The Future of IoT Security in Saudi Arabian Start-Ups: A Position Paper

Safar Albaqami*, Maziar Nekovee, Imran Khan
6G Lab-Centre for Advanced Communications, Mobile Technology and IoT-School of Engineering and Informatics, University of Sussex, Brighton BN1 9RH, UK

***Abstract*—This research explores the intricacies of implementing and securing Internet of Things (IoT) technology in Saudi Arabian startups. In the middle of Saudi Arabia's ambitious pursuit of social and economic progress via IoT breakthroughs, entrepreneurs have emerged as critical participants grappling with serious computing security challenges. This study conducts a thorough examination of the cybersecurity risks associated with start-up in Saudi Arabia's IoT applications, technologies and innovations by reviewing a wide range of publications. The key objectives are to identify the main cybersecurity risks, analyze the impact of IoT device networking on privacy and security, and propose strategies to mitigate these threats. Furthermore, the study stresses the importance of funding up-to-date security technologies, cooperation with the cyber experts, and shifting towards the cloud-based security. Also, the study identifies the importance of cybersecurity education and training to enhance the defensive mechanisms of the startups against cyber threats. This study provides novel insights by identifying the distinct cybersecurity obstacles encountered by IoT-enabled businesses in Saudi Arabia and proposing a complete framework to enhance their security architecture. Robust cybersecurity policies are vital for both unleashing the transformative potential of IoT for startups and guiding Saudi Arabia towards its objective of being a worldwide leader in IoT. This paper advocates for a cooperative strategy that involves policymakers, industry stakeholders, and entrepreneurs to prioritize and allocate resources towards a safe and robust IoT ecosystem. This would help promote economic development and innovation in the country.**

Keywords*—*IoT; Saudi Arabia; start-ups; computing security challenges; technology; innovation; cyber threats

I. Introduction

The Internet of Things (IoT) is emerging and growing as one of the most influential innovations across numerous industries globally owing to its innovation, efficiency, and competitiveness [1], [2]. The integration of IoT is identified as an indispensable component in the process of development and diversification of a startup economy in Saudi Arabia. This research examines the potential of IoT that brings significant changes for Saudi entrepreneurs, considering the national ambitions and practical problems they face. Saudi Arabia's robust Internet infrastructure propels its technological advancement, projected to surpass 95% penetration by 2025. This is a suitable environment for the emergence of digital firms [3], [4]. Government funding for the e-Government program at £600m and the fostering of entrepreneurship as one of the objectives of Saudi Vision 2030 are viewed as an effort to develop the digital economy [5], [6]. These activities in conjunction with venture capital investments, aim to reduce the financial disparity for firms that use IoT technology, in line with the country's objectives of fostering innovation and entrepreneurship. Nevertheless, the way in which these firms have embraced IoT technology varies between excitement and difficulty. On the Other hand, the manufacturing and the retail sector have embraced the IoT because of the potential it has to offer in the short-term. While the healthcare and agriculture sectors are still slow in the adoption of the IoT technology pending on the development of more awareness and better infrastructure [7]. Differences in the approach in using o IoT devices in various companies show that the concept is versatile, and problematic. Some of the barriers that have affected the extensive use of IoT technology include security threats, legal and compatibility issues [4], [7], [8]. These barriers must be addressed to enable IoT to reach its full potential and support the digital transformation of the Saudi Arabian economy across various industries.

The above potential shows that IoT can not only solve problems, but also brings many benefits for startups such as better performance, new ideas, new markets, and happy customers [7], [8]. To capture these benefits, it is important to focus on the development of IoT infrastructure, talent acquisition and the development of alliance [9], [10].

Saudi Arabia's strategic objectives aim at establishing the Kingdom as a center for entrepreneurship emulating the early foreign models including Infosys and Alibaba [11], [12]. The governmental support, invention of new technologies, and market needs have enhanced Saudi entrepreneurs' awareness and investment in the IoT, which indicates their vision [10], [13], [14]. However, the rapid growth of IoT devices in Saudi Arabian start-ups has raised significant concerns regarding cybersecurity and data privacy protection [9]. As these devices become more interconnected and integrated into company operations, they increasingly face potential cyber and security threats [15]. Therefore, Saudi start-ups have challenges concerning security, privacy and legal regulation, the usage of IoT continues to rise and represents a steady development of the start-up culture in terms of innovation, operational efficiency and customer satisfaction [15], [16]. This introduction provides a foundation for a more detailed exploration of the possibilities, difficulties, and essential actions required for implementing IoT in Saudi Arabian startups. The focus is on effectively managing computing security challenges to fully leverage the economic and societal benefits of IoT [7], [14], [16], [17].

*Corresponding Author

A. Background

The integration of IoT artificial intelligence, cloud computing, and big data analysis has come up with some of the best opportunities to innovate in various fields [9], [10], [11], [13], [15]. Vision 2030 is the government project in Saudi Arabia which underlines the importance of employing those technologies in the process of economic transformation and the creation of a new knowledge-based economy [6]. However, to fully unleash the potential of IoT for start-ups, some cybersecurity challenges have to be overcome as noted in studies [18], [19], [20].

B. Scope of the Paper

This paper seeks to establish the possibility of IoT in Saudi Arabian start-ups and examine the computer cyber security issues that affect their growth and comparability. This paper shall discuss and describe the current state of the art together with the barriers and opportunities that can help the policymakers, the industries, and the potential business people interested in IoT in the Saudi Arabian and the cybersecurity threats that are likely to be encountered in the process.

C. Research Problem

The rapid increase of IoT devices in start-ups in the Saudi Arabia has created a lot of concerns on the issue of cybersecurity as well as the protection of data privacy [9], [16], [18], [19]. Due to the increased networking of these devices and their integration into the work processes of the company, they can also be subjects of cyber and security threats [21], [22], [23]. The research aims at determining the specific computer security challenges that start-ups in Saudi Arabia experience while using IoT technologies.

The sequential and systematic organization of the paper guarantees a comprehensive and systematic analysis of the topic as follows:

- Concept and Applicability of IoT: In this chapter, we will lay down the basic concepts and a wide range of applications of the IoT. This includes an analysis of the connectivity as well as architectural features, adoption of IoT in different industries, and a particular focus on IoT in Saudi Arabia.
- Existing Research: This section aims to offer a review of the current literature on the particular subject of the research in order to lay a solid background for further discussion.
- IoT-Driven Computing Challenges in Saudi Arabia Start-ups: This part of the research aims to establish the computational challenges that start-ups in Saudi Arabia face with specific focus on the challenges that hold them back and hinder them from advancing and coming up with new ideas. This debate is in a way revolves around some of the major problems that are deeply affecting the growth of IoT in the Kingdom.
- The Role of Vision 2030 in Promoting IoT: This section focuses on the role of Saudi Arabia's Vision 2030 in supporting the integration of the IoT technology into the Saudi Arabia innovation and economic transformation agendas. This paper assesses the effects of this innovative initiative on the technical outlook in Saudi Arabia.
- Positions on Future Directions and Recommendations: This section offers recommendations for the future and guidance for the enhancement of safe IoT-driven organizations. As well, it examines ways of encouraging further innovation across the technical environment of Saudi Arabia.
- Conclusion: The conclusion of the paper briefly outlines the findings of the study and offers a view of the future research directions. Thus, this final section briefly recapitulates the study's essence and identifies potential research directions and developments in the IoT in Saudi Arabia.

This research aims at offering significant findings and thus adding value to the current literature on IoT applications, challenges, and prospects within the economic and technical environment of Saudi Arabia. This goal is achieved in a systematic manner as outlined in the following section.

II. Concept and Applicability of IoT

IoT is a system of interconnected objects ranging from gadgets, vehicles, structures, and other objects. Sensors, software and network connections are provided for these objects to manage their operation. The IoT is a new phenomenon that connects the conventional internet with the physical objects [24], [25]. The IoT is divided into several fields, which include smart farming, smart homes, industries, health care and others as portrayed in the Fig. 1 [3], [8], [25]. Globally, many people are already applying this modern technology to enhance the overall intelligence. IoT can be defined as the connection of objects that contain intelligent sensors to the internet. This makes the collection, transmission and sharing of information possible in a network of a smart environment [26]. Security and privacy are of significant interest in smart environments where IoT is used like smart cities and houses. Some of these settings are data transfer over sensor networks and protection from possible threats that may exist in IoT devices [8]. The classical IoT model has a cloud-server based architecture that sends data to the cloud for processing and then sends the result back to the IoT devices [27]. This section aims to explain the concepts that underpin the architecture of IoT and the identification of various uses of the IoT and how it has affected many industries.

A. IoT Connectivity and Architecture

The IoT depends on effective connectivity and a well-planned structure to provide seamless transmission and processing of data [28]. Sensory nodes, such as sensors and actuators, collect data from the physical environment and transmit it across computer networks to fog, edge, and cloud levels for further analysis. The fog layer is intermediate between the edge and the cloud layer. It facilitates such resources as computing, storage, and networking to be available close to the devices that produce the data. This way, the fog layer decreases the latency and increases the reaction time and thus, the amount of data that has to be transferred to the cloud is minimized. This is very important in real time applications as

indicated by [28] and [29]. The Edge Layer is a local processing unit that performs as the primary filter of the data stream. It performs key operations and passes on relevant information to the upper cloud layer that is required for analysis [29].

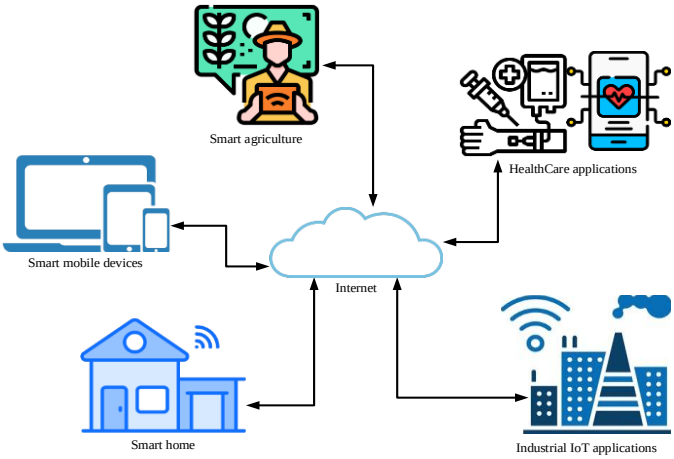

Fig. 1. Concept and applicability of IoT.

