Regulatory Policy for IoT Devices in Pakistan

By

Afsah ur Rehman

Supervisor

Prof. Dr. Haider Abbas

A thesis submitted to the faculty of Information Security Department, Military College of Signals, National University of Sciences and Technology, Rawalpindi, in partial fulfilment of the requirements for the degree of MS in Information Security

Sep 2022

THESIS ACCEPTANCE CERTIFICATE

Certified that final copy of MS Thesis written by **Ms Afsah Ur Rehman**, Registration No. **00000277348**, of **Military College of Signals** has been vetted by undersigned, found complete in all respects as per NUST Statutes/Regulations/MS Policy, is free of plagiarism, errors, and mistakes and is accepted as partial fulfilment for award of MS degree. It is further certified that necessary amendments, as pointed out by GEC members and local evaluators of the scholar, have also been incorporated in the said thesis.

Signature: _____

Name of Supervisor: Prof. Dr. Haider Abbas

Date: _____

Signature (HOD): _____

Date: _____

Signature (Dean/Principal) _____

Date: _____

Declaration

I hereby declare that no portion of work presented in this thesis has been submitted in support of another award or qualification either at this institution or elsewhere.

Acknowledgements

All praises be to Allah for the strength and His blessing in completing this thesis.

I want to convey my gratitude to my supervisor, Dr. Haider Abbas, for his supervision and constant support. His invaluable help of constructive comments and suggestions throughout the experimental and thesis works are significant contributions to the success of this research. Also, I would thank my committee members, especially Maj Muhammad Sohaib Khan, for his constant support and knowledge regarding this topic.

Lastly, I am highly thankful to my family and friends, who have always stood by me and have been a great source of inspiration for me.

Abstract

The number of connected devices in the world is increasing day by day. This network of interconnected systems, devices, and services is called the Internet of Things (IoT). Besides its numerous advantages, the high adoption rate of IoT in almost all application areas of life sets attractive, often easy targets for cybercriminals. IoT's threat landscape is broader than other conventional networks and systems. The Government of Pakistan has already shown a significant interest in the IoT. In this regard, the Ministry of Information Technology and Communication Pakistan also released a Regulatory Framework for IoT and SR Devices, but this is a licensing framework to enable the development of IoT and does cover its cybersecurity aspects.

The “National Cyber Security Policy” of Pakistan also lacks IoT specific security suggestions and is a broader security suggestion document. This can potentially lead to an insecure IoT environment and malicious activities in the IoT ecosystem of Pakistan. After analyzing this critical gap in national security, a Security Policy Draft for IoT Devices in Pakistan is proposed in this research after analyzing various international standards and deriving best practices. This draft aims to cover key security challenges faced by the IoT and propose solutions to them. This research also suggests an implementation framework for the policy that can be rolled out in three stages.

Keywords—Internet of Things, Cyber Security, Policy, Pakistan

Abbreviations

IoT—Internet of Things

SRD—Short Range Devices

PTA—Pakistan Telecommunication Authority

LPWAN—Low-Power Wide Area Network

UAV—Unmanned Aerial Vehicles

ICT—Information and Communication Technology

INCB—Israel National Cyber Bureau

IGF—Internet Governance Forum

APNIC—Asia Pacific Network Information Center

ISP—Internet Service Providers

BLE—Bluetooth Low Energy

PKI—Public Key Infrastructure

MINKOMSVYAZ—Ministry of Digital Development, Communications and Mass Media of the Russian Federation

IP—Internet Protocol

HLAC—High-Level Advisory Committee

IT—Information Technology

Telecom—Telecommunication

DDoS—Distributed Denial of Services

MITM—Man in the Middle

Table of Contents

Declaration ii

Acknowledgements iii

Abstract iv

Abbreviations v

List of Figures xi

List of Tables xi

Chapter 1 1

Introduction 1

1.1 Introduction to IoT 1

1.2 Security Issues in IoT 1

1.2.1 Software and Hardware Vulnerabilities 2

1.2.2 Insecure Communication 3

1.2.3 Data Leaks 3

1.2.4 Malware Threats 3

1.2.5 Cyber Attacks 4

1.3 IoT Attacks Globally 4

1.4 IoT Security Policy Needs in Pakistan 4

1.5 Problem Statement 6

1.6 Motivation 7

1.7 Aim & Objectives 8

1.7.1 Research Aim 8

1.7.2 Research Objectives 8

1.8 Dissertation Structure 8

Chapter 2 10

IoT Threats and Security Landscape of Pakistan 10

2.1 Introduction to the IoT Ecosystem 10

2.2 IoT Ecosystem in Pakistan 12

2.2.1 Smartphones 12

2.2.2 Wearables 13
2.2.3 Enterprise Solutions 13
2.2.3 Smart Homes 13
2.2.5 Smart Cities 13
2.2.6 Supply Chain Management 14
2.2.7 Healthcare Functions 14
2.2.8 Smart Grids 14
2.3 Major Threats to the IoT Ecosystem of Pakistan 15
2.3.1 Hacking 15
2.3.2 Organized Cyber Crime 16
2.3.3 Cyber Terrorism 16
2.3.4 Cyber Warfare 17
2.4 Risks Due to the Lack of an IoT Security Policy in Pakistan 17
2.4.1 IoT Botnets 18
2.4.2 Shadow IoT 18
2.4.3 Mismanagement and Misconfiguration of IoT Devices 19
2.4.4 Complex IoT Environments 19
2.4.5 DNS Threats 19
2.4.6 Insecure Data Transfer 19
2.4.7 Unsafe Communication 20
2.4.8 Remote Access 20
Chapter 3 21
Literature Review of Existing Standards 21
3.1 NIST Cybersecurity for IoT Program 21
3.1.1 NISTIR 8259 Series 21
3.1.2 SP 800-213 Series 22
3.1.3 Consumer IoT Products 22
3.1.4 Takeaways 22
3.2 IEEE Internet of Things (IoT) Security Best Practices 23
3.2.1 Introduction 23
3.2.2 Best Practices 23
3.2.3 Takeaways 24
3.3 ACM Statement on Internet of Things Privacy and Security 26
3.3.1 Takeaways 27
3.4 GSMA IoT Security Guidelines 28

3.4.1 Recommendations For Mobile Devices 28
3.4.2 Recommendations For Mobile Services 29
3.4.3 Recommendations For Networks 29
3.5 ENISA: Baseline Security Guidelines for IoT 31
3.5.1 Recommendations and Best Practices 31
3.6 Comparative Analysis 33
3.7 Best Practices Derived from International Standards 34
3.7.1 Secure Device Firmware and Hardware 34
3.7.2 Secure the Entire IoT Network 34
3.7.3 Secure the Overall IoT System 34
Chapter 4 35
Analysis of IoT Strategies of Different Countries 35
4.1 Introduction 35
4.2 IoT Security Policies of the USA 36
4.2.1 IoT Security Suggestions from the US Dept of Homeland Security 36
4.2.2 IoT Cyber Security Improvement Act of 2020 37
4.3 IoT Security Policies of UK 39
4.3.1 Product Security and Telecommunications Infrastructure (PSTI) Bill 39
4.4 IoT Security Policies of Russia 42
4.4.1 Minkomsvyaz Study on Security of IoT 42
4.4.2 Future for IoT Security 42
4.5 IoT Security Policies of India 43
4.5.1 National Digital Communications Policy 2018 43
4.5.2 Code of Practice for Securing Consumer Internet of Things (IoT) 44
4.5.3 IoT Ecosystem Development Initiatives 44
4.6 IoT Security Policies of China 46
4.3.1 MIIT Guidelines for Security Standard System for IoT 46
4.6.2 China Standards Plan 2035 48
4.7 IoT Security Policies of Israel 50
4.7.1 The Corporate Defense Methodology 50
4.7.2 Best Practice Reducing cyber security risks in video surveillance cameras 51
4.8 Derived Best Practices 54

4.9 Comparative Analysis of Different Country's Policies 56
Chapter 5 58
Analysis of Security Policies in Pakistan 58
5.1 National Cyber Security Policy of Pakistan 58
5.1.2 Principles of National Cyber Security Policy of Pakistan 58
5.1.3 Objectives of the National Cyber Security Policy of Pakistan 58
5.1.4 Gaps in Terms of IoT Security 63
5.2 Digital Pakistan Policy 64
5.2.1 Key Objectives of the Digital Pakistan Policy 64
5.2.2 Policy Strategy 65
5.2.3 Relevance to IoT Security 67
Chapter 6 68
Security Policy for IoT Devices in Pakistan: A Draft 68
6.1 Introduction 68
6.2 Vision, Scope & Objectives 71
6.2.1 Vision 71
6.2.2 Scope 71
6.2.3 Objectives 71
6.2.4 IoT Security Policy Details 74
Chapter 7 89
Policy Implementation Framework 89
7.1 Introduction 89
7.2 Phase 1: Short Term Plan 90
7.2.1 Nationwide IoT Survey 90
7.2.2 Governance/Legislation 90
7.2.3 Standardization 91
7.2.4 Infrastructure Development 91
7.3 Phase 2: Long Term Plan 92
7.3.1 Creating Awareness 92
7.3.2 Human Resource Development 93
7.3.3 Adoption of Local Manufacturing 93
7.3.4 International Standardization 94

