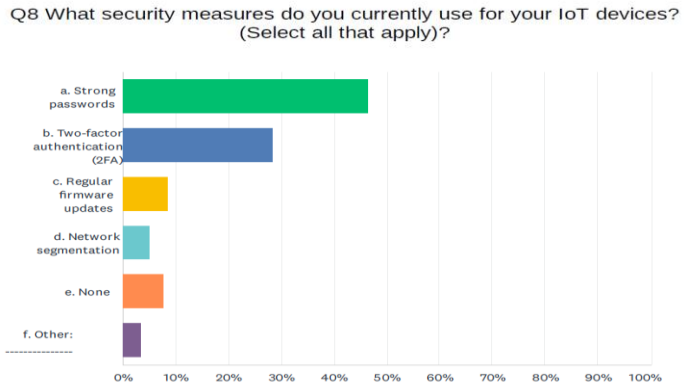


Fig. 10 Security measures used to safeguard IoT devices

In this section, we aim to emphasize the significance of how participants view updating their security settings. Option (a) received 20% of responses, producing a similar outcome to question 6. Conversely, option (b) attracted less than 20% of respondents. Option (c) exceeded 30% of participants, while in question 6, the same option ("Every few months") had around 28% of respondents. Therefore, we can conclude that most participants typically check the security settings of their IoT devices every two to three months. Option (d) accounted for approximately 22% of participants, and about 9% of respondents stated that they never review these settings, as illustrated in Fig. 11.

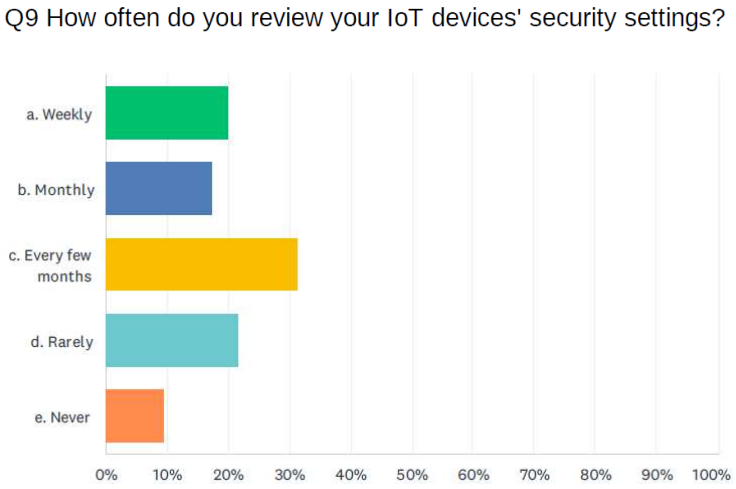


Fig. 11 Frequency of reviewing IoT device security settings

In this survey, over 50% of participants chose 'yes' to enable two-factor authentication (2FA) in their IoT systems for secure device management. Conversely, around 26% of respondents do not implement this method for their IoT systems or applications. The option 'Not sure' accounts for approximately 21% of participants, indicating their uncertainty regarding this technique and its functionality, as reflected in our earlier inquiries. As shown in Fig. 12.

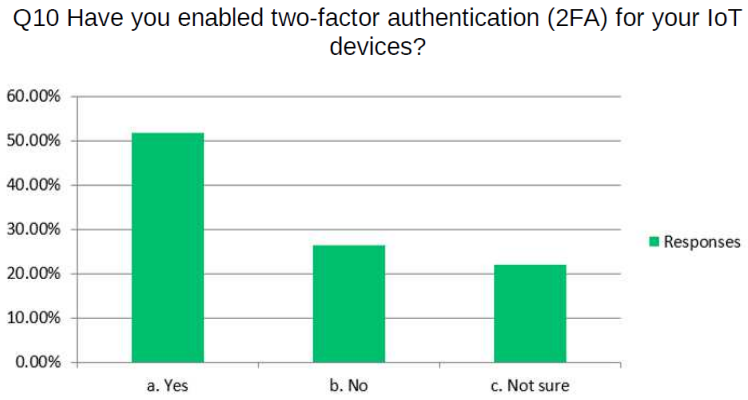


Fig. 12 Use of two-factor authentication (2FA) for IoT systems

This question focuses on device ownership among the broader public. The most common devices were smart appliances, security cameras and smart thermostats, used by roughly 40%, 39% and 37% of participants, respectively. According to several studies [64], [65], [66] and [45], businesses also commonly deploy security cameras and related IoT devices. Smart speakers and smart lighting were each reported by roughly 28% of participants, as shown in Fig. 13. This part of the survey therefore reflects individual-level IoT use.

IoT adoption is also expanding in the business sector. The study in [45] shows that the United States, Canada, Australia, Singapore and the United Kingdom possess essential national infrastructures that can support IoT and Industrial IoT (IIoT) deployment in the context of Industry 4.0, as shown in Table 5. Table 6 summarizes selected fields and locations where IoT technology is used in Arab

countries, although each country has a different level of infrastructure [56], [64], [66]-[71].