Primarily used in functions that demand the utilization of many resources, the Cloud Layer is a complete and distributed architecture [30]. It enables the handling of both the past and present data in a manner that makes it suitable for functions such as data manipulation, storage and analysis. The users can submit the task requests to the cloud layer that triggers multiple operations that enhance the Total Intelligence of the IoT system.

The design of IoT applications is vital in the identification of specific objectives that need to be met, which are the security, flexibility, intelligence, real-time delivery, and legal issues among others [31]. Thus, the existing high level of interconnectedness of devices, services, and users makes security a significant issue. Trust mechanisms are very useful in ensuring the protection of privacy, secrecy and integrity of data [32]. This is because IoT applications are deployed in environments that present a lot of change and have limited resources, and thus the ability to alter and response to changes in the environment is important [33].

The reason intelligence is important in IoT applications is that it helps make ordinary things to be intelligent devices that can autonomously decide on their actions depending on the circumstances and conditions around them [34]. Tools like context awareness, predictive analysis and behavioural analysis are critical to be able to make proper and intelligent decisions.

Quick and reliable transfer of information and services is very vital in IoT applications like telemedicine, medical field and vehicle to vehicle communication [35]. This is because IoT applications have the potential of capturing detailed personal information of people's daily lives and therefore, there must be regulation to protect against privacy infringement [36]. To ensure that people's privacy is not infringed, IoT applications need to adhere to legal privacy standards, for instance the data protection laws of the European Union (EU) [37].

B. *Commonly used Communication Technologies in IoT and Their Main Characteristics*

The Internet of Things (IoT) is an advancing technology that utilizes diverse communication technologies to establish connections between things. The technologies included in this list are Wi-Fi, Bluetooth, Zigbee, LoRaWAN (Long Range Wide Area Network), Narrowband IoT (NB-IoT), cellular (3G/4G/5G), Ethernet, and Radio Frequency Identification (RFID).

Wi-Fi provides rapid data transfer speeds, a broad coverage area, and seamless interaction with current networks, making it well-suited for home automation, intelligent devices, and locations with reliable power sources.

Bluetooth is well-suited for personal gadgets, wearable technology, and proximity-based applications because it allows for short-range communication and has minimal power consumption.

Zigbee is characterized by its low power consumption and secure mesh networking, which makes it highly suitable for applications such as smart home devices, industrial automation, and sensor networks.

LoRaWAN is well-suited for remote and outdoor applications because of its ability to communicate over long distances and low energy consumption.

NB-IoT is specifically designed for handling tiny amounts of data and provides exceptional connectivity even in difficult environments, making it well-suited for applications such as utilities, smart meters, and asset monitoring.

Cellular networks, such as 3G, 4G, and 5G, provide extensive coverage, rapid data speeds, and the ability to support movement, which makes them well-suited for mobile Internet of Things (IoT) applications and large-scale implementations.

Ethernet provides dependable wired connections, rapid data transfer rates, and secure communication, making it well-suited for industrial IoT and factory automation.

RFID utilizes electromagnetic fields to identify and monitor tags. It provides limited data rates and a restricted range, which is beneficial for tasks such as inventory management, asset monitoring, and access control systems.

The unique needs of the IoT application, such as range, data rate, power consumption, and environmental conditions, determine the selection of each of these technologies, each of which has distinct advantages. Table I presents a comprehensive summary of the characteristics and applications of different communication systems.

TABLE I. OVERVIEW OF FEATURES AND USE CASES OF THESE COMMUNICATION TECHNOLOGIES

Technology	Features	Use Cases
Wi-Fi	High data transfer rates, wide range, easy integration with existing networks	Home automation, smart appliances, environments with consistent power supply
Bluetooth	Short-range communication, low power consumption	Personal devices, wearable technology, proximity-based applications
Zigbee	Low power consumption, secure mesh networking	Smart home devices, industrial automation, sensor networks
LoRaWAN	Long-range communication, low power consumption	Remote and outdoor applications
NB-IoT	Optimized for small data volumes, excellent coverage in challenging locations	Utilities, smart meters, asset tracking
Cellular (3G/4G/5G)	Wide coverage, high data rates, support for mobility	Mobile IoT applications, large-scale deployments
Ethernet	Reliable wired connections, high data transfer speeds, secure communication	Industrial IoT, factory automation
RFID	Uses electromagnetic fields to identify and track tags, low data rates, short-range capabilities	Inventory management, asset tracking, access control systems

C. IoT in Industry

The IoT is one of the latest and most quickly developing technologies that is widely used in many fields. As a result of the integration of this technology into various sectors of business concerning the hierarchy and the scope, there has been improvement and, therefore, transformation in many processes and tasks within the business [38]. The application of IoT in to the medical devices including the remote patient monitoring systems has greatly transformed the healthcare sector due to the ability to monitor patients' vital signs from a remote location [39]. Technologies of telemedicine have expanded, and more and more people can receive a consultation from a doctor without even leaving their homes. Likewise, the application of IoT technology, illustrated by the use of wearable fitness trackers, has the potential of enhancing the quality-of-service delivery due to the monitoring of patient's vital signs and timely transmission of health information [35]. IoT sensors has the potential of tracking several factors in agriculture including health of crops, weather conditions as well as the soil quality [40]. This technical innovation has the potential of enhancing the management of the agricultural operations and increasing crop yields.

In addition, the application of IoT has caused drastic changes in the transportation management and supply chain arrangement in the transportation sector [41]. Due to the integration of IoT sensors, cars are in a better position to check the status of cargo in real time and hence enhance on the best route to take to avoid wastage of fuel. Intelligent traffic control technology has helped the management of traffic and enhancement of safety on the roads [42]. Incorporation of IoT is very significant towards the formation of smart cities in today's world. Certain works have been done and these include various solutions such as waste management systems and smart energy grids in enhancing power distribution efficiency [26], [41], [42]. Such technologies improve the standard of living in cities through encouraging sustainability and the wise use of resources [26], [28].

Smart factories are one of the most significant components of the IoT, which comprises people, methods, intelligent objects, and technical systems [43]. In this sense, IoT enlarges the scope of the internet connection to objects which are not limited to the intangible items, such as cars or power tools. Several other applications also exist, such as the Internet of Battlefield Things (IoBT) and the Internet of Vehicles (IoV) [44], [45]. Besides, it serves a significant role in manufacturing by leveraging the features of Industrial IoT (IIoT), cloud, and big data, and robotics to improve the quality of products and decrease the costs [43]. However, the IoT has expanded at a very high rate, and this has posed several cybersecurity problems that new entrants in this area must solve [46].

D. IoT in Saudi Arabia

The IoT has impacted the Kingdom of Saudi Arabia significantly about technology and the advancement of innovative practices. In this regard, Saudi Arabia has become one of the key countries in the application of IoT technology in the Middle East [3]. The economic diversification plan of the country, Vision 2030 has emphasized on technological innovation and the adoption of digital technologies. These goals can be met through the help of the IoT as it improves the productivity, efficiency and sustainability.

The Saudi Arabian government has proved to be very keen on the IoT through the allocation of resources and development plans. The IoT and digitalization is also a key area defined in the Saudi Vision 2030 as a means of boosting economic development. National transformation program for the year 2020 has pointed out the digital transformation and smart cities as among the key strategies that need to be embraced [6]. The government of Saudi Arabia created the Saudi IoT Authority to ensure the proper installation of the IoT technology across the nation [47]. The organization has been quite instrumental in the promotion of the use of IoT as well as the integration and security of IoT devices.

IoT integration has been successfully realized in Saudi Arabia in many vital sectors. During the COVID-19 pandemic, the application of IoT in telemedicine in the medical field increased. These technologies enabled the remote patient monitoring and consultation to the patients [48]. Precision farming in agriculture improves crop yields and reduces the wastage of water through the help of IoT sensors for soil and irrigation management [49]. The implementation of IoT in the predictive maintenance of industries minimizes the downtime and increases the productivity [50].

The sector of start-ups in the kingdom of Saudi Arabia has experienced rapid growth and success, as the entrepreneurs took the opportunities available to them to create new products and services in the market and challenge the large companies [16]. Thus, the integration of the IoT technology, as well as any other technology, offers many opportunities but at the same time, it brings new challenges and threats as the environment is constantly changing [8]. Several security concerns encompass:

1) Data privacy: This creates a problem of data privacy since IoT devices are always capturing and sending data. Security breaches or unauthorized access may result in the exposure of certain information that is confidential.

2) Device authentication: It is necessary to perform a device authentication process to ensure that only authorized devices are able to connect to the network. The threat actors can use poor authentication techniques and gain access into the IoT systems without the permission of the owners.

- Data Integrity: Data integrity is a very important aspect that deals with the accuracy and consistency of the data as it passes through the different devices. Data manipulation could result in the deployment of wrong information in the most sensitive processes of decision making.
- Network Security: IoT devices are connected over the wireless network and transmit data over a channel which is prone to threats such as eavesdropping if not properly protected.
- Software Vulnerabilities: There are many IoT devices that rely on embedded software, which can sometimes not be updated regularly and are therefore at risk for basic known flaws and for malware.
- Due to this, it is essential that these start-ups ensure that they protect the sensitive data, secure the connections and reduce the risks of cyber-attacks. These factors are critical for any long-term business success, and to sustain the confidence of the customers [9], [16]. Due to the complex nature of cybersecurity threats in the IoT, technologies such as blockchain technology is seen as a solution [36], [38]. The feature of decentralization and the immutability of its ledger technology is useful for the creation of trust, increased security and data integrity. By using the features that are inherent in blockchain, organizations can enhance the security of their IoT systems and be leaders in the development of secure and effective technical solutions [51].

Nonetheless, the works in [36], [38] show that because of the computational and storage nature of blockchain, it is not appropriate for the small and energy limited sensors in IoT. To implement blockchain in these scenarios, one can employ the following strategies:

- Lightweight Blockchain Protocols: Redesigning blockchain protocols that are computationally and storage intensive to work on IoT devices can be beneficial to the use of blockchain in IoT. These protocols are aimed at increasing the efficiency of the utilization of resources preserving their security and decentralization.
- Off-Chain Storage: Off-chain is a storage mechanism in which most of the data is stored off the blockchain with some data stored on the blockchain. This way, the data processing load on IoT devices can be effectively lowered. This technique relies on the use of the blockchain to guarantee the security and the integrity check with minimal use of the device's resources.
- Edge Computing Integration: Edge computing integration is the combination of blockchain technology with edge computing, which means data processing and blockchain activities are performed at the network's edge near the IoT devices. This way the workload of computing is divided among several more capable fog devices and the latency is also reduced and the load on each sensor is minimised.