7.4 Phase 3: Ongoing Efforts 94
7.4.1 Monitoring 94
7.4.2 Reviews 95
Chapter 8 96
Conclusion and Future Work 96
8.1 Background Study 96
8.2 Policies Analyzed 96
8.3 Proposed Solution/Policy 97
8.4 Implementation Strategy 97
8.5 Future Work 98

List of Figures

Figure 1:Common IoT Security Challenges 2
Figure 2: The generic ecosystem of IoT 10
Figure 3: Critical factors to a thriving IoT Ecosystem 11
Figure 4: Common applications of IoT Technology 12
Figure 5: Major Threats to IoT Ecosystem in Pakistan 15
Figure 6: Risks due to lack of an IoT Security Policy 18
Figure 7: Overview of Proposed National IoT Security Policy 70
Figure 8: IoT Security Policy Objectives 72
Figure 9: Proposed Structure of IoT Advisory Committee 75
Figure 10: Risks in the IoT Landscape of Pakistan 78
Figure 11: Risk Management in the IoT Ecosystem 85
Figure 12: IoT Security Implementation Framework 89

List of Tables

Table 1: Comparative Analysis of International Standards and Policies 33
Table 2: Comparative Analysis of Different Country's Policies 56
Table 3: Summary of the objectives of the National Cyber Security Policy of Pakistan and Loopholes Pertaining to IoT Security 63
Table 4: Summary of the objectives of the Digital Pakistan Policy and their relevance to IoT Security 67
Table 5: Risk Management Overview 80

Chapter 1

Introduction

1.1 Introduction to IoT

Internet of Things (IoT) is a network of connected devices in which seamless Machine to Machine (M2M) communication is possible without any kind of human interference [1]. IoT is a concept that enables all the devices — whether it's a computer, a car, a printer, a coffee maker, a fridge, a watch, or any other device — to connect to each other without any human intervention and exchange data. The data exchange can happen in real time or in an automated fashion. It could be any type of data: from simple to complex and from structured to unstructured. It could be sent and received between two devices or more. The magnitude of the data exchange can be small or large. It can be one-to-one or one-to-many. Any device can be connected to any other device.

With the advent of IoT, the world has become a communication ecosystem, where devices, systems, and environments can exchange data and information to create a distributed network. With this transformation, businesses and individuals can now view, record, and analyze all the data points that were previously unavailable, unmeasurable, or unquantifiable. All things can now "talk" with one another.

Thanks to IoT, we are now living in a very different world, where physical things are connected with each other. The evolution of IoT has opened up a world of new possibilities, and we have only just begun to see its full impact.

1.2 Security Issues in IoT

IoT systems are often designed to be connected to the Internet. Because of this, they are open to threats from third parties. In addition, many IoT systems are designed to be used remotely, meaning that they need to be very user-friendly. This ease of use usually comes at the cost of security. The consequences of a successful cyber attack on an IoT system are often serious, as they can pose a serious risk to the physical safety of people. For example, a cyber attack on a fitness tracker can give an attacker access to sensitive information, such as the location of the owner.

Here is a list of common security challenges face by Internet of Things:

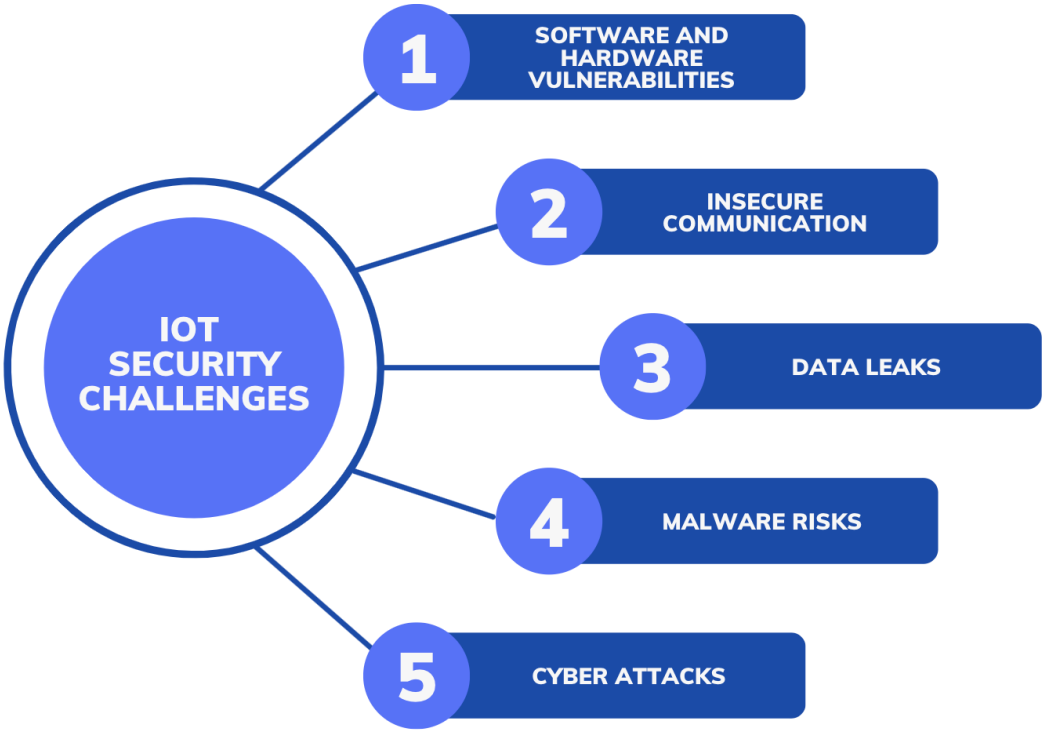

Figure 1:Common IoT Security Challenges

1.2.1 Software and Hardware Vulnerabilities

Because many smart devices are resource-poor and have little computing power, ensuring the security of IoT systems is difficult. These devices are unlikely to have more vulnerabilities than non-IoT devices because they cannot run resource-intensive security functions. Many IoT systems have security vulnerabilities for the following reasons:

- Lack of computational resources for efficient in-built security
- Lack of access control in IoT systems
- Limited testing and improving hardware security
- Lack of regular software patches and updates due to limited monetary and computing resources
- Lack of proper update routines on devices
- Unavailability of updates with time

- Lack of physical security

1.2.2 Insecure Communication

Since IoT devices are resource-constrained, traditional security measures are difficult to implement and hence are less effective at safeguarding their communications. Therefore, traditional security measures are not as efficient at protecting the communication of IoT devices.

The biggest risk of insecure communication is the man-in-the-middle (MitM) attack. If a device does not use safe encryption and authentication techniques to update, hackers can pull off a MitM attack and take over the device. Malware may be installed, or a device's functionality altered. Even if your device isn't victimized by an MitM attack, cybercriminals may still seize data it transmits to other gadgets and systems if it sends it in clear text messages.

A single device connected to a network can compromise all other unisolated devices if attackers gain access to it.

1.2.3 Data Leaks

Attackers can get access to the data your IoT system processes by capturing unencrypted messages from it. In addition to sensitive information like your location, bank account details, and health records, attackers may collect valuable data by abusing poorly secured communications.

Devices can leak data either via their own systems or via the cloud environments they are connected to, since all data is transferred through the cloud and stored there.

The data leak in your IoT systems might result from a third-party service. In this case, Ring smart doorbells were leaking customer data to Facebook and Google without proper consent, thanks to third-party tracking services in the Ring mobile app.

1.2.4 Malware Threats

Zscaler recently reported that set-top boxes, smart TVs, and smartwatches were the most susceptible to malware. By gaining access to an IoT system, attackers might alter its operations, collect personal data, or perform other malicious activities. In addition, some devices come pre-infected with viruses due to inadequate software security, particularly if manufacturers do not take adequate precautions.

1.2.5 Cyber Attacks

In addition to other attacks, IoT systems can be subject to various other cyberattacks. Some of these common attacks are:

1. Denial of Service (DoS) attacks
2. Denial of Sleep (DoSL) attacks
3. Device Spoofing
4. Physical Intrusion
5. Application based attacks

1.3 IoT Attacks Globally

IoT faces remarkable vulnerabilities because of its large attack surface and easy lateral infections. Because too few organisations follow best practices, too many are unprepared for the threat environment, the number and sophistication of potential attackers is growing, and too few are prepared. [2] From January to June 2021, there were 1.5 billion IoT security breaches.[2] On the other hand global IoT attacks rose 33% year-on-year 2018-2019.[3]

1.4 IoT Security Policy Needs in Pakistan

The ecosystem of IoT is thriving exponentially, not only in Pakistan but all over the globe. More than 80 billion internet-connected devices are expected at the end of 2025 [3]. This number is almost three times as compared to the number of devices connected to the internet in 2017. The connectivity and usage of internet will grow exponentially in near future and IoT is expected to fuel this growth. Research firm Statista predicts that worldwide spending on IoT technology is expected to grow from $157B in 2017 to $192B in 2021. IoT has a potential to transform almost every industry. From agriculture to healthcare, IoT has a role to play in every business and organization. IoT is expected to create billions of dollars in value for businesses over the next few years.