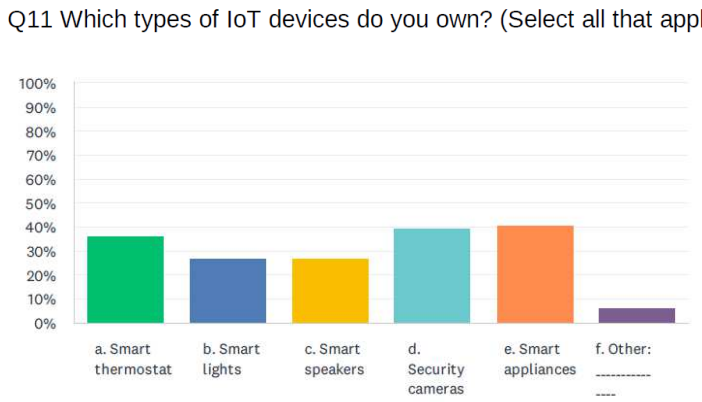


Fig. 13 Types of IoT devices used by participants

Table 5 Overview of key national infrastructures that may support IIoT deployment

Country	Number of fields	Fields	Ref.
The USA	16	Industry, finance, healthcare, energy, water and transportation systems	[45]
The UK	13	Not specified	Not specified
Canada	10	Not specified	Not specified
Singapore	9	Not specified	Not specified
Australia	8	Not specified	Not specified

Table 6 Selected Arab country infrastructure and IoT adoption indicators

Country	Number of companies	Number of fields	Fields	Ref.
Saudi Arabia	32	9	Industry, finance, healthcare, energy, water, transportation, education and agriculture	[64], [71]
Egypt	-	8	Not specified	[56], [67]-[69]
Tunisia	9	7	Not specified	[66], [70]
Qatar	-	9	Not specified	[71]

Country	Number of companies	Number of fields	Fields	Ref.
UAE	-	9	Not specified	[71]

The security of IoT devices and applications fundamentally depends on the network through which they operate. This section outlines the types of networks participants use to connect their IoT devices. Two primary options were identified, both reflecting users' awareness of IoT-related risks and their level of concern regarding security. Approximately 60% of participants reported relying on both their home networks and mobile networks supporting 4G and 5G connectivity. Fewer than 10% selected company networks, despite generally perceiving them as secure, likely due to strict organizational security policies. Meanwhile, more than 10% of respondents identified public networks as the least secure option, as illustrated in Fig. 14.

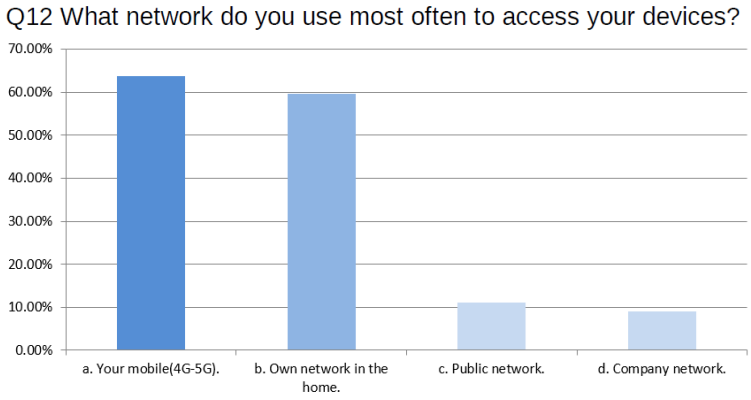


Fig. 14 Types of networks used to connect IoT devices

This question thoroughly explores users' understanding of IoT device security procedures and protocols. It also shows the number of tools they employed. Therefore, precisely 40% of respondents use antivirus software to protect their Internet of Things devices. However, roughly 27% of participants activated the firewall to secure their gadgets. Approximately 20% of participants reported using VPNs to establish secure connections for their devices, recognizing this as an effective method for protecting data exchanged between two endpoints. In addition, more than 20% indicated that they rely on IoT-specific security software to safeguard their devices. Notably, none of the participants selected the option indicating that they use no additional security measures in the corresponding survey option. As Fig. 15 demonstrates, less than 5% of respondents selected other tools, while more than 20% indicated that they do not use any specific program or tool to secure their

devices. The majority of users recognize the importance of employing security tools (programs, protocols, or approaches) to safeguard their IoT devices from IoT risks.

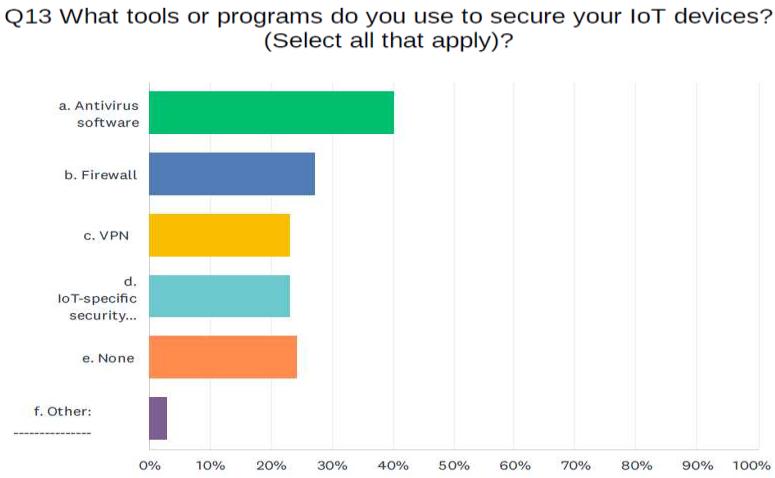


Fig. 15 Tools and programs used to secure IoT devices

Question 14 examines participant satisfaction with the tools and programs used to secure IoT devices. Fewer than 25% of respondents were very satisfied with their current methods. More than 40% were satisfied, while approximately 27% reported a neutral position. A small proportion were unsatisfied or very unsatisfied, indicating that existing tools still need to become clearer, more reliable and easier to use, as depicted in Fig. 16.