3) Consensus mechanisms: To make the blockchain operations more suitable for the IoT applications one can use consensus mechanisms that do not demand more computational power for instance the Proof of Authority or the Delegated Proof of Stake. All of these are more efficient when it comes to the utilization of resources than the conventional proof of work (PoW).

These strategies assist in the integration of Blockchain technology into IoT, primarily those that have many small and energy-efficient sensors; thus, improving the security and dependability of the system without impacting the functioning of the devices [51].

III. Existing Research

The current body of study in the field of startups, namely those using the Internet of Things, is extensive and diverse [52], [53]. This section examines the significant influence of startups on economic development and innovation, as well as the intricate relationship between technical breakthroughs and entrepreneurial success. In this context, the following sections provide a systematic analysis of the critical areas of focus that influence the ecosystem of startups using IoT technology. The areas covered in this study encompass a comprehensive analysis of global startup ecosystems from a worldwide perspective. It identifies the various security risks that are linked with the use of IoT applications. It also examines the factors that affect the implementations and adaptations of IoT technologies in start-up firms. Also, it explores the strategic moves that Saudi Arabia has put in place to foster an environment that supports IoT startups. Finally, it assesses the current standards and frameworks put in place to protect the IoT security. All these components play a vital role in understanding the current state of knowledge and identifying the directions for the future studies.

A. Global Perspective on Startup Ecosystems

Worldwide, governments and politicians acknowledge the importance of entrepreneurs in advancing economic development. The Government of Canada recognizes entrepreneurs as a vital and dynamic force necessary for the country's growth [54], [55]. In a similar vein, the United Kingdom has seen a substantial increase in entrepreneurial activity, establishing itself as the foremost investment hub in Europe [56], [57]. The entrepreneurial sector in the United States significantly contributes to the nation's economic success, making it the biggest economy in the world [58], [59]. Developed countries emphasize creating a secure environment against cyber threats to support the development of startups and

entrepreneurship, highlighting the significance of cybersecurity in today's digital world [60].

B. Security Concerns in IoT-Enabled Startups

Startups that implement IoT technology are at a high risk of cybersecurity threats since the effects of a cyber-attack are usually negative [19]. Security breaches, besides affecting the confidence of the customers and the image of the company, causes significant financial losses [18]. Due to the rise of IoT devices, they have become vulnerable to cyber threats and hence becomes a target of cyber criminals. This means that robust strategies have to be put in place to ensure that key data is secure while at the same time ensuring that the operations remain credible [61].

Here are some security threats that are particular to the startups that incorporate IoT solutions into their business.

- Device Vulnerabilities: Most of the IoT devices are characterized by limited computational power and memory, and thus have inadequate security features. This makes them prone to several attacks such as firmware attacks, unauthorized access, and malware infection.
- Insecure Communication Protocols: IoT devices are connected wirelessly and many of them use protocols with inherent weaknesses in terms of security. An attacker can employ encryption technologies that are either not strong or outdated to intercept and alter data in the course of transmission.
- Default and Weak Credentials: Many a times, users fail to change the default username and passwords on many IoT devices. These credentials are default and can be easily used by the attackers in order to gain access to the devices.
- Data Privacy: IoT devices generate and transmit information that is sensitive, for example, user's data and their behavior. Lack of proper encryption and access control makes it very easy for the hackers to intercept and misuse the information.
- Security Solutions Scalability: The major challenge for the startups is the scalability of their security solutions. Since there are more devices that are connected in the IoT, it becomes a difficult process to manage and regulate on the security aspect of each device.
- Patch Management: IoT devices should be updated from time to time with the current security patches. However, most of the devices do not have a clear way of updating, and this exposes them to common threats.

The continuous study is significant in overcoming the cyber security problems that are related to the utilization of IoT in startups. There are several flaws in IoT devices identified by the researchers and the consequences that may arise from the security threats are loss of data and damage to one's reputation [62], [63]. Moreover, a large number of empirical studies have examined the factors that influence the uptake of IoT in various industries and countries, thus helping to understand the drivers and challenges of organizations [43].

We need a comprehensive strategy to address these problems. This strategy should include the adoption of more robust authentication mechanisms, the establishment of secure communication channels, the frequent upgrading of device firmware, and the education of users on the significance of changing default credentials. In addition, entrepreneurs should contemplate using sophisticated security frameworks, such as blockchain technology, to augment the overall security of their Internet of Things (IoT) ecosystems. By prioritizing these specific concerns, companies can improve the security of their IoT implementations and reduce the potential dangers of security breaches.

In addition, cybersecurity is mainly concerned with protecting the network, systems, and data against threats such as DDoS attacks, malware attacks, and social engineering; however, the insecurity of the physical aspect of IoT devices is equally important. Some of the Physical security measures that can be employed are; implementing tamper proof hardware. In the same way, gadgets that can be easily tampered with as they are not openly changeable, present a significant threat to security. Therefore, IoT-based organizations need to establish a full-fledged security plan that incorporates cybersecurity alongside physical protection of devices for the entire IoT environment.

C. Factor Influencing IoT-enabled Startup Ecosystem

The success of companies that use IoT technology depends on effectively resolving critical elements in technical, political, social, and economic aspects [64], [65]. From a technological standpoint, having access to a robust telecommunications infrastructure and reasonable bandwidth is important for the smooth implementation of the IoT [8]. From a political standpoint, it is essential for the government to provide support for technical development and innovation in order to create a favorable environment for startups [18]. Societal factors, like the speed at which people use the Internet and their level of acceptance of technology, significantly influence the adoption and spread of IoT solutions [66]. In terms of economics, variables like average income levels, accessibility to technology, and general economic development influence the feasibility and scalability of IoT-enabled companies [67].

D. Saudi Arabia's Endeavor in Fostering IoT-Enabled Startup Ecosystem

Saudi Arabia has a strong desire to foster the IoT-enabled startup ecosystem, as seen by its significant investments and strategic efforts. To meet this expectation of internet usage standing at over 95% in the year 2025, much resources have been allocated to programs such as the e-Government and the Saudi Vision 2030 that seeks to foster business and invest in new business ventures [4], [6]. Saudi Arabia aims to establish itself as the center of entrepreneurship in the region by making strategic investments and providing assistance in several sectors, albeit starting later than other countries [14].

Nevertheless, despite its high readiness score, which exceeds that of many other countries, Saudi Arabia has had difficulty fully utilizing the potential of startups provided by the Internet of Things (IoT). Studies that are directed towards the computer security issues of startups that are employing IoT is rather limited. This is the reason why it is critical to pay

attention and act in this area [4], [9]. Nevertheless, the review of literature on cybersecurity and technology use in the area reveals other important findings in the present study thus underlining the importance of the topic in Saudi Arabia today [4], [8].

E. Standards and Frameworks for IoT Security

Several works have been done by international organizations and standards groups regarding the security standards and frameworks of IoT [68], [69]. These standards are important due to the need to have a uniformity, compatibility and safety of the IoT systems [70]. The International Telecommunication Union (ITU) [71], the International Organization for Standardization (ISO) [72], the International Electrotechnical Commission (IEC) [73], and the Institute of Electrical and Electronics Engineers (IEEE) [74] set significant standards. Organizations such as National Institute of Standards and Technology (NIST), the IoT Security Foundation, and European Union Agency for Cybersecurity (ENISA) have issued recommendations and best practices for protecting IoT systems [46], [75], [76].

These organizations have published several vital IoT standards such as

- ITU is an organization that deals with the regulation of telecommunication standards.
    - ITU-T Y.2060 is one of its standards that provides detail on the structure of IoT and the key enablers for IoT.
    - The ITU-T Y. 4000-Y.4999 series encompasses a number of recommendations that are associated with the design, requirements, and challenges of the IoT.
- ISO has prescribed ISO/IEC 27030 and ISO/IEC 30141 which are associated with security strategies for IoT.
    - The ISO/IEC 27030 standard defines guidelines for Information Security Risk Management in IoT systems.
    - The ISO/IEC 30141 is a standard that defines the architecture of IoT to ensure that the different IoT systems are compatible and also secure.
- The IEC is an organization that deals with the standardization of many industries.
    - Among the standards developed by the IEC, one of the most important is the IEC 62443 standard that is mainly oriented towards industrial automation systems and can be applicable to the IoT systems as well. It contains guidelines on the security of network and systems.
- IEEE has also come up with standards that include IEEE 2413 and IEEE P1451 regarding the security of IoT.
    - The IEEE 2413 standard defines the IoT. This framework is based on the concepts such as interoperability, security, and privacy concerns.
    - The IEEE P1451 standard is mainly devoted to the smart transducer interfaces and these are vital for the IoT. This standard focuses on the aspects of interoperability and security.
- The NIST has produced a document called NIST Special Publication 800-183.
    - This publication provides a comprehensive and extensive overview of security in the IoT. It encompasses various aspects of security including device security, data security and network security.
    - The NIST Cybersecurity Framework is not aimed at IoT but it provides a robust model for managing and, therefore, minimizing cybersecurity risks in IoT environments.
- The IoT security foundation can thus be viewed as a reference for the implementation of security in IoT devices and services right from the development of the concepts to the final product.
- ENISA gives an insight of the guidelines and recommendations that are required in the IoT security compliance.
    - The Baseline Security Recommendations for IoT are quite specific and focus on preserving data, device, and network security for IoT devices.
    - The ENISA Good Practices for IoT and Smart Infrastructures are guidelines that offer real-life recommendations on how to secure IoT deployments and minimize the associated threats.
- Thus, by adhering to these guidelines and models, organizations can ensure that their IoT systems are secure, interoperable, and reliable, which in turn enhances the confidence and reliability in any IoT solution offered.

In conclusion, the previous study finds important findings regarding the security issues and challenges related to the IoT applications in Saudi Arabian startups. Thus, organizations can implement effective security measures and guidelines to minimize the risks and ensure the data security and privacy of IoT devices by referring to the standard and frameworks developed by international organizations and standards development organizations [69]. Although there is already research available, there is still a lack of information about the distinct computer security concerns that entrepreneurs in Saudi Arabia have when implementing IoT solutions. It is critical to address this deficiency in order to provide a safe and prosperous environment for IoT-enabled companies throughout the country [16]. Table II presents a thorough summary of the current study and offers valuable insights derived from the difficulties, characteristics, and suggestions.