It is predicted that IoT technology has the potential to offer opportunities and tremendous scope for various industries in Pakistan [4]. Therefore, on February 16, 2022, a regulatory framework for Internet of Things (IoT) services and Short-Range Devices (SRD) was issued by Pakistan Telecommunication Authority (PTA). According to the official press

release of PTA[1], the licensing applications of the Low-Power Wide Area Network (LPWAN) class was accepted by PTA from March 31, 2022. The main objectives of PTA's IoT and SRD regulatory framework are:

- Enabling the IoT ecosystem development in Pakistan with governing mechanism for the industry
- Accelerating the growth of IoT services in Pakistan
- Facilitating the IoT-enabled digital transformation in Pakistan
- Supporting the various sectors in automating their operations
- Rendering reliable electronic services to the Pakistani citizens

The Government of Pakistan has shown significant interest and efforts in forming an effective structure for pertinent regulations of IoT implementations and activities. However, some essential concerns described below were ignored by PTA in their regulatory framework for IoT services and SRDs.

- **Privacy**

  A large volume of sensitive information and personal data is exchanged every time through IoT devices. Therefore, the policy is one of the significant concerns in the IoT ecosystem. In Pakistan, data networks are subtle, and secure cloud data storage facilities are still underdeveloped. Thus, data stored over the cloud and not protected sufficiently may become prone to leakage and unauthorized access. Comprised data may be used for various unwarranted purposes. For example, data collected by smart fitness tracking devices can be used for marketing purposes by medicine companies after analyzing users' health conditions, or malicious parties can blackmail the users after analyzing their watching habits from data shared by smart televisions. Hence, in this regard, stringent regulations are required to ensure users' privacy and keep a check on the service providers. [5] [6] [7]

---

[1] https://www.pta.gov.pk/en/media-center/single-media/pta-issues-regulatory-framework-for-srd-and-iot-services-170222

2 https://www.iotworldtoday.com/2021/09/17/iot-cyberattacks-escalate-in-2021-according-to-kaspersky/

3 https://blog.sonicwall.com/en-us/2019/10/sonicwall-encrypted-attacks-iot-malware-surge-as-global-malware-volume-dips

However, PTA's IoT and SRD regulatory framework has failed to address this critical issue and deserves close attention.

- **Security**

  Security is an essential aspect of the design and development of IoT devices. IoT technology already facilitates various critical and sensitive organizations of Pakistan in their operations. For example, connected drones and sensors are used by Pakistan Army for military surveillance. Therefore, information and communication security principles such as confidentiality, integrity, availability, accountability, authenticity, access control, identity management, and so on are undeniable in the IoT devices and ecosystem design and development. However, it is a notable concern that after determining the massive increase in demand, IoT device manufacturers shifted their focus on producing the quantity of IoT devices instead of their quality and security. [8] This low standard and cheap quality of IoT devices make them vulnerable and prone to cyber security attacks. Unfortunately, this crucial concern is also not included in Pakistan's IoT and SRD regulatory framework.

- **Lack of Standardization**

  The IoT and SRD regulatory framework of Pakistan ignored setting up any SOP or standard for designing and manufacturing IoT devices. IoT devices result in low security and troublesome operations due to the absence of valuable guides and standards for manufacturers. This lack of standard and quality in developing IoT devices may expand the security and privacy issues to the whole nation due to the homogeneity in the design and operations of IoT devices. Therefore, formulation of standards and SOPs in designing and developing IoT devices and ecosystems is required to ensure the industry's stable growth with efficient, effective, and non-disruptive operations.

1.5 Problem Statement

The current ‘Regulatory Framework for IoT and SRD’ and other policies such as the ‘National Cyber Security Policy’ and ‘Digital Pakistan Policy’ do not encompass best practices for designing and developing a secure national IoT ecosystem. It also does not provide guidelines on how to operate the ecosystem in a secure manner. As a result, this has created a regulatory vacuum in the form of uncertainty, which has resulted in a lack of investment in the IoT sector. Uncertainty regarding the regulatory framework for IoT

has created a perception in the market that the government does not have a comprehensive plan for regulating IoT. Despite the significant potential of the IoT sector in Pakistan, investors have avoided investing in this space due to the regulatory uncertainty. The government needs to work towards creating a clear and comprehensive regulatory framework for the IoT sector in Pakistan.

Privacy and security are among the significant challenges to the reliable and successful deployment of the IoT ecosystem. This is mainly due to the fact that most of the IoT devices are designed with a view to meeting business requirements and not the security regulatory compliance aspect. As a result, the potential risk factors that may be inherent in the design of these devices can often go unnoticed. In case of non-compliance or security risks being discovered in these devices, it would not be possible for them to be fixed. These regulatory gaps are expected to be addressed by the Government of Pakistan through this policy.

Thus, due to the absence of these critical concerns in its regulatory IoT regulatory framework, the national cyberspace of Pakistan possesses serious security threats related to cyber espionage and cyber-terrorism. Furthermore, the absence of regulatory framework for IoT devices in the national cyberspace of Pakistan might result in cyber-attacks against critical infrastructures and public utilities. Data protection laws are also absent in the national cyberspace of Pakistan. Consequently, due to the absence of laws on data protection in the national cyberspace of Pakistan, the personal data of citizens is at risk of being exposed to malicious entities. In the national cyberspace of Pakistan, there is no regulatory framework for IoT technologies. Consequently, the national IoT cyberspace of Pakistan is likely to experience serious artificial intelligence -based cyber-attacks.

1.6 Motivation

Nowadays, due to the rapid advancement in Information and Communication Technology (ICT), everyone wants to be connected, and an intelligent living style is a desire of every citizen. The IoT industry in Pakistan is expected to grow at an exponential speed due to the continuous fundamental efforts by the Government. However, challenges like lack of standardization, privacy, and security can negatively impact Pakistan's IoT industry growth. The primary motivation behind this research is to address

the security and privacy concerns in the IoT ecosystem of Pakistan for its stable, reliable, and growth at the competitive edge.

1.7 Aim & Objectives

1.7.1 Research Aim

This research proposes a policy to regulate the privacy and security of the IoT ecosystem in Pakistan. It outlines the factors that could go into regulatory guidelines for IoT in the country, as well as the benefits that could come from its implementation and the challenges that might be faced. The research also looks at regulatory frameworks in other countries to highlight the best practices that could be used in the development of regulations in Pakistan. The proposed cybersecurity regulatory framework for IoT devices will ensure that cyber threats to the IoT ecosystem of Pakistan do not dominate the possible positive impacts it can bring to the nation.

1.7.2 Research Objectives

To achieve the primary aim of the research, the following is the list of objectives required to complete:

1. Study and analyze Pakistan's current cyber threat landscape with a focus on IoT threats.
2. Analyze different IoT strategies of leading countries and focus on following best practices.
3. Critically analyze the National Cyber Security Policy and other regulations in Pakistan to highlight loopholes pertaining to IoT security.
4. Formulate a National IoT Security Policy draft for Pakistan, considering the current threat landscape.
5. Suggest an implementation strategy for the proposed IoT security policy.

1.8 Dissertation Structure

The thesis is organized as under:

Chapter 2

IoT Threats and Security Landscape of Pakistan: Review of existing literature on IoT security in Pakistan and other countries.

Chapter 3

Literature Review of Existing Standards: Detailed analysis and comparison of existing IoT security international standards.

Chapter 4

Analysis of IoT Strategies of Different Countries: Presents the review of IoT strategies of various developed countries, focusing on their best practices to secure their IoT ecosystem.

Chapter 5

Analysis of the Security Policies in Pakistan: Presents the critical analysis of the National Cyber Security Policy and Digital Pakistan Policy with a focus on highlighting the weak points pertaining to the security of the IoT ecosystem.

Chapter 6

National IoT Security Policy of Pakistan (A Draft): Formulates the National IoT Security Regulation for Pakistan to mitigate the observed threats to the IoT landscape of Pakistan.

Chapter 8

Policy Implementation Framework: Discusses the implementation strategy for the policy in both short and long term.

Chapter 7

Conclusion and Future Work: Concludes the dissertation and outlines work that can be done in future.

Chapter 2

IoT Threats and Security Landscape of Pakistan

2.1 Introduction to the IoT Ecosystem

The generic ecosystem of IoT (figure 1) is a combination of hardware (electronic devices), software, interoperable communication protocols, standards, and telecommunication industries [9].