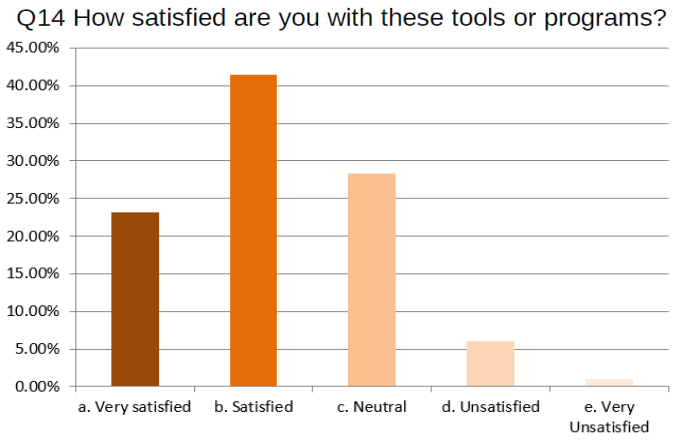


Fig. 16 User satisfaction with IoT security tools and programs

The main issues people face with IoT devices are outlined here. Over 50% of participants worry about privacy invasion, more than 49% about data theft, and around 46% are concerned about device hacking. To protect user data, all concerns highlight the need for strong security, which is considered the primary issue in the Internet of Things. According to [45], [64], [65], [66], [67], security is not only a concern for regular users but also for governments. Consequently, various studies have sought to find effective solutions for IoT risks such as Edge-of-Things and BC (BEoT) [19], Multi-Access Edge Computing (MEC) [57], and (DAG)-based blockchain like IOTA [62]. However, over 20% of participants are worried about losing control over their devices, and about 1% remain uncertain about their concerns regarding IoT security, as shown in Fig. 17.

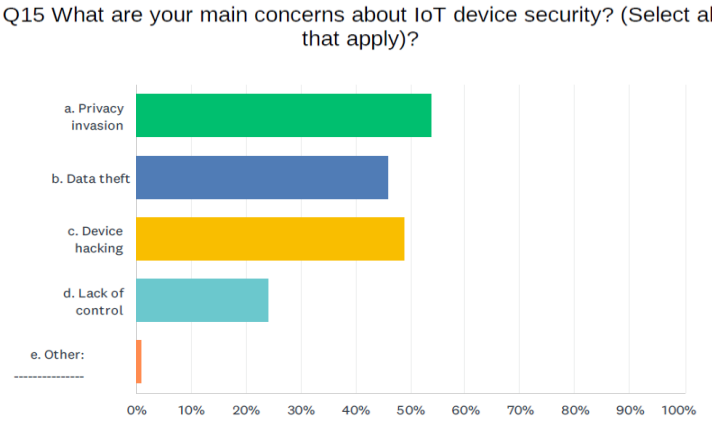


Fig. 17 Main concerns when using IoT devices

This question reveals the extent of users' awareness regarding IoT device security. 27% of participants are extremely knowledgeable about how to secure their IoT devices, while about 33% are somewhat informed. Additionally, 31% of respondents to option (c), “Not very experienced, ” stated that they lacked sufficient experience to handle configuring security on their IoT devices. Around 9% of respondents selected option (d), which is “not at all knowledgeable”. Overall, approximately 60% of participants have the knowledge necessary to secure their devices and protect their data, which is adequate to reduce IoT risks. Moreover, this percentage is considered excellent, reflecting the level of user awareness of IoT security, as shown in Fig. 18.

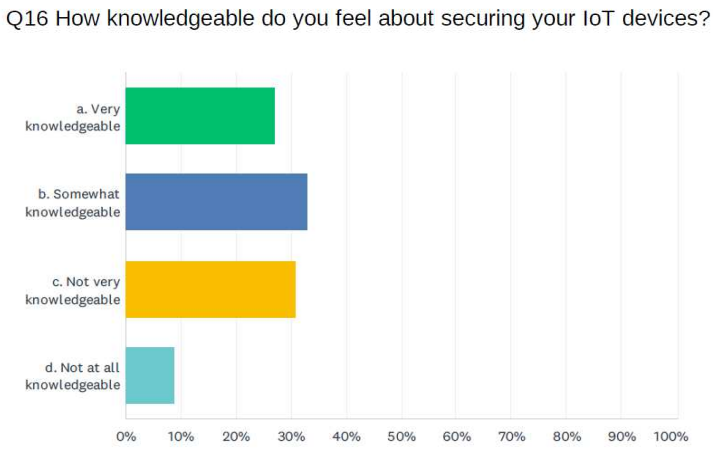


Fig. 18 User knowledge of IoT device security

Resources that could help users protect IoT devices more effectively are summarized in Fig. 19. Guides/tutorials and security checklists received the highest levels of support, at approximately 48% and 50%, respectively. Professional consultations and workshops or webinars were also identified as useful resources.