TABLE II. COMPREHENSIVE OVERVIEW OF THE EXISTING RESEARCH

Section	Summary	Challenges	Attributes	Recommendations
Global Perspective on Startup Ecosystems	Developed nations prioritize fostering a cyber-threat-free environment to enable startup growth and entrepreneurship [54], [55], [56], [57], [58], [59].	Regulatory barriers Cybersecurity concerns Interoperability issues	Government support Access to capital Technological infrastructure	Establish clear regulatory frameworks Enhance cybersecurity education and awareness Foster collaboration between government and industry
Security Concerns in IoT-enabled Startups	Security breaches undermine consumer trust and lead to significant financial losses; robust security measures are necessary [18], [62], [63].	Data breaches Compromised IoT devices	Encryption techniques Authentication protocols Intrusion detection systems	Implement end-to-end encryption Regularly update firmware and software Conduct security audits and penetration testing
Factors Influencing IoT-enabled Startup Ecosystem	Success factors include technological infrastructure, government support, societal acceptance, and economic conditions [18], [52], [66], [67].	Technological limitations Limited government support Societal resistance to technology Economic instability	Telecommunication infrastructure Government initiatives Societal attitudes towards technology Economic growth	Invest in expanding technological infrastructure Provide incentives for startups Promote digital literacy programs Foster economic diversification and stability
Saudi Arabia's Endeavor in Fostering IoT-enabled Startup Ecosystem	Saudi Arabia invests in initiatives like the e-Government program and Saudi Vision 2030 to foster entrepreneurship [3], [4], [6], [13], [14].	Limited access to funding Infrastructure gaps Bureaucratic issues	Government investments Strategic initiatives Vision 2030 initiatives	Establish dedicated funding programs for startups Improve infrastructure development Streamline regulatory processes and reduce bureaucratic red tape
Standards and Frameworks for IoT Security	International organizations and standards bodies have developed standards and frameworks to ensure IoT system security [46], [71], [72], [73], [74], [75], [76], [77].	Lack of standardized regulations Complexity of compliance	ITU standards ISO/IEC standards IEEE standards	Implement standardized security protocols and guidelines Simplify compliance procedures and provide support for implementation Encourage participation in certification programs and compliance frameworks

IV. IOT-DRIVEN COMPUTING CHALLENGES IN SAUDI ARABIAN START-UPS

This section explores the computational challenges faced by startups in Saudi Arabia, namely those that hinder their ability to expand and innovate. Fig. 2 shows that most of the computing problems IoT-driven startups in Saudi Arabia face are caused by four main things: worries about cybersecurity [4], [9], a lack of skilled IT professionals [9], [16], problems with infrastructure [8], [16], and issues with following rules and regulations [3], [15].

Among all the problems, cybersecurity is the most significant and pressing issue because it has an immediate impact on the operations and sustainability of organizations that use IoT devices. Due to the fact that these organizations are in the digital environment, they are very vulnerable to cyber risks, which may affect the important information, services, and, consequently, consumer trust. This issue shows that there is a necessity of proper cybersecurity measures which might be difficult for startups since they have a small budget.

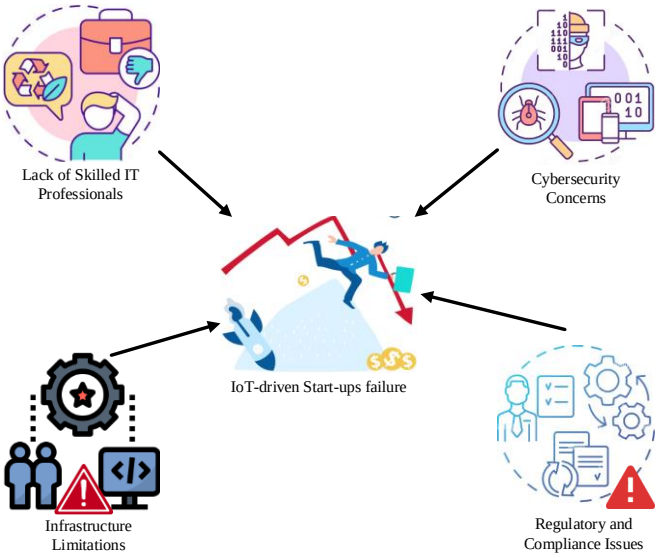

Fig. 2. Computing challenges in Saudi Arabian IoT-driven start-ups.

A. Cybersecurity Concerns

Startups in the Saudi Arabia are becoming more technology-oriented and apply digital technologies in their business processes which makes cybersecurity an important factor for them [4]. In view of the above, it is important that the valuable information and systems are protected as more cyber threats and attacks are being reported in the context of IoT-based startup companies [9].

However, some of the Internet of Things (IoT) start-ups might lack the necessary funds and personnel to develop robust cybersecurity mechanisms [12]. Lack of funding and lack of skilled personnel in the IT department are other drawbacks in their IT systems [4], [16]. Moreover, the identified danger of the dynamic nature of cyber threats is a continuous challenge that requires the permanent monitoring and tuning of the security measures [8].

This makes it essential for IoT based start-ups to prioritize the spending on cybersecurity technologies and protocols in order to address cybersecurity issues. In collaboration with cybersecurity professionals and employing cloud-based security measures, organizations can enhance their defenses against cyber threats [4], [8]. Also, organizations can minimize risks by raising awareness on the importance of cybersecurity and conducting comprehensive trainings [4], [9]. This section discusses some of the most significant and diverse cybersecurity threats that are directed towards IoT applications.

1) Security threats to IoT applications: Due to the increased integration of IoT devices, along with the big data they generate, the IoT faces a high level of security threats [76]. IoT devices often lack basic security features like secure boot and encryption and are vulnerable to exploitation through default configurations, weak passwords, and unencrypted communication channels [68]. These risks can lead to unauthorized access, data manipulation, or device compromise, which can be risky to privacy and organizational credibility. Thus, high-profile attacks like the Mirai botnet attack and the Stuxnet worm emphasize the importance of security in IoT systems [78], [79].

Fig. 3. Different security threats to IoT applications.

The IoT ecosystem consists of four layers: They are sensors and actuators, communication networks, middleware, and end-to-end applications. Each layer has its own security challenges and gateways help in transferring data from one layer to another. The existence of the weaknesses at these levels makes it vulnerable to attacks and, therefore, a need to understand the security situation [63]. Fig. 3 highlights these vulnerabilities and underscores the importance of preventive security measures in securing IoT applications from potential attackers.

a) Security Concerns about the Sensors and Actuators (Sensory) Layer

Threats to the sensory layer, which consists of physical sensors and actuators, include node capture, side-channel attacks, and malicious code injections [63].

- Node capture: Attackers replace low-power nodes with malicious ones. Solution: Employing physical security measures to safeguard nodes and utilizing tamper-resistant hardware will effectively deter node capture.
- Malicious Code Injections: Affect the potential of nodes. Solution: Secure boot and coded signing prevent the usage of unauthorized software on the devices.
- Side-Channel Attacks: In this case, the program utilizes CPU microarchitectures to gain data without permission. Solution: It is possible to decrease the effect of these attacks by employing hardware encryption and shielding measures.
- Eavesdropping and Interference: Target IoT systems in public areas. Solution: Employing encrypted communication channels and frequency-hopping methods may effectively safeguard against eavesdropping and interference.
- Sleep Deprivation and Booting Attacks: Cause devices to become inoperable or compromised. Solution: Deploying robust firmware update mechanisms and using advanced anomaly detection systems may effectively detect and mitigate these types of attacks [2], [21], [23].

b) Security Concerns about the Communication Network (Network) Layer

The network layer, which is responsible for delivering data, gets vulnerable to the phishing scams, unauthorized access, and denial of services (DoS) [63].

Phishing: mainly focuses on the IoT devices with the aim of collecting the login details. Resolution: It is possible to eliminate this risk by implementing and using multi-factor authentication (MFA) and training the users to recognize phishing schemes.

- Access attacks: Their role is to infiltrate the networks and to obtain information from there. Solution: It is also recommended to prevent illegal access through improving the establishment of robust network access control (NAC) and implementing intrusion detection systems (IDS).
- DDoS attacks: These are such as flooding the servers; an act that ends up disrupting the provision of relevant services. Solution: The attacks can be prevented by

using rate restriction, traffic analysis and services that prevent Distributed Denial of Service.

- Data transit and routing attacks: Their objective is to challenge the authenticity of data and juncture involved. Solution: On data transmission, it is possible to ensure data security and prevent the information from being intercepted in the process by employing secure and well encrypted end to end and safe routing pathways.

c) Security Concerns about the Middleware Layer

The extra layer called the middleware is also a weak link due to the risk of man-in-the middle attack, SQL injection and cloud malware injection [63].

- Man-in-the-Middle Attacks: These are such as controlling the protocol like the MQTT through which unlawful communication is made. Solution: Mutual authentication along with TLS (Transport Layer Security) could possibly help prevent such attacks.
- SQL injection: Combined with the factors above, it complicates and compromises the integrity of data. Resolution: Using parameterized queries or using input validation, one can meet the needs to counter SQL injection.
- Cloud Malware Injection and Flooding Attacks: They are designed for cloud infrastructure. Solution: To counter such threats, it is recommended to work with cloud safeguards that cover API protection, the assessment of critical weaknesses more often, and implementation of cloud-native security solutions.

d) Security Concerns about the End-To-End Application (Application) Layer

The application layer, which is directly related to the end-users, is concerned with problems like data theft, access control, and service interruption attacks [63].

- Malicious code injection and sniffer attacks can further lead to threats to the system integrity. Resolution: Implementing application firewalls; code reviews on a regular basis; having secure coding practices may minimize these risks.
- Reprogramming attacks: These have the propensity of causing hijacking of the network. Using such measures as implementing secure firmware upgrade and code signing will help to ensure that only trustworthy code is run on the devices.

e) Security Concerns about Gateways

While gateways are necessary to interconnect IoT devices, these devices are still susceptible to eavesdropping as well as man-in-the-middle attack during GW on-boarding [43], [61].