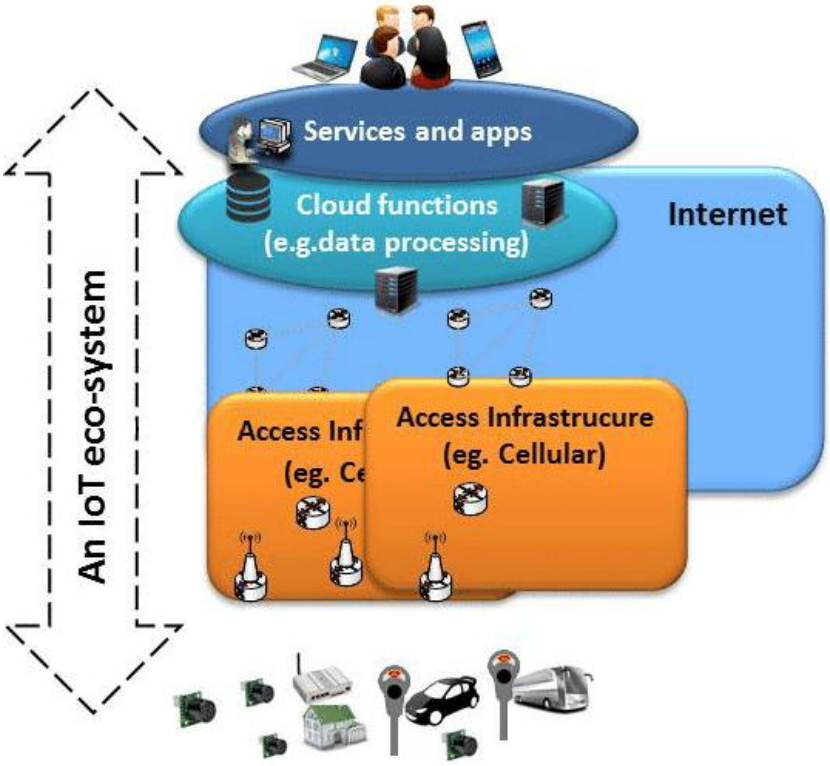

Figure 2: The generic ecosystem of IoT

IoT technology helps automate the solutions for various industries, including the health industry, national security services, disaster management, agriculture, defense, energy, business, and so on. Simply, this interplay of electronic hardware, telecom, and software promises to provide a great scope and marvelous opportunities for nations' growth. Various countries like China, the United States, and South Korea have gained advantages from IoT due to their advanced preparedness [10].

Three distinct stages of IoT operation involve:

1. Collection of data by sensors or electronic devices
2. Transmission of collected data towards respective applications to analyze that data for further alliance
3. Automated decision-making with the help of analytical engines, according to the specific application area of IoT deployment.

The key stakeholders of any IoT ecosystem are the Government, industry, and the citizens [11]. For a successful implementation, functioning, and growth of the IoT ecosystem, active collaboration, and participation of each stakeholder at a suitable stage is necessary. At this junction, the Government must implement regulations and policies for smooth, stable, and secure functions and promote the IoT ecosystem.

Countries currently progressing in the field of IoT, such as Pakistan, can adopt a more innovation-driven approach in their IoT ecosystems by learning from other countries who pioneers in this field. The critical factors to a thriving IoT ecosystem are:

- Governance
- Active research and development
- Building scalable models
- The utilization of citizens as sensors; and
- IoT regulations and policy at the top of all

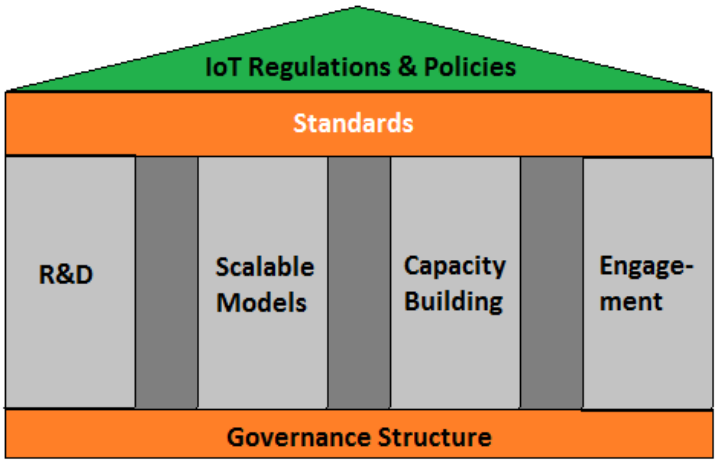

Figure 3: Critical factors to a thriving IoT Ecosystem

2.2 IoT Ecosystem in Pakistan

The role of IoT technology is undeniable in every domain and aspect of the modern day. [12] However, some of the most utilized IoT applications in Pakistan are discussed below.

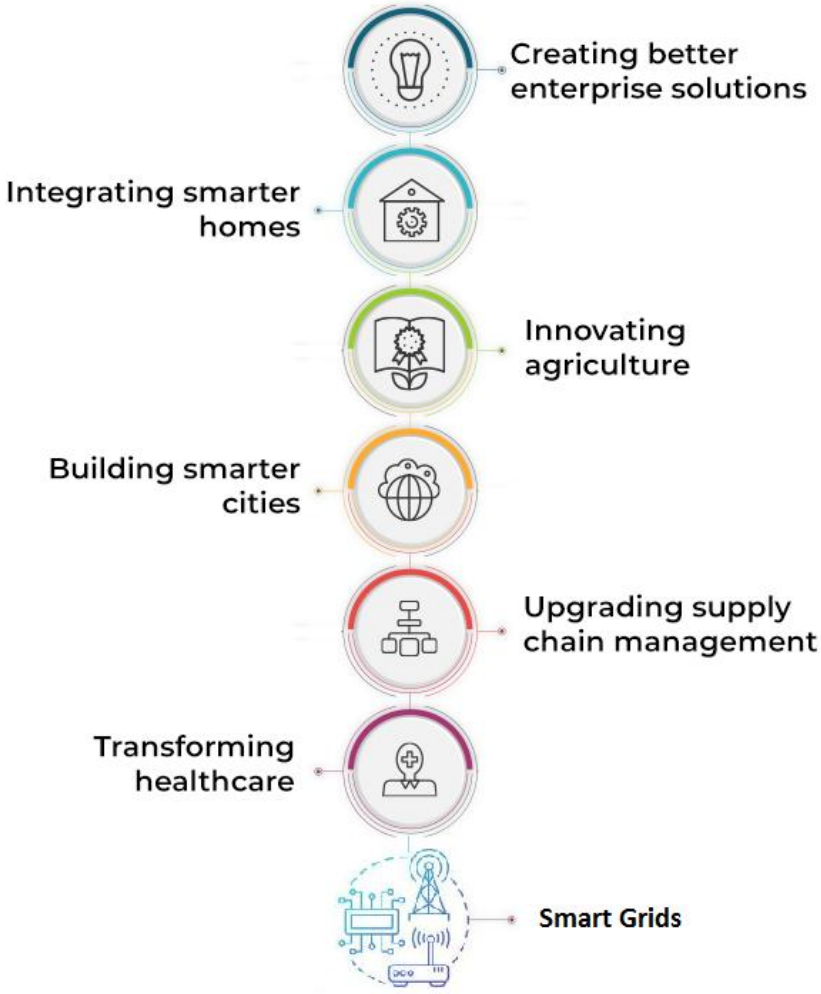

Figure 4: Common applications of IoT Technology

2.2.1 Smartphones

Smartphones have now become an essential part of our daily lives, and we cannot imagine a life without them. From making calls and sending texts to booking flights and ordering food, you can do everything on your phone. There are a lot of things one can do with your smartphone to make your life a little easier. Data from GSMA Intelligence shows that there were **186.9 million** cellular mobile connections in Pakistan at the start of 2022. Pakistan ranks 20th in the world for smartphone usage. All these smartphones are

basically handheld IoT devices, constantly connected to the internet and downloading and streaming data.

2.2.2 Wearables

Connected wearable devices are projected to become an essential part of people's daily lives. As their adoption rate increases, connected wearable devices will become even more widely used. This adoption rate is expected to skyrocket as the cost of sensors and other hardware components falls. [13] The forecasted growth in the number of connected wearable devices is driven by their convenience, ease of use, and their expanding functionality. [14]

2.2.3 Enterprise Solutions

Large organizations use tailored enterprise IoT solutions that require dedicated staff to implement, monitor and maintain their IT infrastructure. Real-time monitoring and data transmitted by IoT-backed systems help enterprises achieve organizational goals. Enterprises need to prepare effective incident response plans using IoT. Moreover, IoT technology can potentially display customer analytics based on real-time data. Thus, enterprises make effective decisions based on the real-time data extracted by IoT. [15]

2.2.3 Smart Homes

The smart home is one of the most common applications of IoT. IoT technology lets smart home residents control their electronic peripherals and security devices anywhere and anytime. Security cameras, speakers, home hubs, automatic blinds and light are some of the most used household IoT devices. [16] [17] [18]

2.2.5 Smart Cities

IoT technology is also incorporated into the better and smarter functioning of some cities. Some of the most valuable functions of IoT technology in cities are:

- Traffic management and monitoring
- Monitoring of pollution in cities
- Effective management of resources to save the valuable resources of nations
- Infrastructure management
- Disaster management
- Security solutions

2.2.6 Supply Chain Management

This application area of IoT started getting attention in 2020 [19]. In early 2020, supply chain issues affected many businesses due to the global shutdown caused by the pandemic. New working normal sets the trend of remote operations that made sense for enterprises to consider the integration of IoT into their supply chain management process [20]. Thus, integration of IoT in the supply chain offered valuable advantages to enterprises that adopted them, such as:

- Enabling enterprises to choose the best and smart routes
- Remote and real-time management of fleets
- Ensuring a high level of customers satisfaction and a smooth experience for managers

2.2.7 Healthcare Functions

The utilization of IoT in the healthcare industry had existed previously but it was accelerated during the Covid-19 pandemic. IoT has shown valuable potential in linking patients with doctors and pharmacies. With the help of IoT technology, doctors can monitor their patients remotely. Sensors attached to patients enable doctors to monitor their health conditions and prescribe accordingly from anywhere and anytime. Moreover, IoT is also playing an essential role in medical research, optimization of the manufacturing process in pharmacies, vaccine cold monitoring, and so on. [21]

2.2.8 Smart Grids

Energy provisioning has become more efficient and reliable with the help of IoT [22]. Appropriate IoT sensors attached to energy transmission lines, electric meters, production plants, and distribution points collectively set up the smart grid. Motivations behind leveraging the IoT in smart grids are:

- In time alerts in the case of electricity failure to ensure the high availability of power to users
- Identification of abnormalities in transmission lines
- Real-time collection of electricity consumption data for statistics and resource management
- Identification of lossy nodes.