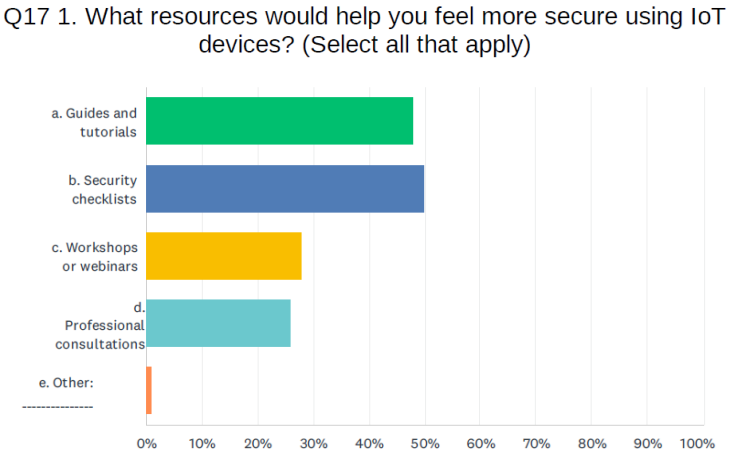


Fig. 19 Resources that can help users secure IoT devices

This section highlights that users' primary concern when using IoT devices is data privacy. Over 50% of respondents identified data privacy as their main worry. Furthermore, "Unauthorized Access" is selected by nearly 47% of respondents as the main threat to IoT security. About 27% of respondents chose "Device malfunction, " indicating that

devices may sometimes experience issues. The "Network security" option receives 40% of responses, which is less than the "Data privacy" option, as shown in Fig. 20. This suggests that users focus more on protecting their data than on the security of their network. However, the network security concern is still significant. According to [64], 52% of 328 businesses are worried about security and privacy. Additionally, developers are primarily concerned with this issue [66]. Since hacking and data theft could have severe consequences for users, researchers and developers should prioritize developing methods to reduce IoT risks.

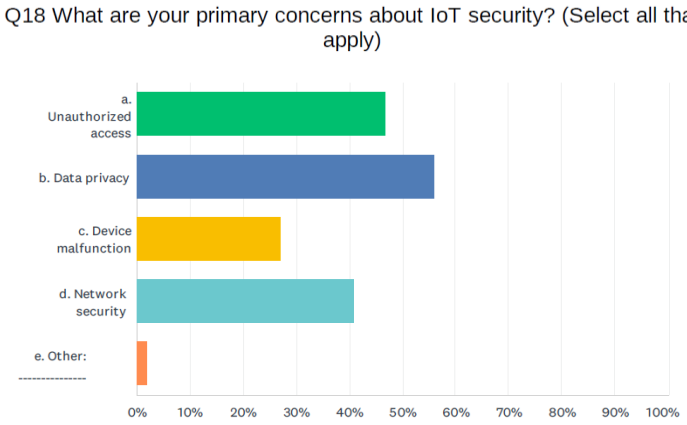


Fig. 20 Primary concerns about IoT security

This question directly supports the main objective of the study by showing that both individuals and organizations require stronger guidance and practical tools for IoT security. Approximately 55% of respondents expressed a need for more information on security tools, while 31% selected professional security assessment and 22% selected community support groups, as shown in Fig. 21.

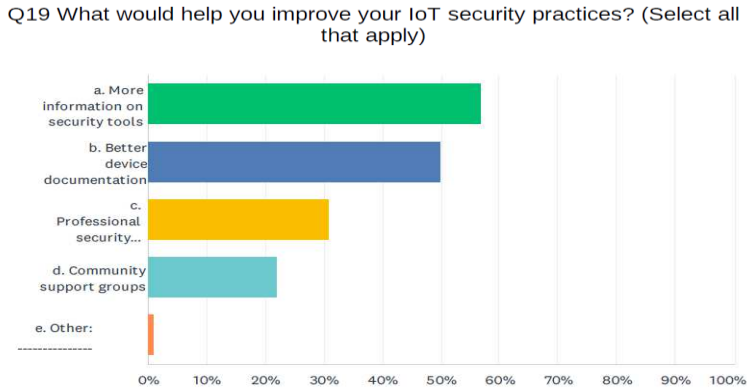


Fig. 21 Options that can help users improve IoT security practices

5 Recommendations

Based on the survey findings, we recommend combining user-oriented security tools with IoT applications and devices. Recommended mechanisms include strong authentication, regular firmware updates, firewall protection, VPNs, network segmentation and IoT-specific security software. In organizational settings, blockchain and edge computing can also strengthen confidentiality, data integrity and authentication while helping to address latency and scalability constraints [4], [14], [15], [45]. These recommendations are summarized in Tables 7 and 8.