- Man-in-the-Middle Attacks: Solution: To eliminate the possibility of a third-party intercepting said information, a means of mutual authentication, as well as encrypted pathways of communication needs to be established.
- Eavesdropping resolution: It can be prevented by ensuring that the onboarding procedure that is invoked during the entire process is safe from the people who would want to snoop on the data transfer process and by making sure that the information exchanged has the highest level of encryption possible.
- Updating firmware must be done securely. Solution: We can therefore exclude the so-called unwanted access into the firmware by embracing reliable update procedures and ensuring the firmware is validated prior to use.

f) 4.1.1.6 Other Security Concerns

IoT devices provide issues like insufficient authentication, encryption mechanisms, and physical security measures [80], [81]. Implementing standardized protocols, regularly updating software, and having solid APIs are essential for reducing these risks. It is essential to address privacy concerns, supply chain vulnerabilities, and legacy system integration challenges in order to provide complete security for the Internet of Things (IoT) [78].

To address these difficulties, researchers propose using robust authentication, encryption, regular firmware upgrades, security audits, and industry-wide standards to minimize the security risks associated with IoT [44], [48], [49]. Implementing such solutions is crucial for protecting IoT applications and guaranteeing their ability to withstand emerging threats.

1) IoT Users' Privacy Concerns, Scalability and Interoperability

Currently, the risk of privacy compromise has been deemed very high, especially in areas such as the smart home since there is a growing prevalence of networked IoTs. This is the case because tracking user activity in such contexts could inadvertently disclose private data [82]. With IoT data storing parameters for individual customers the opportunity to use this chance to develop new products and individualized advertising has emerged the issues with data utilization and breaches that may lead to issues like identity theft. Various governments including the Saudi Arabia are trying to mitigate the challenges that relate to data governance and protection of data through organizations like the Saudi Data and Artificial Intelligence Authority (SDAIA) [83]. Thus, compliance with the rules of the protection of personal data prescribed by the international legal acts, including the General Data Protection Regulation created by the European Union [82], proves commitment to ethic data usage in IoT environments.

In the same way, more and different IoT devices increase the management and scalability challenges [62]. This means that there is a need to fit in large volumes of data, which exerts storage and network resources pressures so that interoperability enhances efficient data exchange across platforms and devices. Integration is key in the formation of composite services most importantly in smart city initiatives whereby the collaboration of IoT devices enhance distribution of resources and management of the civil structures [84].

In response to concerns about scalability and interoperability, IoT platforms and middleware have become popular solutions. These solutions include various features, such as device management, data integration, and application development [68]. These technical interventions reduce

fragmentation and inefficiencies while maximizing the advantages of IoT technology. In order to guarantee the ongoing development and effectiveness of IoT ecosystems, it is important to prioritize privacy protections, scalability, and interoperability, as shown in Fig. 4.

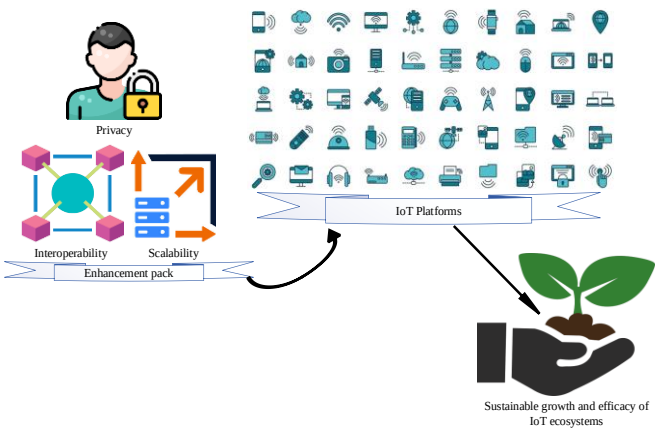

Fig. 4. Ensuring a sustainable growth and efficacy in IoT ecosystems.

B. Other Computing Challenges in Saudi Arabian Start-ups

This section examines the computational difficulties encountered by start-ups in Saudi Arabia, emphasizing significant barriers impeding their expansion and ingenuity.

1) Lack of skilled IT professionals: A significant challenge that start-ups in Saudi Arabia encounter is the limited availability of highly trained IT experts [9], [16]. Although there is a growing need for skilled professionals in fields like software development, data analytics, and cybersecurity, there is still a lack of competent workers to meet this need [4]. The country's education system may not adequately equip students with the skills and knowledge required for employment in IT-related industries, resulting in a limited supply of local talent for start-ups to hire. Additionally, the favoritism towards engineering and business degrees in comparison to IT fields worsens this shortage [10].

In order to tackle this difficulty, it is necessary to implement efforts that aim to enhance IT education and training programs at academic institutions and vocational training centers [9], [16]. Due to the lack of adequate number of skilled IT staffs, students should be encouraged to pursue IT degrees and professionals should be motivated to enhance their skills in the development of technologies.

2) Infrastructure limitations: Infrastructure restraints currently present a significant barrier to start-up firms in Saudi Arabia [16]. Although there have been improvements in the development of digital infrastructure, there are still gaps that remain, particularly in rural and disadvantaged regions [12]. Limited availability of dependable internet connections and power interruptions may disrupt corporate operations and hinder the use of digital technology. Also, the expense associated with building and sustaining infrastructure may be a hindrance for new businesses, particularly those with low financial means [8].

In order to overcome the limits of infrastructure, start-ups have the option to consider other solutions, such as using shared infrastructure services and forming partnerships with existing technology providers [13], [85]. It will prove useful to explore more efficient methods of obtaining the required IT solutions, such as cloud solutions and software-as-a-service (SaaS). Moreover, contributing to the government initiatives that aim at the improvement of the digital connectivity and the increase of the internet accessibility can also contribute to the formation of the more suitable environment for the start-ups [10].

3) Regulatory and compliance issues: Besides those common challenges, start-ups in Saudi Arabia face another challenge that is the tough regulatory and compliance requirements [3], [15]. With many start-ups emerging and constantly advancing technologies, legislation and law practices may be intricate with constantly varying differentiations and yet posing challenges of ensuring technology and data compliance. Thus, data privacy, intellectual property rights and some industry-specific rules add up to the complexity of the operational environment [16]. Also, there may be challenges incurred by start-ups due to bureaucratic procedures and legal issues which may hinder market entry and growth [14].

In considering how to overcome barriers and challenges to new start-ups, it will be necessary for start-ups to adopt regulatory compliance as a critical consideration and to formally include compliance as part of the business strategy. It may be helpful to involve a legal counsel and to follow the changes in legal regulation in order to minimize the risks and adhere to the laws. Moreover, backing regulatory adjustments, and also participating in the process of assisting governmental bodies in making procedures less burdensome can potentially contribute to improvement of the environment for start-ups [13].

In conclusion, the major challenges that start-ups in Saudi Arabia experience following computational issues includes: The absence of skilled IT personnel, limited infrastructure, and legal and regulatory issues. To tackle these difficulties, it is necessary for stakeholders from government, business, and academia to work together and create an environment that promotes innovation and growth [7], [10]. By surmounting these obstacles, start-ups may unleash their full capabilities and make a significant contribution to the country's economic diversification and digital transformation.

V. The Role of Vision 2030 in Promoting IoT

This section analyses how Vision 2030 has helped in the incorporation of IoT to Saudi Arabia's dream of a smarter future and diversification of economy. Vision 2030 was formulated by the Saudi Arabian government as a major social program aimed at diversifying its economy and developing it in various spheres [6]. The main goals of the organization are to improve the business climate, attract foreign investment, and foster innovation and entrepreneurship [6].

Saudi Arabia views the integration of IoT technology into Vision 2030 efforts as a crucial method for driving digital transformation, enhancing productivity, and fostering

innovation [3]. The main goals of Vision 2030 are shown in Fig. 5. They include building smart cities, speeding up the digital transformation of society, businesses, and government, supporting innovation, encouraging industrialization, and giving digital health top priority [86], [87]. These projects use IoT technology, including sensors, actuators, and networked devices, to enable the digitalization of processes, the gathering of data, and the optimization of operations [83].

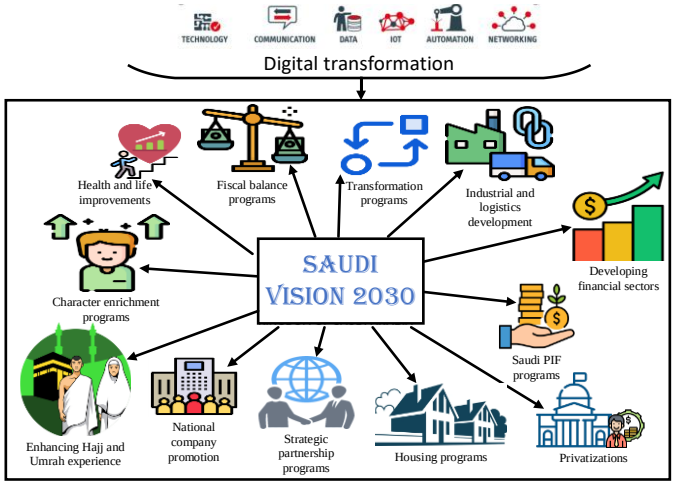

Fig. 5. Achieving Saudi Vision 2030 via digital transformation.

Furthermore, the government plays a significant role in assisting secure IoT-driven start-ups via many channels. Such resources consist of financial assistance, grants, access to spaces that incubate entrepreneurial ventures, accelerated programs for business, and hubs for innovation. The Badir Program for Technology Incubators and the KAUST Entrepreneurship Centre offer crucial support in the form of guidance, development, and connection-making to start-ups [7], [10], [54], [83]. Moreover, regulation authorities ease bureaucratic processes and establish conducive conditions for safe IoT-led start-ups through setting up of regulatory sandboxes and innovation zones.

The government also makes provisions for expending funds on skills development programs to improve the competencies of businesspersons and other professionals operating in the IoT value chain. The National Industrial Development and Logistics Program (NIDLP) provides necessary skills development, training sessions, and capacity enhancement interventions [88]. The government develops a pool of human capital to have skilled IoT personnel who can promote innovative development [54].

Saudi Arabia is moving towards promoting its Vision 2030 framework of bringing innovation and sustainable growth in business through supporting its programs in IoT technology and helping in the financial assistance in IoT based start-ups. It is therefore possible for Saudi Arabia to position itself as one of the foremost global leaders in IoT enablement and innovation through its smart investments, strategic changes in policies, and the promotion of partnership.