2.3 Major Threats to the IoT Ecosystem of Pakistan

Awareness of cyber security is crucial in all sectors. To survive in a current digitized world, it is critical to have interconnected systems. However, interconnected systems set an attractive target for adversaries. Cyber security knowledge is required at each level, i.e., from the Government to citizens, to mitigate the threats. Similarly, the Government of Pakistan should be aware of and take proper actions to avoid online crimes. Other citizens will start losing their trust in the digital landscape, which can be dangerous for the country in this age of digitization. [23] [24] [25]

Pakistan falls low, i.e., 67th in the Global Cyber Security Index [26]. Enhanced awareness about cyber security threats among residents of Pakistan can change that disappointing figure in Global Cyber Security Index. Moreover, this awareness can lead the Government to maintain the privacy and security of users on the IoT landscape. Some of the implications of lack of proper IoT security are discussed below:

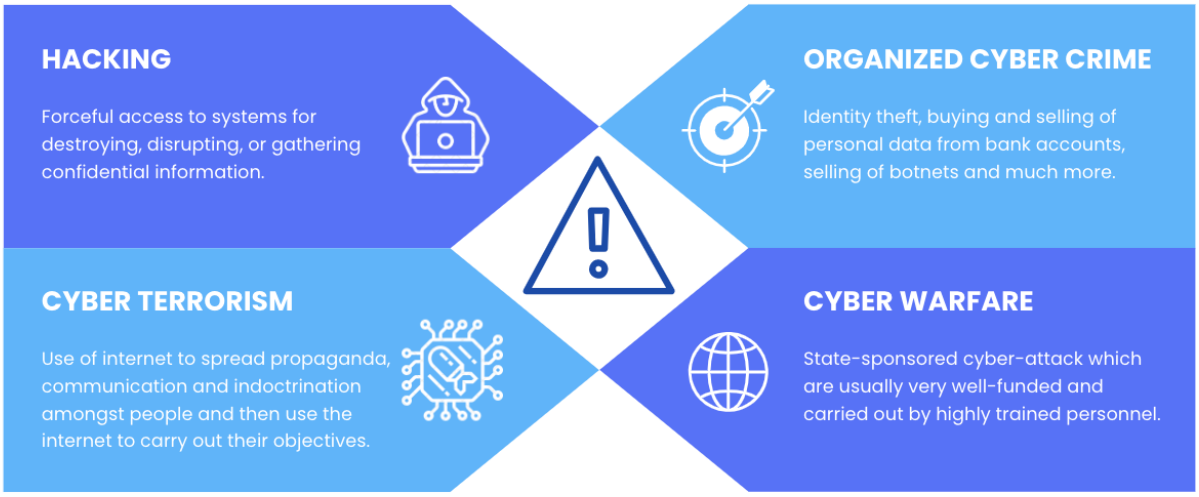

Figure 5: Major Threats to IoT Ecosystem in Pakistan

2.3.1 Hacking

Forceful access to systems for destroying, disrupting, or gathering confidential information is the biggest cyber security threat today. The types of hackers can vary in their motivation and skill levels. Some hack others merely for fun, petty theft and sometimes revenge or they can be fueled by bigger agendas like ideological or political reasons or state sponsored agendas. In terms of motivation, hackers may be seen as those

who hack for themselves or activism, or those who are doing it for criminal purposes, or those who are sponsored by the states. IoT devices manufactured without proper security considerations are highly vulnerable to getting hacked and misused, from individual homes to other setups such as hospitals or state institutions, if an IoT device is hacked the hacker can gain access to a lot of confidential data and use those devices to infiltrate further into the networks being used. During an 'Insiders on cyber-security' session at Davos, it was pointed out that new technology is making things a lot easier for hackers – webcams and other IoT devices can be very easily weaponized to bring down large portions of the internet.

2.3.2 Organized Cyber Crime

With the world moving towards digitalisation of financial and commercial activity, it has created a huge window of opportunity for organised and skilled criminals to operate using cybercrime. The internet's black market or Dark Web is seething with a variety of cyber crimcyber-criminal activity such as identity theft, buying and selling of personal data from bank accounts gained through compromised devices, selling of botnets and much more. Real world organized crime has effectively moved to the digital world as well and in this scenario, it has become increasingly necessary to implement an efficient IoT security policy on a national level to mitigate the threats posed by these criminals.

2.3.3 Cyber Terrorism

Cyberspace provides ideologically like-minded individuals with a platform to band together and plot politically or otherwise motivated terrorism, since it is an easily accessible medium, it is much easier for individuals to adopt this platform as compared to the traditional outlets. [27] Such individuals use the internet to spread propaganda, communication and indoctrination amongst people and then use the internet to carry out their objectives as well. IoT devices are a very easy medium for them to exploit for their objectives as it does not require them to be present on ground to carry out terrorist activities. Post anti-terrorist operations in Pakistan, the physical space for miscreants has diminished greatly and they are resorting to the cyber space for their objectives. They are also known to use drones, controlled IEDs and other similar devices to carry out terrorism activities. [28]

2.3.4 Cyber Warfare

Cyberwarfare refers to the state-sponsored cyber-attack which are usually very well-funded and carried out by highly trained personnel. [29] States have political and strategic motivations behind such cyber-attacks. Owing to Pakistan's unique geopolitical location and role in international affairs it is a prime target for such cyber-attacks. In today's world where traditional man to man wars have become obsolete, the cyberspace is being strategically used to replace old school military attacks. This cyber warfare first destroys key infrastructures to facilitate a physical or cyber attack on a strategic target. IoT devices can be one of the major weak links during such attacks [30]. For example, in 2007, Israel shut down Syria's air defence capabilities using a cyber-attack and launched an air strike on a nuclear reactor in the country, without being detected. Similarly, in 2008, Russia allegedly made strategic use of cyberspace in the midst of its conflict with Georgia over South Ossetia.

2.4 Risks Due to the Lack of an IoT Security Policy in Pakistan

Pakistan has no IoT security regulatory framework or policy. This means that home users and businesses are on their own to deal with IoT-related cyber security threats. [31]There are no guidelines from the government regarding purchasing or installing IoT devices. There is also no industry certification for IoT devices, leaving consumers with no way of knowing whether a particular device is safe or not. Pakistan does not have a national IoT security authority either. Instead, the Ministry of Information and Technology (MIT) is responsible for developing the country's cyber security policies and regulations. [32]

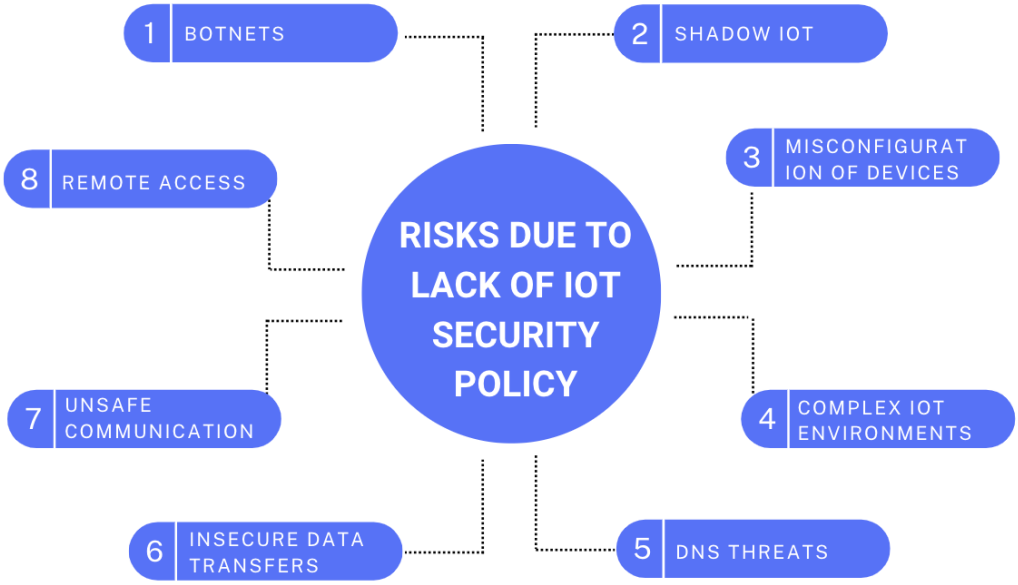

Figure 6: Risks due to lack of an IoT Security Policy

2.4.1 IoT Botnets

In 2016, an IoT botnet attack called Mirai left cyber security specialists, administrators, and IoT developers in shock [33]. Because of weak security configurations, IoT devices are more vulnerable to botnets than other devices [34]. Therefore, attackers can easily infect IoT devices with botnets through insecure and unprotected ports or psychologically exploit the users using social engineering tricks. Another alarming danger of botnet attack is that it is hard to detect. The most common use case of IoT botnets is overwhelming the resources of targeted network traffic via Distributed Denial of Services (DDoS) attacks. [35] [36]

2.4.2 Shadow IoT

Home users or enterprise administrators sometimes cannot control what devices can connect to their personal, home, or business networks. This situation creates a threat to the IoT landscape called Shadow IoT. [37] IoT devices with a valid IP address, such as wireless network printers, personal digital assistants, and fitness trackers, do not meet the security standards of organizations but can be added by various persons for assistance or convenience. IT admins or users can’t ensure the vulnerabilities of connected shadow IoT

devices due to their invisibility. On the other hand, hackers can access those shadow IoT devices to escalate the privileges and access the sensitive information of the individual user or business corporate.