Table 7 Techniques for safeguarding data in IoT devices

No.	Tool used	Technique	Latency	Security
1	IoT-specific security software	Secures IoT applications and devices	Depends on the number of IoT devices	Yes
2	Firewall	Works as a filter	Yes; scanning may add delay	Yes
3	VPN	Secures connections and transactions	Depends on distance and technology	Yes
4	Antivirus software	Works as a filter	Yes; scanning may add delay	Yes
5	Two-factor authentication (2FA)	Requires two authentication steps	Yes; authentication adds delay	Yes
6	Network segmentation	Distributes network load and reduces congestion	No; it can reduce congestion when configured properly	Yes
7	Strong passwords	Protects access credentials but does not by itself secure data or transactions	No; single-step access	No

Table 8 Comparison of technologies based on security, energy cost, scalability, performance and latency

Technology/protocol	Security	Energy cost	Scalability	Performance	Latency	Ref.
IoT apps/devices	Weak	Low	Low	Low	Yes	[28], [31], [37], [66]
EC	Medium	High	No	High	No	[15], [38], [40], [62]
BC	Strong	Depends on complexity	Yes	High	Depends on complexity	[14], [19], [20], [45], [72]
PUFchain, PoW, PUF-enabled, BEoT, BlockEdge and BC-edge frameworks	See Table 2	See Table 2	See Table 2	See Table 2	See Table 2	Table 2

The comparative analysis demonstrates that the proposed MENA-based study addresses an important gap between technical security research and conceptual security studies. While technical studies provide detailed insights into vulnerabilities, and global surveys provide theoretical frameworks, the present work contributes a practical perspective by analyzing how security tools are actually used in real environments. This enables the development of recommendations that are more applicable to real-world deployments, particularly in emerging IoT markets within the MENA region.

Table 9 Comparative security recommendations

Category	MENA region recommendation	China study recommendation	Global studies recommendation
Device security	Encourage adoption of security tools and regular updates	Improve secure default configurations	Standardized device security architecture
Network protection	Promote firewall usage and network segmentation	Enforce secure firmware updates and TLS implementation	Multi-layered security models
Manufacturer role	Provide simplified and accessible security tools	Strengthen default security settings	Develop interoperable security standards
Framework direction	User-centric protection framework	Device-centric evaluation framework	Holistic ecosystem security frameworks

6 Conclusion

As the Internet of Things (IoT) continues to expand into various sectors, including healthcare, smart homes, and industrial applications, significant security and privacy challenges arise. This study has highlighted the pressing concerns individuals and

organizations face regarding IoT security, reflecting a strong preference for privacy over security measures. Survey results indicate that a majority of respondents prioritize methods to enhance the security of their existing devices rather than investing in newer technology. Moreover, despite general awareness of the IoT landscape, many users still lack adequate knowledge and tools for effectively safeguarding their devices. Nevertheless, the research conducted by Ratna (2020) highlighted numerous challenges to the deployment of IoT, including security issues, costs, infrastructure limitations, and IoT quality. Furthermore, security and scalability have emerged as urgent issues for essential infrastructures in the context of Industry 4.0 [45]. To address these vulnerabilities, it is imperative to adopt comprehensive security frameworks that integrate advanced technologies like blockchain and edge computing. Such solutions can provide robust protection through decentralization, improved authentication, data integrity, and user privacy. Continued research and development in security protocols are essential to create a safer IoT ecosystem. Engaging stakeholders and raising awareness about IoT security measures will also empower users to make informed decisions, ultimately fostering a more secure digital environment.

Declarations

Funding
The authors declare that no funding was received for this work.

Competing interests
The authors declare no competing interests.

Ethics approval and consent to participate
The study used an anonymous online questionnaire. Participation was voluntary, and informed consent was obtained from participants before completing the survey.

Consent for publication
Not applicable.

Data availability
The datasets generated and analyzed during the current study are available from the corresponding author on reasonable request.

Author contributions
All authors contributed to the conception, survey design, analysis, writing and revision of the manuscript. All authors read and approved the final manuscript.

Acknowledgements

The authors thank all survey participants for their contribution to this study.