Furthermore, Table III shows the comparison of proposed and existing research on IoT security in Saudi Arabia Start-ups.

TABLE III. COMPARISON BETWEEN PROPOSED RESEARCH AND EXISTING STUDIES ON IOT SECURITY IN SAUDI ARABIAN START-UPS

Aspect	Proposed Research	Existing Studies
Target	Examines IoT security challenges specifically in Saudi Arabian start-ups.	Various studies cover IoT security across different sectors globally but may not focus specifically on Saudi start-ups [18], [62], [63].
Objectives	Identify cybersecurity risks, analyze the impact of IoT networking on privacy/security, and propose mitigation strategies.	Existing research often identifies security risks, however, lack comprehensive frameworks for specific contexts like Saudi Arabia [3], [4], [6], [13], [14].
Methods	Review of diverse publications and analysis of cybersecurity issues in the context of Saudi Vision 2030.	Many studies utilize case studies or empirical data, potentially overlooking broader contextual analyses like national strategies [54], [55], [56], [57], [58], [59].
Importance Findings	Highlights distinct cybersecurity obstacles faced by IoT-enabled businesses in Saudi Arabia; calls for funding, collaboration, and education.	Most of studies mention general IoT security challenges but may not address specific funding or educational needs in emerging markets [46], [71], [72], [73].
Contextual Relevance	Positions research within Saudi Arabia's economic goals and Vision 2030.	Various existing studies focus on developed countries or global trends without considering local economic and cultural factors [74], [75], [76], [77].
Recommendations	Advocates for a cooperative strategy involving policymakers, industry stakeholders, and entrepreneurs to enhance IoT security.	Many studies recommend technical solutions or policy frameworks; however, they did not emphasize collaboration with local stakeholders [13], [14].
Contributions to the Field of Research	Provides novel insights and a framework tailored to the unique challenges of Saudi Arabian start-ups in IoT.	Most of existing research do not focus on the unique socio-economic landscape of Saudi Arabia, limiting their applicability [46], [71], [72], [73].

VI. Discussion on Future Direction and Recommendations

This section provides a discussion on the paths that are to follow and gives recommendations on ways through which the Saudi Arabian government can foster the evolution of safer IoT devices led start-ups and promote creativity. These attempt to offer a strategic approach; however, it is high time to consider them in relation to the existing socio-economic conditions in Saudi Arabia and the peculiarities of the mentioned cybersecurity challenges.

1) Establish innovation networks: Creating innovation networks may help stakeholders share resources, skills, and best practices, leading to increased creativity and the ability to overcome difficulties [88]. These networks should highlight cybersecurity best practices to ensure that IoT start-ups place a high value on security right from the beginning.

2) Encourage open innovation: The open models help start-ups access resource, technologies and market opportunities and in turn existing enterprises can avail benefits of external innovation and entrepreneurial skills [89]. Some measures to empower open innovation may involve establishing safe IoT spaces and information sharing systems that enhance the knowledge of potential cybersecurity threats and the ways to combat them.

3) Support technology transfer: The government should endorse technology transfer efforts and collaborations to expedite the commercialization of research and innovation [54]. It is important to focus on sharing information and technologies that improve the security of the Internet of Things (IoT) such as blockchain technology. This will assist in avoiding new innovations from negating the authenticity of the data or the confidentiality of the user.

Cultivate a Culture of Innovation and Entrepreneurship: The implementation of the culture of innovation and entrepreneurship plays a key role in establishing secured IoT based Start-ups and Innovations in Saudi Arabia [85]. The following are the primary recommendations:

- Promoting a new organizational culture where people would embrace the principles of entrepreneurship in tackling cybersecurity issues.
- Supporting and encouraging start-up incubation and acceleration initiatives that focus on enhancing safe IoT innovation.
- Celebrating achievements in entrepreneurship, including specific accomplishments that can potentially convey success in protecting IoT applications.
- State-sponsored honors, competitions, and meetings can inform about successes of prospering start-ups and businesses to inspire a new generation of innovators and actors of change [18].

4) Leverage international partnerships: Consequently, it's wiser for Saudi Arabian IoT-drive start-ups to capitalize on foreign partnerships since this will afford them the international markets and foreign experience along with the advanced technologies that are vital for their growth [13]. Some recommendations are as follows:

- Remain committed to the search for international cooperation and funding sources to strengthen protection of IoT networks with the participation of specialized organizations.
- Works with other universities and industries that have well-strategized cybersecurity system mechanisms across the globe for technology update and knowledge sharing.
- Providing help in the access to international markets, distribution channels, and business networks while meeting international cybersecurity standards for start-up companies.

5) Specific socio-economic considerations: To make these suggestions realistic and effective in the Saudi context, the following should be considered given the country's socio-economic values:

- Economic Diversification: ensuring that the development of IoT start-ups in Saudi Arabia aligns with the aims of economic diversification outlined in Vision 2030, with a specific emphasis on supporting non-oil industries.
- Education and Training: More resources need to be directed to education and training that can help in improving cybersecurity and create workforce that can handle IoT security threats.
- Regulatory Environment: Creation and enforcement of laws that foster IoT security, thus ensuring that the start-ups follow the regional and international standards of cybersecurity.

Thus, Saudi Arabia can contribute to the development of an active environment in the IoT industry by considering socio-economic factors and specific cybersecurity challenges, as well as cooperation, innovation, and entrepreneurship [10]. This strategy will ensure that the economy grows and becomes prosperous as required by Vision 2030 while at the same time ensuring that the security of IoT systems is not compromised in any way.

VII. Conclusion

This paper has reviewed the literature on the adoption of IoT technology in start-up companies in Saudi Arabia with a focus on the cybersecurity challenges. The research highlights the critical cybersecurity risks associated with IoT adoption in Saudi Arabian startups, particularly in the context of data privacy and network security vulnerabilities. The study emphasizes the necessity for startups to implement advanced security measures despite limited resources and proposes strategic solutions, such as cloud-based security, collaboration with cybersecurity experts, and enhanced cybersecurity education. This research fills a notable gap by addressing the unique cybersecurity needs of startups in emerging markets, advancing the understanding of IoT security in the

entrepreneurial landscape. Moreover, the government is to seek solutions to social issues and promoting corporate growth through IoT investment, these start-ups face significant cybersecurity challenges. This is due to the fact that the threats are constantly evolving, and the resources available in such efforts are scarce.

For this reason, start-ups need to allocate their resources to cybersecurity technology and procedures to address these issues. Another way of improving the organizations' cybersecurity is through engaging the services of cybersecurity professionals, and the use of cloud technologies. In the same manner increasing the awareness of the public regarding the proper measures to take to improve cybersecurity and increasing the frequency of educational campaigns is also an effective way in increasing the level of cybersecurity preparedness.

Therefore, there is the need to do more work and engage in more research to discover new strategies in the protection of IoT in Saudi Arabian start-ups. It is important to address the cybersecurity issues to harness the full potential of IoT, boost the economy, foster innovation, and position Saudi Arabia as a leader in the IoT technology sector.

The IoT industry decision makers, stakeholders and investors in Saudi Arabia should ensure that proper cyber security measures are put in place and resources to be directed towards development of secured IoT ecosystem. Saudi Arabian start-ups could navigate their way through the cybersecurity environment and succeed in the era of digital and interconnected world by collaborating and investing more.

Future Research and Implementation:

- Lightweight Blockchain Protocols and Edge Computing Solutions: It is recommended that further studies focus on the enhancement of blockchain protocol that has low power consumption and is suitable for the IoT devices' edge computing.
- Standardized Cybersecurity Frameworks: From the findings of the present study, it can be suggested that there is a need for the formulation of suitable cybersecurity models that can be applied to the context of the startups and at the same time ensure that all the IoT systems are compliant.
- Synergy among academia, industry, and government: This implies that new challenges must be taken and safer IoT technologies and environments have to be created.
- Educational Initiatives: Awareness and education of entrepreneurs and IT specialists in the context of the creation of secure IoT systems can be considered as one of the most significant activities directed towards the development of the IoT security sphere.

Implementing these measures can help Saudi Arabia create a competitive environment in the IoT industry and promote cooperation, innovation, and business growth. This strategy will foster economic growth and prosperity in line with Vision 2030 while at the same time focusing on the security of IoT devices. Through close cooperation with all stakeholders, the country can become a global leader in safe and innovative IoT solutions.

ACKNOWLEDGMENT

The research presented in this paper is funded by the Saudi Arabian Cultural Bureau (SACB) through a PhD studentship at the University of Sussex.

REFERENCES

[1] A. Sallam, F. Al Qahtani, and A. S. A. Gaid, "Blockchain in Internet of Things: A Systematic Literature Review," in 2021 International Conference of Technology, Science and Administration, ICTSA 2021, 2021. doi: 10.1109/ICTSA52017.2021.9406545.

[2] M. A. Obaidat, S. Obeidat, J. Holst, A. Al Hayajneh, and J. Brown, "A comprehensive and systematic survey on the internet of things: Security and privacy challenges, security frameworks, enabling technologies, threats, vulnerabilities and countermeasures," Computers, 2020, doi: 10.3390/computers9020044.

[3] M. N. Al Otaibi, "Internet of Things (IoT) Saudi Arabia Healthcare Systems: State-Of-The-Art, Future Opportunities and Open Challenges," J Health Inform Dev Ctries, vol. 13, no. 1, 2019.

[4] M. Alanazi and B. Soh, "Investigating Cyber Readiness for IoT Adoption in Saudi Arabia," IBIMA Business Review, vol. 2020, 2021, doi: 10.5171/2020.937087.

[5] A. M. AL-Shehry, "Transformation towards E-government in The Kingdom of Saudi Arabia: Technological and Organisational Perspectives," 2008.

[6] F. Y. Al Anezi, "Saudi Vision 2030: Sustainable economic development through IoT," in Proceedings - 2021 IEEE 10th International Conference on Communication Systems and Network Technologies, CSNT 2021, 2021. doi: 10.1109/CSNT51715.2021.9509592.

[7] J. Alzahrani, "The impact of e-commerce adoption on business strategy in Saudi Arabian small and medium enterprises (SMEs)," Review of Economics and Political Science, vol. 4, no. 1, 2019, doi: 10.1108/REPS-10-2018-013.