2.4.3 Mismanagement and Misconfiguration of IoT Devices

According to the [38], most users tend to set default or easy passwords to their devices. Such kind of poor password hygiene and security oversights can assist malicious actors in gaining access to misconfigured or mismanaged IoT devices. The primary cause behind this cyber security threat to the IoT landscape is the lack of knowledge and capabilities for implementing the proper security measures on IoT devices.

2.4.4 Complex IoT Environments

In their research paper [39], the authors defined complex IoT environments as an interconnection of a minimum of 10 IoT devices. Such complex IoT environments are challenging to control because they have an intricate web of linked functions, especially for users with less cybersecurity-related expertise or knowledge. In such a scenario, there are more chances of overlooked configuration that can lead to dire penalties.

2.4.5 DNS Threats

In order to save cost, most organizations in Pakistan tend to use old machines that are old and not designed with the latest security standards. IoT devices connected with older machines for data collection can uncover the IoT devices network of an organization to the security vulnerabilities in older devices. Therefore, this type of connection of IoT devices with the legacy machines or organizations' servers can lead the attackers to DNS tunneling attacks. By conducting the DNS tunneling attack, adversaries can introduce spyware, ransomware, or any other kind of malicious malware inside the private network of business corporates or industries under the Government. [40]

2.4.6 Insecure Data Transfer

IoT devices have limited resources, i.e., power, processing, and storage capabilities. Thus, it is hard to implement complex encryption standards and other security standards on IoT devices. Therefore, data transferred by IoT devices in plain text format is insecure and prone to Man in the Middle attacks. [41]

2.4.7 Unsafe Communication

Many unregulated IoT devices do not encrypt their communications with their networks. This is one of the major IoT security challenges. We need to ensure that communication between devices and cloud services is secured via encryption as communication channels that are unencrypted are very easy to compromise and can leak important data.

The best practice is to use transport encryption and use of international standards like TLS. Isolating devices by using different networks also helps to create a secure and private communication channel, which keeps the transmitted message secure and confidential.

2.4.8 Remote Access

Documents released by WikiLeaks revealed that the CIA had been hacking into IoT devices and turning the camera/microphones on without the knowledge of the owners. The possibility that organizations can gain access to and record all activity on a personal device is terrifying revelation and can be a great threat to national security if the compromised device belongs to any remotely important individual.

The documents pointed to vulnerabilities in both Android and iOS, which means not just official organizations, but other criminals can also take advantage of these vulnerabilities and carry out crimes.

Chapter 3

Literature Review of Existing Standards

This chapter discusses literature review in detail. It presents work done so far related to IoT security locally and globally.

3.1 NIST Cybersecurity for IoT Program

NIST has an extensive IoT security program that sets forward in-depth security guidelines for all kinds of IoT devices. The NIST IoT cybersecurity programme helps create standards, guidelines, and other tools to improve the security of IoT devices, products, and environments. With government, industry, international organisations, academia, and consumers, the programme seeks to build trust and create a global environment conducive to innovation. This program was studied to get an idea about the international best practices in IoT security so that key takeaways can be applied to Pakistan's National IoT Security Policy that is proposed later in this dissertation.

3.1.1 NISTIR 8259 Series

NISTIR 8259 recommends cybersecurity guidelines that manufacturers should adhere to before they sell their IoT devices to customers. The IoT Cybersecurity Improvement Act of USA states that government agencies shall only obtain or use IoT devices that comply with NISTIR 8259 guidelines. [42]

The NISTIR 8259 series is a series of reports providing guidance for manufacturers and other third parties as they conceive, design, develop, test, sell, and support IoT devices. The series consists of three final documents and one draft document. Final documents being:

- NISTIR 8259: *Recommendations for IoT Device Manufacturers: Foundational Activities* (May 29, 2020)
- NISTIR 8259A: *Core Device Cybersecurity Capability Baseline* (May 29, 2020)
- NISTIR 8259B: *IoT Non-Technical Supporting Capability Core Baseline* (August 25, 2021)

3.1.2 SP 800-213 Series

The IoT Cybersecurity Act of 2020 states that NIST is responsible for publishing guidelines for federal agencies about “the appropriate use and management of [IoT] devices” that are connected to information systems in the government. The RMF (Risk Management Framework) remains the fundamental security guidance for federal systems, including IoT devices. It applies to IoT technology as much as to any other communications or operational technology. The RMF publication, the NIST Cybersecurity Framework, and SP 800-82, SP 800-181, and other relevant standards must be adhered to when selecting, acquiring, deploying, and using IoT technology in federal agencies. NISTIR 8228 provides assistance in applying present guidance to IoT, demonstrating how many unique issues are involved in IoT.

3.1.3 Consumer IoT Products

NIST is contributing to the multi-pronged response to Executive Order 14028, which directs NIST to work on several subjects. In order to fulfil this obligation, NIST worked on consumer IoT device security, developing and releasing a draft baseline security criteria. On October 18, 2021, NIST released a draft white paper for public comment. NIST received more than 400 comments during the comment period. On December 3, 2021, an updated white paper was released, followed by a workshop on December 9.

3.1.4 Takeaways

The IoT Cybersecurity Program charter was issued at the end of 2016 to help safeguard connected products and the environments in which they are used. Standards, guidelines, and other tools can be used to improve IoT cybersecurity. Government, industry, international bodies, and academic institutions will be consulted to achieve this goal. Globally, trust and innovation environments will be developed in order to foster trust.

The IoT Cybersecurity Program will work towards the development of guidelines, standards, and other tools that can be used to improve IoT cybersecurity. It will also explore ways to establish a more secure environment for connected devices, systems, and services. Collaboration between government, industry, and academic institutions will be fostered in order to advance innovation. The Program will create a framework that can be used by stakeholders to evaluate the risks and benefits of connected products. It will also develop and publish best practices that can be used by stakeholders to mitigate risks. The Program will be managed by the NSTC to ensure continuity and coordination.

3.2 IEEE Internet of Things (IoT) Security Best Practices

IEEE has a whitepaper on IoT security which lays down guidelines and best practices for everyone to follow. These guidelines were studied in detail so that relevant portions can be cherry pick and molded to be included in Pakistan's IoT security policy going forward in the thesis. [43]

3.2.1 Introduction

This paper provides Internet of Things (IoT) security guidelines that are well investigated and also outlines the best practices for others to use as a basis for future standards, certifications, laws, policies, and product ratings globally. This paper concentrates on security measures that are either specific to the IoT industry or particularly significant to the it, although they would apply to any Internet-connected device. It supposes that security features are part of the network in the Internet end-to-end processing model, where they are managed by end nodes, client, and server hardware. These guidelines state that manufacturing designs should include security mechanisms by design, such as patching and updating.

The IEEE Internet Initiative, ETAP Forum on Internet Governance, Cybersecurity, and Privacy recently released a study about security concerns with the Internet of Things. In 2015 and 2016, ETAP hosted conferences in Israel, China, India, and the United States, among other countries. Security issues with the IoT were discussed frequently in these gatherings. In this paper, we suggest methods for improving the security of IoT devices. While the recommendations in this paper are meant to be implemented by manufacturers of IoT devices, they may also be understood by non-technical, well-educated lawmakers, corporate and governmental policymakers, and standard-setting participants.

3.2.2 Best Practices

There are many best practices papers targeted toward similar audiences as the IEEE. The IEEE studied suggestions from all of these sources when preparing this list. This paper details a list of widely-accepted security techniques which may serve as a basis for creating future security standards anywhere in the world. It highlights practices which might it found most relevant to IoT security and which might encourage standards and policies that improve IoT security. The Best Practices section is divided into three parts: securing devices, securing networks and securing the overall system.