References

1. Nguyen, T. , Nguyen, H. , & Gia, T. N. (2024). Exploring the integration of edge computing and blockchain IoT: Principles, architectures, security, and applications. Journal of Network and Computer Applications, 226, 103884.
2. Hammoud, A. , Sami, H. , Mourad, A. , Otrok, H. , Mizouni, R. , & Bentahar, J. (2020). AI, blockchain, and vehicular edge computing for smart and secure IoV: Challenges and directions. IEEE Internet of Things Magazine, 3(2), 68-73.
3. Rakshe, A. , & Dongre, N. (2024, April). Survey on Security Protocols for IoT. In 2024 IEEE 9th International Conference for Convergence in Technology (I2CT) (pp. 1-5). IEEE.
4. Sharma, V. , You, I. , Andersson, K. , Palmieri, F. , Rehmani, M. H. , & Lim, J. (2020). Security, privacy and trust for smart mobile-Internet of Things (M-IoT): A survey. IEEE access, 8, 167123-167163.
5. Touqeer, H. , Zaman, S. , Amin, R. , Hussain, M. , Al-Turjman, F. , & Bilal, M. (2021). Smart home security: Challenges, issues and solutions at different IoT layers. Journal of Supercomputing, 77(12).
6. Kavitha, L. , & Shaik, K. (2025, August). A Comprehensive Survey of Threat Detection and Mitigation in Layered IoT Security Frameworks. In 2025 5th International Conference on Soft Computing for Security Applications (ICSCSA) (pp. 277-283). IEEE.
7. Park, J. H. , Yotxay, S. , Singh, S. K. , & Park, J. H. (2024). PoAh-enabled federated learning architecture for DDoS attack detection in IoT networks. Hum. -Centric Comput. Inf. Sci, 14(3).
8. https: //www. statista. com/statistics/1183457/iot-connected-devices-worldwide/
9. Panwar, N. , Sharma, S. , Mehrotra, S. , & Venkatasubramanian, N. (2019). Smart home survey on security and privacy. arXiv preprint arXiv: 1904.05476.
10. Pattnaik, N. , Li, S. , & Nurse, J. R. (2023). A survey of user perspectives on security and privacy in a home networking environment. ACM computing surveys, 55(9), 1-38.
11. Siddiqa, A. , Shah, M. A. , Khattak, H. A. , Akhunzada, A. , Ali, I. , Razak, Z. B. , & Gani, A. (2018). Social internet of vehicles: Complexity, adaptivity, issues and beyond. IEEE access, 6, 62089-62106.
12. Khan, Zulfiqar Ali, and Akbar Siami Namin. "The applications of blockchains in addressing the integration and security of iot systems: A survey. " 2021 IEEE International Conference on Big Data (Big Data). IEEE, 2021.
13. Minh, Q. N. , Nguyen, V. H. , Quy, V. K. , Ngoc, L. A. , Chehri, A. , & Jeon, G. (2022). Edge computing for IoT-enabled smart grid: The future of energy. Energies, 15(17), 6140.
14. Zhang, J. , Lu, C. , Cheng, G. , Guo, T. , Kang, J. , Zhang, X. , . . & Yan, X. (2021). A blockchain-based trusted edge platform in edge computing environment. Sensors, 21(6), 2126.
15. Xu, Z. , Liu, W. , Huang, J. , Yang, C. , Lu, J. , & Tan, H. (2020). Artificial intelligence for securing IoT services in edge computing: a survey. Security and communication networks, 2020, 1-13.
16. Jurcut, A. , Niculcea, T. , Ranaweera, P. , & Le-Khac, N. A. (2020). Security considerations for Internet of Things: A survey. SN Computer Science, 1(4), 193.
17. Bastos, D. , Shackleton, M. , & El-Moussa, F. (2018). Internet of things: A survey of technologies and security risks in smart home and city environments. In Living in the Internet of Things: Cybersecurity of the IoT-2018 (p. 30). Stevenage UK: IET.

18. Alaskri, A. , Ahmed, N. A. S. , & Shaari, H. (2023, May). Internet of Things (IoT): survey of most important security risks. In 2023 IEEE 3rd International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering (MI-STA) (pp. 295-299). IEEE.
19. Parker, B. , & Bach, C. (2020). The synthesis of blockchain, artificial intelligence and internet of things. European Journal of Engineering and Technology Research, 5(5), 588-593.
20. Xuan, S. , Chen, Z. , Chung, I. , Tan, H. , Man, D. , Du, X. , . . & Guizani, M. (2021). ECBCM: a prestige-based edge computing blockchain security consensus model. Transactions on Emerging Telecommunications Technologies, 32(6), e4015.
21. K. Gai, Y. Wu, L. Zhu, Z. Zhang, and M. Qiu, Differential Privacy- Based Blockchain for Industrial Internet-of-Things, IEEE Trans. Ind. Inf. , vol. 16, no. 6, pp. 4156–4165, Jun. 2020, doi: 10. 1109/TII. 2019. 2948094.
22. P. B et al. , Toward Blockchain for Edge-of-Things: A New Paradigm, Opportunities, and Future Directions, IEEE Internet Things M, vol. 4, no. 2, pp. 102–108, Jun. 2021, doi: 10. 1109/IOTM. 0001. 2000191. Available: https: //ieeexplore. ieee. org/document/9409843/. [Accessed: Sep. 20, 2025].
23. J. Li, J. Wu, L. Chen, J. Li, and S. -K. Lam, Blockchain- Based Secure Key Management for Mobile Edge Computing, IEEE Trans. on Mobile Comput, vol. 22, no. 1, pp. 100–114, Jan. 2023, doi: 10. 1109/TMC. 2021. 3068717. Available: https: //ieeexplore. ieee. org/document/9387145/. [Accessed: Sep. 20, 2025].
24. Sun, Y. , Ochiai, H. , & Esaki, H. (2021). Decentralized deep learning for multi-access edge computing: A survey on communication efficiency and trustworthiness. IEEE Transactions on Artificial Intelligence, 3(6), 963-972.
25. Al-Garadi, M. A. , Mohamed, A. , Al-Ali, A. K. , Du, X. , Ali, I. , & Guizani, M. (2020). A survey of machine and deep learning methods for internet of things (IoT) security. IEEE communications surveys & tutorials, 22(3), 1646-1685.
26. Akli, A. , & Chougdali, K. (2024, July). A Survey on IOTA Based Technology for Enhanced IoT Security. In 2024 11th International Conference on Wireless Networks and Mobile Communications (WINCOM) (pp. 1-6). IEEE.
27. Handayani, I. , Apriani, D. , Mulyati, M. , Zahra, A. R. A. , & Yusuf, N. A. (2023). Enhancing security and privacy of patient data in healthcare: A smartpls analysis of blockchain technology implementation. IAIC Transactions on Sustainable Digital Innovation (ITSDI), 5(1), 8-17.
28. Hameed, A. , & Alomary, A. (2019, September). Security issues in IoT: A survey. In 2019 International conference on innovation and intelligence for informatics, computing, and technologies (3ICT) (pp. 1-5). IEEE.
29. Zhang, C. , & Green, R. (2015, April). Communication security in internet of thing: preventive measure and avoid DDoS attack over IoT network. In Proceedings of the 18th Symposium on Communications & Networking, International Society for Computer Simulation, pp. 8-15, 2015.
30. Strohmier, H. , Lowe, J. R. , Rodriguez, A. G. , & Trammell, M. M. (2024, April). Security and Privacy Threats Posed by IoT Devices Used by Students on College Campuses. In 2024 12th International Symposium on Digital Forensics and Security (ISDFS) (pp. 1-6). IEEE.
31. Hassija, V. , Chamola, V. , Saxena, V. , Jain, D. , Goyal, P. , & Sikdar, B. (2019). A survey on IoT security: application areas, security threats, and solution architectures. IEEE Access, 7, 82721-82743.
32. Miller, D. (2018). Blockchain and the internet of things in the industrial sector. IT professional, 20(3), 15-18.