[8] O. Almutairi and K. Almarhabi, "Investigation of Smart Home Security and Privacy: Consumer Perception in Saudi Arabia," International Journal of Advanced Computer Science and Applications, vol. 12, no. 4, 2021, doi: 10.14569/IJACSA.2021.0120477.

[9] M. S. Albarrak and S. A. Alokley, "FinTech: Ecosystem, Opportunities and Challenges in Saudi Arabia," Journal of Risk and Financial Management, vol. 14, no. 10, 2021, doi: 10.3390/jrfm14100460.

[10] M. Mahmud, Y. O. Akinwale, R. A. Khan, and A. Alaraifi, "Techno entrepreneurship adoption: An intention based assessment study of start-ups in the Kingdom of Saudi Arabia," J Entrep Educ, vol. 22, no. 5, 2019.

[11] W. Basri, "Examining the impact of artificial intelligence (Ai)-assisted social media marketing on the performance of small and medium enterprises: Toward effective business management in the saudi arabian context," International Journal of Computational Intelligence Systems, vol. 13, no. 1, 2020, doi: 10.2991/ijcis.d.200127.002.

[12] A. Y. Alqahtani, "Investigation of startups' sustainability: empirical evidence from Saudi Arabia," Entrepreneurship and Sustainability Issues, vol. 10, no. 1, 2022, doi: 10.9770/jesi.2022.10.1(6).

[13] A. R. Abu Bakar, S. Z. Ahmad, N. S. Wright, and H. Skoko, "The propensity to business startup: Evidence from Global Entrepreneurship Monitor (GEM) data in Saudi Arabia," Journal of Entrepreneurship in Emerging Economies, vol. 9, no. 3, 2017, doi: 10.1108/JEEE-11-2016-0049.

[14] R. A. Mohammed, M. Horoub, and H. Walwil, "Establishing a start-up in Saudi Arabia: the Innosoft story," Emerald Emerging Markets Case Studies, vol. 9, no. 2, 2019, doi: 10.1108/EEMCS-05-2017-0076.

[15] N. Trad and M. A. Al Dabbagh, "Use of Social Media as an Effective Marketing Tool for Fashion Startups in Saudi Arabia," Open J Soc Sci, vol. 08, no. 11, 2020, doi: 10.4236/jss.2020.811029.

[16] Majed Qabil Alsolamy, "Startups in Saudi Arabia: Challenges and Opportunities," International Journal of Research in Business and Social Science (2147- 4478), vol. 12, no. 2, 2023, doi: 10.20525/ijrbs.v12i2.2312.

[17] H. M. Aboalsamh, L. T. Khrais, and S. A. Albahussain, "Pioneering Perception of Green Fintech in Promoting Sustainable Digital Services Application within Smart Cities," Sustainability (Switzerland), vol. 15, no. 14, 2023, doi: 10.3390/su151411440.

[18] A. M. K. Alkhazaleh, "Challenges and Opportunities for Fintech Startups: Situation in the Arab World," Academy of Accounting and Financial Studies Journal, vol. 25, no. 3, 2021.

[19] C. PÖPPER, M. MANIATAKOS, and R. DI PIETRO, "Cyber Security Research in the Arab Region: A Blooming Ecosystem with Global Ambitions.," Commun ACM, vol. 64, no. 4, 2021.

[20] K. Kim, "Security and Privacy Liability Policy in the Arab World," Security Policy Paper, vol. 2, no. 1, 2021, doi: 10.26735/outi8333.

[21] V. Sharma, I. You, K. Andersson, F. Palmieri, M. H. Rehmani, and J. Lim, "Security, privacy and trust for smart mobile-Internet of Things (M-IoT): A survey," IEEE Access, 2020, doi: 10.1109/ACCESS.2020.3022661.

[22] D. Choudhary, "Security Challenges and Countermeasures for the Heterogeneity of IoT Applications," Journal of Autonomous Intelligence, vol. 1, no. 2, 2019, doi: 10.32629/jai.v1i2.25.

[23] H. F. Atlam and G. B. Wills, "IoT Security, Privacy, Safety and Ethics," in Internet of Things, 2020. doi: 10.1007/978-3-030-18732-3_8.

[24] A. Lakhdari, A. Bouguettaya, S. Mistry, and A. G. Neiat, "Composing Energy Services in a Crowdsourced IoT Environment," IEEE Trans Serv Comput, vol. 15, no. 3, 2022, doi: 10.1109/TSC.2020.2980258.

[25] L. Li and G. Wu, "Development and Design of Electronic Information Management System Based on Internet of Things Technology," in ACM International Conference Proceeding Series, 2023. doi: 10.1145/3585967.3585976.

[26] M. Dobrojevic and N. Bacanin, "IoT as a Backbone of Intelligent Homestead Automation," Electronics (Switzerland), vol. 11, no. 7. 2022. doi: 10.3390/electronics11071004.

[27] R. Martínez-Peláez et al., "An enhanced lightweight IoT-based authentication scheme in cloud computing circumstances," Sensors (Switzerland), 2019, doi: 10.3390/s19092098.

[28] L. Belli et al., "IoT-enabled smart sustainable cities: Challenges and approaches," Smart Cities, vol. 3, no. 3, 2020, doi: 10.3390/smartcities3030052.

[29] K. Yeow, A. Gani, R. W. Ahmad, J. J. P. C. Rodrigues, and K. Ko, "Decentralized Consensus for Edge-Centric Internet of Things: A Review, Taxonomy, and Research Issues," IEEE Access, 2017, doi: 10.1109/ACCESS.2017.2779263.

[30] P. K. Senyo, E. Addae, and R. Boateng, "Cloud computing research: A review of research themes, frameworks, methods and future research directions," Int J Inf Manage, 2018, doi: 10.1016/j.ijinfomgt.2017.07.007.

[31] K. Mahmood, W. Akram, A. Shafiq, I. Altaf, M. A. Lodhi, and S. H. Islam, "An enhanced and provably secure multi-factor authentication scheme for Internet-of-Multimedia-Things environments," Computers and Electrical Engineering, 2020, doi: 10.1016/j.compeleceng.2020.106888.

[32] B. Liu, M. Ding, S. Shaham, W. Rahayu, F. Farokhi, and Z. Lin, "When Machine Learning Meets Privacy: A Survey and Outlook," ACM Computing Surveys. 2021. doi: 10.1145/3436755.

[33] Md. A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian, "A Survey on the Adoption of Blockchain in IoT: Challenges and Solutions," Blockchain: Research and Applications, p. 100006, 2021, doi: 10.1016/j.bcra.2021.100006.

[34] X. Huang, D. Zou, G. Cheng, X. Chen, and H. Xie, "Trends, Research Issues and Applications of Artificial Intelligence in Language Education," EDUCATIONAL TECHNOLOGY & SOCIETY, 2021.

[35] A. A. Qaffas, R. Hoque, and N. Almazmomi, "The Internet of Things and Big Data Analytics for Chronic Disease Monitoring in Saudi Arabia," Telemedicine and e-Health, vol. 27, no. 1, 2021, doi: 10.1089/tmj.2019.0289.

[36] L. Hirtan, P. Krawiec, C. Dobre, and J. M. Batalla, "Blockchain-based approach for e-health data access management with privacy protection," in IEEE International Workshop on Computer Aided Modeling and Design of Communication Links and Networks, CAMAD, 2019. doi: 10.1109/CAMAD.2019.8858469.

[37] L. Edwards, "Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective," SSRN Electronic Journal, 2016, doi: 10.2139/ssrn.2711290.

[38] M. U. Hassan, M. H. Rehmani, and J. Chen, "Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions," Future Generation Computer Systems, vol. 97, pp. 512–529, 2019, doi: 10.1016/j.future.2019.02.060.

[39] P. Kumar and L. Chouhan, "A privacy and session key based authentication scheme for medical IoT networks," Comput Commun, 2021, doi: 10.1016/j.comcom.2020.11.017.

[40] S. Qazi, B. A. Khawaja, and Q. U. Farooq, "IoT-Equipped and AI-Enabled Next Generation Smart Agriculture: A Critical Review, Current Challenges and Future Trends," IEEE Access, vol. 10. 2022. doi: 10.1109/ACCESS.2022.3152544.

[41] A. Babiyola, V. Saillaja, S. P. Shally, and S. Omkumar, "Development of an Internet of Things-based Integrated System for Fleet Management in RealTime," in Proceedings of the 2nd International Conference on Edge Computing and Applications, ICECAA 2023, 2023. doi: 10.1109/ICECAA58104.2023.10212331.

[42] S. Bansal and A. Gupta, "IoT-Enabled Intelligent Traffic Management System," in EAI/Springer Innovations in Communication and Computing, 2023. doi: 10.1007/978-3-031-04524-0_6.

[43] J. Sengupta, S. Ruj, and S. Das Bit, "A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT," Journal of Network and Computer Applications. 2020. doi: 10.1016/j.jnca.2019.102481.

[44] H. Taslimasa, S. Dadkhah, E. C. P. Neto, P. Xiong, S. Ray, and A. A. Ghorbani, "Security issues in Internet of Vehicles (IoV): A comprehensive survey," Internet of Things (Netherlands), vol. 22. 2023. doi: 10.1016/j.iot.2023.100809.

[45] P. Rutravigneshwaran and G. Anitha, "Security Model to Mitigate Black Hole Attack on Internet of Battlefield Things (IoBT) Using Trust and K-Means Clustering Algorithm," International Journal of Computer Networks and Applications, vol. 10, no. 1, 2023, doi: 10.22247/ijcna/2023/218514.

[46] V. Sklyar and V. Kharchenko, "ENISA Documents in Cybersecurity Assurance for Industry 4.0: IIoT Threats and Attacks Scenarios," in Proceedings of the 2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2019, 2019. doi: 10.1109/IDAACS.2019.8924452.

[47] S. Aljarallah and R. Lock, "An empirical study of sustainable e-government characteristics in saudi arabia," in Proceedings of the European Conference on e-Government, ECEG, 2018.

[48] M. E. E. Alahi et al., "Integration of IoT-Enabled Technologies and Artificial Intelligence (AI) for Smart City Scenario: Recent Advancements and Future Trends," Sensors, vol. 23, no. 11. 2023. doi: 10.3390/s23115206.

[49] N. S. Abu et al., "Internet of Things Applications in Precision Agriculture: A Review," Journal of Robotics and Control (JRC), vol. 3, no. 3. 2022. doi: 10.18196/jrc.v3i3.14159.