3.2.2.1 Securing Devices

What many people do not realize is that everything that is connected to the Internet is vulnerable to cyber-attack. While most IoT devices are relatively low risk, they can still be used as entry points for hackers to get into your network and wreak havoc. This section proposes the following security suggestions:

1. Make hardware tamper proof
2. Ensure provision of firmware upgrades and patches
3. Perform dynamic testing of devices
4. Specify procedures to protect data when getting rid of devices

3.2.2.2 Securing Networks

IoT devices are not just standalone devices, their security depends on the entire network. The security of an IoT device largely depends on the network it is connected to. The network may be public or private. In a public network, you have no control over who has access to data travelling on that network. Thus, you must secure your devices against potential threats on public networks. Hence this section proposes:

1. Use of strong authentication
2. Use of strong encryption and secure protocols
3. Minimization of device bandwidth
4. Network segmentation

3.2.2.3 Secure the Overall IoT System

An IoT system is only as strong as their weakest link. Therefore, it is necessary to secure them all the way from their inception. This leads to better monitoring and control. It is also necessary to design them in a way that minimizes the potential for hacking or data breaches. This helps to avoid situations where one breach may lead to other breaches and cause irreparable harm. In order to do so, we mist

1. Protect sensitive information
2. Encourage ethical hacking to find out vulnerabilities
3. Setup an IoT security and privacy organization

3.2.3 Takeaways

I found this to be most comprehensive and detailed document on IoT security policies and the most relevant for use as a baseline for a national IoT security policy. It covers all

the aspects necessary to be taken into consideration when drafting a policy for a whole IoT environment. It provides a detailed overview of the main tasks to be completed and the key areas to be considered. It can be used as a reference document for all stakeholders involved in the process of drafting a policy. The policy template is structured in a way that makes it easy to adapt to the specifics of your organization. It comes with a checklist that can be used to make sure that the policy covers all the necessary aspects. The national policy proposed ahead covers all the suggestions stated in this document.

3.3 ACM Statement on Internet of Things Privacy and Security

The ACM U.S. Public Policy Council and ACM Europe Council Policy Committee jointly released a statement on IoT privacy and policy in 2017. As the IoT ecosystem grows globally, its wide range of functions and components are posing significant privacy and security challenges that really need to be addressed. The data collected by IoT devices and algorithms that use this data for decision-making may result in dangerous consequences if left unattended. The uniqueness of IoT also presents new security and privacy concerns, making it important to incorporate privacy and security controls into the life cycle of IoT devices themself. The principles given in this statement provide an baseline for addressing privacy and security challenges in the IoT ecosystem.

From product design through decommissioning, IoT devices must be designed with privacy and security in mind and meet GDPR standards. Authentication, integrity, and authorization are vital to maintaining privacy and security throughout the device lifecycle. Additionally, IoT devices must be able to be updated and patched as needed to remain compliant with new regulations or to fix security vulnerabilities.

1. Support privacy and security in all steps of the IoT device life cycle from manufacturing to disposal
    a. Address privacy and security risks throughout the IoT device life cycle
    b. Ensure continuous, reliable device operation
    c. Provide regular patches, upgrades, and software updates:
    d. Consider issues with abandoned, discarded, and old legacy components
2. Develop new technologies to support IoT privacy and security
    a. Support flexible access control
    b. Leverage advances in cryptography and cybersecurity
3. Protect consumer data through ownership and encryption
    a. Address data ownership
    b. Build consumer awareness
    c. Protect data integrity
4. Encourage cooperation among all stakeholders
    a. Foster an interdisciplinary approach to trust
    b. Encourage managed and coordinated efforts between stakeholders

3.3.1 Takeaways

This is an old statement from 2017 and does not have in depth considerations about the current IoT landscape. The IEEE document covers the same points as this statement in much more detail. However, it shows that the concerns for IoT security are not new and have been around for some time. Now, it is high time to address these concerns with proper research and standards.

3.4 GSMA IoT Security Guidelines

The GSMA is a global organisation uniting the mobile ecosystem to discover, develop and deliver technology and bring business, environmental and societal change. It has released a set of documents meant to act as best practice guideline ensuring secure design, development, and deployment of IoT services, and to provide a mechanism to evaluate security measures.

The set of GSMA security guideline documents is meant to assist the fledgling "Internet of Things" industry in recognising IoT security issues. These documents provide a method for creating secure IoT Services in order to guarantee security best practices are adhered to throughout the service's life cycle. The documents discuss how to address common security risks and issues in IoT Services. The goal of the Internet of Things Security Guidelines document set is to provide the implementer of an IoT technology or service with a set of design guidelines for building a secure product.

3.4.1 Recommendations For Mobile Devices

The GSMA security guidelines proposes the following recommendations for mobile devices:

- Implement of an endpoint Trusted Computing Base. A TCB is a hardware, software, and protocol suite that enforces computer system security policies. It is a crucial part of an endpoint. The trusted certificate stores and processes cryptographic secrets such as pre-shared Keys (PSKs) and asymmetric keys.
- Devices that have user interfaces must be capable of managing passwords effectively. Ensure that default or hard-coded passwords are not used.
- The device must verify the integrity of its own platform and authenticate the identities of its peers using trusted certificates.
- Anomalies in behaviour must be detected by modelling endpoint behaviour in IoT security. To detect hacked devices, certain behaviours must be recorded.
- Attackers may gain unauthorized access to a connected object by attacking the device's hardware or software. To ensure the connected object's robustness, both its hardware and its software must be resistant to attack.

Ensuring secure communication between devices and the internet. The simplest method to compromise a terminal is through tampering with its communication channel. Therefore, terminal designers must guarantee communication security.

3.4.2 Recommendations For Mobile Services

For mobile services, the recommendations given by the GSMA are:

- It is crucial to establish a public systems safety in order to guarantee infrastructure reliability, data confidentiality, and integrity. In order to accomplish this, infrastructure must be resistant to DDoS attacks, redundant, and protected by firewalls.
- It is not sufficient to isolate targeted servers or computers if an attack occurs, but rather it is important to know how to react and how to defend against the problem. To do so, the organizations must be able to identify the source of the attack, repair the system, and distribute patches across the entire infrastructure.
- It is critical for an organisation to establish an incident response process in case of an attack. In addition to isolating the servers or targeted computers, the organisation must be able to diagnose the source of the attack, fix the system, and distribute patches across the entire infrastructure.
- A proper cryptographic architecture must be managed in order to assure the security of the Internet of Things. All devices participating in the Internet of Things must utilise encryption, regardless of their role or importance.
- Anonymity should not be allowed on any given platform. In order to guarantee the security, privacy, and availability of communications, a centralized certificate authority should be set up to issue certificates of trust between the different parties. Ephemeral encryption keys should also be generated so as not to jeopardize communications encryption in the event that a certificate is broken in the future.
- Before a server can be deployed in a production environment, it must be defined, configured, customized, and deployed. The objective of this procedure is to deploy secure servers, ready to defend against possible assaults.

3.4.3 Recommendations For Networks

For network security he GSMA recommends:

- Ensuring identification and authentication. Gateways, devices, terminals, home networks, and roaming networks involved in the IoT must be properly identified in order to ensure authentication. Authentication relies heavily on identity, and therefore it is crucial that these entities are properly identified.
- The network for the IoT service must be safeguarded against data and communication security breaches. Security and privacy of information stored in the network must be guaranteed. Firewalls, prevention technologies, and data filters must be used to guarantee network resource availability and defend against attack.

The goal of all these recommendations is to maintain a secure IoT ecosystem by establishing a repository of best practices for each IoT object.

3.5 ENISA: Baseline Security Guidelines for IoT

The study 'Baseline Security Recommendations for IoT' by ENISA, in the context of critical information infrastructures' is designed to provide a foundation for future IoT security initiatives in Europe. It is intended to serve as a reference point in the field.

The Report will apply to software developers, platform designers, and IoT integrators, as well as to personnel, infrastructure outages, unintentional damages, physical attacks, legal issues, failures/malfunctions, and malicious or abusive activities. A comprehensive list of IoT security concerns has been created, which categorizes the most significant dangers into the following groups: personnel, outages, unintentional damages, physical attacks, legal issues, failures/malfunctions, and malicious activities. Some scenarios include:

- Embedded devices with insecure credentials—users may choose default or create insecure credentials that would be collected by hackers when scanning for exposed devices—may lead users to be frustrated with the process of setting credentials, resulting in insecure credentials. Phishing/hacks are easy targets in this area.
- Rigid communication protocols– 'man-in-the-middle' attacks on software-based interfaces are possible if they are inflexible, preventing users from applying additional security measures.
- Unsafe software dependencies in cloud services – Cloud services' insecure software dependencies—developers frequently rely on existing dependencies to provide functionality to their software, saving time. These dependencies may not always be updated or checked for potential vulnerabilities; thus, attackers may exploit these outdated components.

3.5.1 Recommendations and Best Practices

The Report outlines the following recommendations and best practices considering the issues mentioned above:

- **Security by design** – Security should be built into the design of an IoT system across all phases of device/application design and development, in addition to a variety of security policies. Penetration testing should be performed on IoT hardware to ensure that tests and penetration tests are performed.