33. J. Zhao, B. Zhou, J. P. Butler, R. G. Bock, J. P. Portelli, and S. G. Bil´en, “IoT-based sanitizer station network: A facilities management case study on monitoring hand sanitizer dispenser usage, ” Smart Cities, vol. 4, no. 3, pp. 979–994, 2021.
34. Adam, M. , Hammoudeh, M. , Alrawashdeh, R. , & Alsulaimy, B. (2024). A survey on security, privacy, trust, and architectural challenges in IoT systems. IEEE Access, 12, 57128-57149.
35. Shtayat, M. B. M. , Hasan, M. K. , Sulaiman, R. , Islam, S. , & Khan, A. U. R. (2023). An explainable ensemble deep learning approach for intrusion detection in industrial internet of things. IEEE Access, 11, 115047-115061.
36. Ye, J. , De Carnavalet, X. D. C. , Zhao, L. , Zhang, M. , Wu, L. , & Zhang, W. (2024). Exposed by Default: A Security Analysis of Home Router Default Settings and Beyond. IEEE Internet of Things Journal.
37. Ahmed, W. K. , & Mohammed, R. S. (2022, March). Lightweight authentication methods in IoT: Survey. In 2022 International Conference on Computer Science and Software Engineering (CSASE) (pp. 241-246). IEEE.
38. Bourechak, A. , Zedadra, O. , Kouahla, M. N. , Guerrieri, A. , Seridi, H. , & Fortino, G. (2023). At the Confluence of Artificial Intelligence and Edge Computing in IoT-Based Applications: A Review and New Perspectives. Sensors, 23(3), 1639.
39. Amanullah, M. A. , Habeeb, R. A. A. , Nasaruddin, F. H. , Gani, A. , Ahmed, E. , Nainar, A. S. M. , . . & Imran, M. (2020). Deep learning and big data technologies for IoT security. Computer Communications, 151, 495-517.
40. Xiao, X. , & Zhao, M. (2022). Edge computing clone node recognition system based on machine learning. Neural Computing and Applications, 34(12), 9289-9300.
41. Lv, Z. , Chen, D. , Lou, R. , & Wang, Q. (2021). RETRACTED: Intelligent edge computing based on machine learning for smart city.
42. Chaabane, N. , Mahfoudhi, S. , & Belkadhi, K. (2024). Interpolation based iot sensors selection. IEEE Sensors Journal.
43. Khan, A. A. , Laghari, A. A. , Baqasah, A. M. , Alroobaea, R. , Almadhor, A. , Sampedro, G. A. , & Kryvinska, N. (2024). Blockchain-enabled infrastructural security solution for serverless consortium fog and edge computing. PeerJ Computer Science, 10, e1933.
44. Gill, S. S. (2024). Quantum and blockchain based Serverless edge computing: A vision, model, new trends and future directions. Internet Technology Letters, 7(1), e275.
45. Wu, Y. , Dai, H. N. , & Wang, H. (2020). Convergence of blockchain and edge computing for secure and scalable IIoT critical infrastructures in industry 4.0. IEEE Internet of Things Journal, 8(4), 2300-2317.
46. Liu, W. , Cao, B. , & Peng, M. (2022). Blockchain based offloading strategy: Incentive, effectiveness and security. IEEE Journal on Selected Areas in Communications, 40(12), 3533-3546.
47. T. Kumar et al. , BlockEdge: Blockchain-Edge Framework for Industrial IoT Networks, IEEE Access, vol. 8, pp. 154166–154185, 2020, doi: 10. 1109/ACCESS. 2020. 3017891.
48. Shouran, Z. , Ashari, A. , & Priyambodo, T. (2019). Internet of things (IoT) of smart home: privacy and security. International Journal of Computer Applications, 182(39), 3-8.
49. Puthal, D. , Mohanty, S. P. , Yanambaka, V. P. , & Kougianos, E. (2020). Poah: A novel consensus algorithm for fast scalable private blockchain for large-scale iot frameworks. arXiv preprint arXiv: 2001. 07297.
50. Bisiach, J. , & Elfving, V. (2021). PUF-enabled blockchain for IoT security: a comparative study