[50] I. Mahnashi, B. Salah, and A. E. Ragab, "Industry 4.0 Framework Based on Organizational Diagnostics and Plan–Do–Check–Act Cycle for the Saudi Arabian Cement Sector," Sustainability (Switzerland), vol. 15, no. 14, 2023, doi: 10.3390/su151411261.

[51] A. Altaf, F. Iqbal, R. Latif, B. M. Yakubu, S. Latif, and H. Samiullah, "A Survey of Blockchain Technology: Architecture, Applied Domains, Platforms, and Security Threats," Soc Sci Comput Rev, 2022, doi: 10.1177/08944393221110148.

[52] W. Hermawan and K. Tjendrasa, "Evaluation Of Investment In IoT Startup at PT TMI," Jurnal Ilmu Sosial Politik dan Humaniora, vol. 3, no. 2, 2020, doi: 10.36624/jisora.v3i2.46.

[53] V. Neerugatti, Dr. B. K.K., J. P. Dr. M., and S. K. V. D., "Internet of Things: A Product Development Cycle for the Entrepreneurs," HELIX, vol. 10, no. 2, 2020, doi: 10.29042/2020-10-2-155-160.

[54] S. Y. Cooper and J. S. Park, "The impact of 'incubator' organizations on opportunity recognition and technology innovation in new, entrepreneurial high-technology ventures," International Small Business Journal, vol. 26, no. 1, 2008, doi: 10.1177/0266242607084658.

[55] P. W. Williams and M. Peters, "Entrepreneurial performance and challenges for aboriginal small tourism businesses: A Canadian case," Tourism Recreation Research, vol. 33, no. 3, 2008, doi: 10.1080/02508281.2008.11081551.

[56] V. Jafari-Sadeghi, "The motivational factors of business venturing: Opportunity versus necessity? A gendered perspective on European countries," J Bus Res, vol. 113, 2020, doi: 10.1016/j.jbusres.2019.09.058.

[57] H. Sandberg, A. Alnoor, and V. Tiberius, "Environmental, social, and governance ratings and financial performance: Evidence from the European food industry," Bus Strategy Environ, vol. 32, no. 4, 2023, doi: 10.1002/bse.3259.

[58] D. B. Audretsch, "Have we oversold the Silicon Valley model of entrepreneurship?," Small Business Economics, vol. 56, no. 2, 2021, doi: 10.1007/s11187-019-00272-4.

[59] F. F. Adedoyin, F. V. Bekun, O. M. Driha, and D. Balsalobre-Lorente, "The effects of air transportation, energy, ICT and FDI on economic growth in the industry 4.0 era: Evidence from the United States," Technol Forecast Soc Change, vol. 160, 2020, doi: 10.1016/j.techfore.2020.120297.

[60] H. Yarovenko, "'Evaluating the threat to national information security,'" Problems and Perspectives in Management, vol. 18, no. 3, 2020, doi: 10.21511/ppm.18(3).2020.17.

[61] S. Prajapati and A. Singh, "Cyber-Attacks on Internet of Things (IoT) Devices, Attack Vectors, and Remedies: A Position Paper," in EAI/Springer Innovations in Communication and Computing, 2022. doi: 10.1007/978-3-030-73885-3_17.

[62] V. Narayandas, M. Archana, and D. Raman, "The Role of MANET in Collaborating IoT End Devices: A New Era of Smart Communication," International Journal of Interactive Mobile Technologies, 2021, doi: 10.3991/ijim.v15i13.23045.

[63] L. Javed, B. M. Yakubu, M. Waleed, Z. Khaliq, A. B. Suleiman, and N. G. Mato, "BHC-IoT: A Survey on Healthcare IoT Security Issues and Blockchain-Based Solution," International Journal of Electrical and Computer Engineering Research, vol. 2, no. 4, 2022, doi: 10.53375/ijecer.2022.302.

[64] A. L. Bozzo, H. D. M. Freitas, and C. D. P. Martens, "Main initial difficulties faced by IoT startups," Revista da Micro e Pequena Empresa, vol. 13, no. 2, 2019, doi: 10.21714/19-82-25372019v13n2p4059.

[65] S. Lim, O. Kwon, and D. H. Lee, "Technology convergence in the Internet of Things (IoT) startup ecosystem: A network analysis," Telematics and Informatics, vol. 35, no. 7, 2018, doi: 10.1016/j.tele.2018.06.002.

[66] J. Kim and E. Park, "Understanding social resistance to determine the future of Internet of Things (IoT) services," Behaviour and Information Technology, vol. 41, no. 3, 2022, doi: 10.1080/0144929X.2020.1827033.

[67] T. Mhlongo, J. A. van der Poll, and T. Sethibe, "A Control Framework for a Secure Internet of Things within Small-, Medium-, and Micro-Sized Enterprises in a Developing Economy," Computers, vol. 12, no. 7, 2023, doi: 10.3390/computers12070127.

[68] E. Lee, Y. D. Seo, S. R. Oh, and Y. G. Kim, "A Survey on Standards for Interoperability and Security in the Internet of Things," IEEE Communications Surveys and Tutorials, vol. 23, no. 2. 2021. doi: 10.1109/COMST.2021.3067354.

[69] N. M. Karie, N. M. Sahri, W. Yang, C. Valli, and V. R. Kebande, "A Review of Security Standards and Frameworks for IoT-Based Smart Environments," IEEE Access, vol. 9, 2021, doi: 10.1109/ACCESS.2021.3109886.

[70] P. Devi, K. Dhivyapriya, D. Venkata Subramanian, and S. Sathyalakshmi, "A review on iot-standards, protocols, frameworks," Journal of Advanced Research in Dynamical and Control Systems, vol. 9, no. Special Issue 18. 2017.

[71] "International Telecommunication Union (ITU)," in International Regulatory Co-operation, 2016. doi: 10.1787/9789264244047-37-en.

[72] F. Schneider, C. Maurer, and R. C. Friedberg, "International organization for standardization (ISO) 15189," Annals of Laboratory Medicine, vol. 37, no. 5. 2017. doi: 10.3343/alm.2017.37.5.365.

[73] T. Büthe and A. fattah Alshadafan, "The International Electrotechnical Commission," in The Evolution of Transnational Rule-Makers through Crises, 2023. doi: 10.1017/9781009329408.021.

[74] "Institute of Electrical and Electronics Engineers (IEEE)," in Cite Them Right online - The Basics, 2022. doi: 10.5040/9781350928060.35.

[75] "National Institute of Standards and Technology," Choice Reviews Online, vol. 50, no. 04, 2012, doi: 10.5860/choice.50-2030.

[76] IoT Security Foundation, "IoT Security Foundation," IOT SECURITY FOUNDATION CONFERENCE 2016.

[77] C. NIST, "Cybersecurity Framework | NIST," NIST Website, 2016.

[78] A. S. Syed, D. Sierra-Sosa, A. Kumar, and A. Elmaghraby, "Iot in smart cities: A survey of technologies, practices and challenges," Smart Cities, vol. 4, no. 2, 2021, doi: 10.3390/smartcities4020024.

[79] A. Borys, A. Kamruzzaman, H. N. Thakur, J. C. Brickley, M. L. Ali, and K. Thakur, "An Evaluation of IoT DDoS Cryptojacking Malware and Mirai Botnet," in 2022 IEEE World AI IoT Congress, AIIoT 2022, 2022. doi: 10.1109/AIIoT54504.2022.9817163.

[80] N. Nanglae, B. M. Yakubu, and P. Bhattarakosol, "Extraction of Hidden Authentication Factors from Possessive Information," Journal of Sensor and Actuator Networks, vol. 12, no. 4, p. 62, Aug. 2023, doi: 10.3390/jsan12040062.

[81] B. M. Yakubu, M. I. Khan, and P. Bhattarakosol, "IPChain: Blockchain-Based Security Protocol for IoT Address Management Servers in Smart Homes," Journal of Sensor and Actuator Networks, vol. 11, no. 4, 2022, doi: 10.3390/jsan11040080.

[82] D. Pal, X. Zhang, and S. Siyal, "Prohibitive factors to the acceptance of Internet of Things (IoT) technology in society: A smart-home context using a resistive modelling approach," Technol Soc, vol. 66, 2021, doi: 10.1016/j.techsoc.2021.101683.

[83] Z. A. Memish, M. M. Altuwaijri, A. H. Almoeen, and S. M. Enani, "The Saudi data & artificial intelligence authority (SDAIA) vision: Leading the Kingdom's journey toward global leadership," Journal of Epidemiology and Global Health, vol. 11, no. 2. 2021. doi: 10.2991/JEGH.K.210405.001.

[84] M. Anagnostopoulos, G. Spathoulas, B. Viaño, and J. Augusto-Gonzalez, "Tracing your smart-home devices conversations: A real world iot traffic data-set," Sensors (Switzerland), 2020, doi: 10.3390/s20226600.

[85] H. Abdullah Alnemer, "Predicting start-up intention among the females of Saudi Arabia using social cognitive theory," World Journal of Entrepreneurship, Management and Sustainable Development, vol. 17, no. 4, 2021, doi: 10.1108/WJEMSD-05-2021-0085.

[86] Abdulkarim AlShinqeeti, "Digital Transformation in Saudi Arabia: A Journey of Progress and Innovation," LinkedIn. Accessed: Mar. 28, 2024. [Online]. Available: https://www.linkedin.com/pulse/digital-transformation-saudi-arabia-journey-progress-alshinqeeti-t5pef/

[87] ArrxdQ, "Saudi Vision 2030," X. Accessed: Mar. 28, 2024. [Online]. Available: https://twitter.com/ArrxdQ/status/1386401941790461956

[88] A. B. E. Aichouni, L. Kolsi, and M. Aichouni, "The Engineering Students Innovation Club Project for Human Capital Development in the areas of Industry 4.0 - From the Design to Implementation," in 2020 Industrial and Systems Engineering Conference, ISEC 2020, 2020. doi: 10.1109/ISEC49495.2020.9229924.

[89] M. K. Sarma and D. Dutta, "Adoption of Technological Service Innovations: A Systematic Review Investigating the Special Role of Incremental Innovations," International Journal of Technology, Policy and Management, vol. 24, no. 2, 2024, doi: 10.1504/ijtpm.2024.10058087.