51. Mohanty, S. P. , Yanambaka, V. P. , Kougianos, E. , & Puthal, D. (2020). PUFchain: A hardware-assisted blockchain for sustainable simultaneous device and data security in the internet of everything (IoE). IEEE Consumer Electronics Magazine, 9(2), 8-16.
52. Mandarino, V. , Pappalardo, G. , & Tramontana, E. (2024). A blockchain-based electronic health record (ehr) system for edge computing enhancing security and cost efficiency. Computers, 13(6), 132.
53. Miriam, H. , Doreen, D. , & Rene Robin, C. R. (2023). Secured Cyber Security Algorithm for Healthcare System Using Blockchain Technology. Intelligent Automation & Soft Computing, 35(2).
54. Kishor, A. , & Chakarbarty, C. (2022). Task offloading in fog computing for using smart ant colony optimization. Wireless personal communications, 127(2), 1683-1704.
55. Lei, K. , Du, M. , Huang, J. , & Jin, T. (2020). Groupchain: Towards a scalable public blockchain in fog computing of IoT services computing. IEEE Transactions on Services Computing, 13(2), 252-262.
56. Yousra, B. , Yassine, S. , Yassine, M. , Said, S. , Lo'ai, T. , & Salah, K. (2023). A novel secure and privacy-preserving model for openid connect based on blockchain. IEEE Access 11, 67660–67678.
57. Ali, B. , Gregory, M. A. , & Li, S. (2021). Multi-access edge computing architecture, data security and privacy: A review. IEEE Access, 9, 18706-18721.
58. Illy, P. , & Kaddoum, G. (2023). A collaborative DNN-based low-latency IDPS for mission-critical smart factory networks. IEEE Access, 11, 96317-96329.
59. Li, J. , Wu, J. , Chen, L. , Li, J. , & Lam, S. K. (2021). Blockchain-based secure key management for mobile edge computing. IEEE Transactions on Mobile Computing, 22(1), 100-114.
60. Wadhwa, S. , Rani, S. , Verma, S. , Shafi, J. , & Wozniak, M. (2022). Energy efficient consensus approach of blockchain for IoT networks with edge computing. Sensors, 22(10), 3733.
61. Gangwani, P. , Perez-Pons, A. , Joshi, S. , Upadhyay, H. , & Lagos, L. (2023). Integration of data science and IoT with blockchain for industry 4.0. In Blockchain and its Applications in Industry 4.0 (pp. 139-177). Singapore: Springer Nature Singapore.
62. T. Qiu, J. Chi, X. Zhou, Z. Ning, M. Atiquzzaman, and D. O. Wu, Edge Computing in Industrial Internet of Things: Architecture, Advances and Challenges, 3rd ed IEEE Commun. Surv. Tutorials, vol. 22, no. 4,
63. Zhang, J. , Chen, H. , Gong, L. , Cao, J. , & Gu, Z. (2019, June). The current research of IoT security. In 2019 IEEE Fourth International Conference on Data Science in Cyberspace (DSC) (pp. 346-353). IEEE.
64. Communications and Technology Information Commission. (2021). IoT Demand in Saudi Arabia-A Survey Based Study (2021).
65. Ahmed, M. , Abdou, M. Y. K. , & Elnagar, A. M. (2022). The impact of implementing the Internet of Things (IoT) on customer satisfaction: evidence from Egypt. Journal of Association of Arab Universities for Tourism and Hospitality, 22(2), 365-380
66. Hamlaoui, S. , & Weber, A. S. (2020, February). The Internet of Things (IoT) in Tunisian education and healthcare: prospects and barriers to improved educational and medical outcomes. In 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT) (pp. 603-607). IEEE.
67. Shahin, Y. (2020). Technological acceptance of the Internet of things (IOT) In Egyptian schools. International Journal of Instructional Technology and Educational Studies, 1(1), 6-10.
68. Abdel Hamid, M. M. (2024). Internet of Things as an Instrument to Improve Businesses of Egyptian Tourism Companies. Journal of Association of Arab Universities for Tourism and Hospitality, 27(2), 155-169.

69. National Telecom Regulatory Authority, (2022), Internet of Things (IoT) Framework In the Arab Republic of Egypt, IoT Regulatory Framework in the Arab Republic of Egypt(report).
70. Frikha, T. , Ktari, J. , Amor, N. B. , Chaabane, F. , Hamdi, M. , Denguir, F. , & Hamam, H. (2024). Low power blockchain in industry 4.0 case study: water management in Tunisia. Journal of Signal Processing Systems, 96(3), 257-271.
71. Merghemi, O. , Klibet, M. A. , & Zermane, T. (2025). The reality and prospects of using internet of things (IoT) technology in the economies of the Arab region (Saudi Arabia, UAE, Qatar). Journal of Engineering Management and Competitiveness (JEMC), 15(2), 83-99.
72. Kotobi, K. , & Sartipi, M. (2018, September). Efficient and secure communications in smart cities using edge, caching, and blockchain. In 2018 IEEE international smart cities conference (ISC2) (pp. 1-6). IEEE.