- **Development of security measures for IoT sSDLC:** ‘People’, ‘Processes’, and ‘Technologies’
    - **People:** Having a security culture (determining security roles and privileges, separating duties, monitoring and responding to security incidents, etc.) is just as important as providing training and raising awareness to keep up to date with security matters.
    - **Processes:** Establishing a control access and authorisation policy, defining security metrics, adopting maturity models, and adopting sSDLC methodologies are all part of ensuring secure deployments. Risk assessments, threat modelling, and other security design considerations are all included.
    - **Technologies:** It is important to ensure secure storage of users' credentials, as well as up-to-date patches for third-party software, secure communications and coding (such as secure logging and white-listing), sSDLC infrastructure, and security reviews and contingency planning, among other things.

3.6 Comparative Analysis

Measures	NIST	IEEE	ACM	GSMA	ENISA
Policy measures	✓	✗	✗	✗	✗
Baseline security recommendations for government procurement	✓	✗	✗	✗	✗
Recommendations for commercial devices	✓	✓	✓	✓	✓
Make hardware tamper proof	✓	✓	✓	✓	✓
Ensure provision of firmware upgrades and patches	✓	✓	✓	✗	✓
Perform dynamic testing of devices	✓	✓	✗	✓	✓
Specify procedures to protect data when getting rid of devices	✓	✓	✓	✗	✗
Use of strong authentication	✓	✓	✓	✓	✓
Use of strong encryption and secure protocols	✓	✓	✓	✓	✓
Minimization of device bandwidth	✗	✓	✗	✗	✗
Network segmentation	✓	✓	✓	✓	✗
Protect sensitive information	✓	✓	✓	✓	✓
Encourage ethical hacking to find out vulnerabilities	✗	✓	✗	✗	✗
Setup an IoT security and privacy organization	✓	✓	✗	✗	✗
Security by design	✓	✓	✓	✗	✓

Table 1: Comparative Analysis of International Standards and Policies

3.7 Best Practices Derived from International Standards

Following are the key best practices derived from all the studied international studies:

3.7.1 Secure Device Firmware and Hardware

What many people do not realize is that everything that is connected to the Internet is vulnerable to cyber-attack. While most IoT devices are relatively low risk, they can still be used as entry points for hackers to get into your network and wreak havoc. This section proposes the following security suggestions:

1. Make hardware tamper proof
2. Ensure provision of firmware upgrades and patches
3. Perform dynamic testing of devices
4. Specify procedures to protect data when getting rid of devices

3.7.2 Secure the Entire IoT Network

IoT devices are not just standalone devices, their security depends on the entire network. The security of an IoT device largely depends on the network it is connected to. The network may be public or private. In a public network, you have no control over who has access to data travelling on that network. Thus, you must secure your devices against potential threats on public networks. Hence this section proposes:

1. Use of strong authentication
2. Use of strong encryption and secure protocols
3. Minimization of device bandwidth
4. Network segmentation

3.7.3 Secure the Overall IoT System

An IoT system is only as strong as their weakest link. Therefore, it is necessary to secure them all the way from their inception. This leads to better monitoring and control. It is also necessary to design them in a way that minimizes the potential for hacking or data breaches. This helps to avoid situations where one breach may lead to other breaches and cause irreparable harm. To do so, we must:

1. Protect sensitive information
2. Encourage ethical hacking to find out vulnerabilities
3. Setup an IoT security and privacy organization

Chapter 4

Analysis of IoT Strategies of Different Countries

4.1 Introduction

This chapter discusses cyber security policies and efforts to secure the IoT ecosystem of different countries. The selected countries and their GCI (Global Cyber Security Index) [44] ranks are as following:

- United States of America (1 – currently leading the table)
- United Kingdom (2)
- Russia (5)
- India (10)
- China (33)
- Israel (36)

The primary motivation behind this related work review is to determine the shortcomings of Pakistan in securing its IoT ecosystem as compared to other countries in the region or those which are geopolitically relevant to Pakistan's security as well as with countries that have a high GCI score. This review of various cyber security policies and steps toward secure IoT ecosystems will help us formulate our own. These nations have different approaches to cyber security and have adopted different policies and strategies to secure the IoT ecosystem. The United States has adopted a federal risk-based approach, while other countries such as China have adopted a risk-management approach. India has adopted a public-private partnership model to improve cyber security. China has adopted an active defence strategy to protect its cyberspace. Russia has adopted a national strategy for cyber security. [45]

If we look at the current scenario, it is quite evident that the IoT is ushering in a new era of technological development in every country. It is also a fact that each country is keen to reap the maximum benefits from the IoT. However, it is equally important that the IoT ecosystem is secured from cyber threats. This chapter attempts to explore the steps being taken by different countries to secure their IoT ecosystems. It also discusses the status of

IoT regulatory framework in different countries. We will also discuss the challenges faced by the IoT ecosystem and how they can be resolved. Finally, this chapter also touches upon the role of AI, blockchain, and other emerging technologies in securing the IoT ecosystem.

4.2 IoT Security Policies of the USA

4.2.1 IoT Security Suggestions from the US Dept of Homeland Security

For developing, improving, and securing the IoT-based infrastructure in the United States, the US Department of Homeland security (DHS) plays a vital role in the US [46]. They used their expertise in critical infrastructure protection and cybersecurity to perform the challenging jobs of securing the IoT infrastructure. DHS is considered the most important specific sector agency in the US that strongly focuses on securing the infrastructure and providing the safety to the public from the different kinds of unauthorized and malicious cyber activities. The IoT offers different cybersecurity ways, mission areas, and IoT-based critical infrastructure. [47]

Some specific strategic rules and principles are proposed by the department of Homeland Security (DHS) that clarify four lines of effort for securing the IoT infrastructure by the US Government [48]. These four lines of effort are:

1. Firstly, encouraging the different agencies and the Federal Government departments to collectively work with the various IoT-based stakeholders to determine the different ways the security of the IoT infrastructure is mitigated. They jointly work to provide the different methods and mechanisms through which IoT security can be enhanced and provides an understanding of the IoT risks, promoting different mechanisms and principles to reduce these IoT security risks and providing the best approaches and practices to improve IoT security in the future.
2. Secondly, in trying to enable the IoT-based stakeholders to be aware, it must be necessary to know the different types of the IOT security risks to find and efficiently correct them easily. Department of Homeland Security (DHS) will use various platforms and mechanisms to provide awareness about the IOT security risks through training, private sectors, education, and with the help of international agencies and partnerships.
3. IOT Stakeholders, policymakers, and legislators must find the latest mechanisms to improve and enhance IoT security. DHS, with the help and cooperation of all other

IoT stakeholders and partners, discusses these IoT security risks and finds different ways to overcome the various issues through regulation, cyber insurance, different standards-setting initiatives, legislation, and the many other mechanisms to improve the IoT security in the US.

4. The DHS must show its contribution to various international standards to develop the different IoT security processes. To promote IoT security, development, and innovation, the US Government must engage the private sector organizations and various internationally connected partners to work together and support the development of the international standards for IoT security.

4.2.2 IoT Cyber Security Improvement Act of 2020

The US govt is a very big customer of IoT devices, much bigger than many may think. From IV pumps to veterans to water pollution sensors for the Environmental Protection Agency, there are countless IoT devices in govt use. This large number of officially used IoT devices is an enticing target for hackers of all sorts from individual hackers to state sponsored individuals as well. [49]

To protect all these devices and their data the the U.S. govt passed a cybersecurity law in December 2020. The "IoT Cybersecurity Improvement Act of 2020" is a framework that will influence IoT security in the country and across the world.

The IoT Cyber Security Improvement Act of 2020 would require the Department of Homeland Security to publish a list of software and hardware vendors that are found to be non-compliant with the Federal Government's Cyber Security standards. The list will be published every six months and will act as a blacklist. This would require vendors on the list to undergo a review of their software and hardware products by the DHS. Vendors will also be required to submit a remediation plan to the DHS that details how they will make their products compliant with the Federal Government's Cyber Security standards. This bill has been referred to the House Committee on Homeland Security and the House Committee on Energy and Commerce but has not yet been voted on.

4.2.2.1 Key Features of the IoT Cyber Security Improvement Act of 2020

The Act was formulated to reduce the risk to the federal government generating from insecure IoT devices by establishing minimum security requirements for connected devices under use by the government. Below we highlight the major requirements outlined in this act:

- The National Institute of Standards and Technology (NIST) will be required to publish standards and guidelines on the use and management of IoT devices by the federal government, including minimum information security requirements for managing cybersecurity risks associated with IoT devices.
- The Office of Management and Budget (OMB) was directed to review federal government's information security policies and make any required changes to ensure they are in line with NIST's official recommendations.
- NIST and OMB will be required to update IoT security standards, guidelines and policies at least once in every five years.
- Stop the procurement of IoT devices by the federal government that do not comply with the above stated security requirements, this prohibition will be however, subject to a waiver process for devices deemed necessary for national security, needed for research or ones that are secured using alternative effective methods.
- NIST will be required to publish guidelines for reporting of security vulnerabilities relating to federal agency information systems, including IoT devices.
- Also, direct OMB to develop and implement policies that are necessary to address security vulnerabilities relating to federal agency information systems, including IoT devices, consistent with NIST's published guidelines.
- Contractors providing IoT devices to the U.S. government will be required to adopt coordinated vulnerability disclosure policies, so that if a vulnerability is uncovered, that information is duly disclosed.

4.3 IoT Security Policies of UK

IoT security continues to remain a problem worldwide including UK. According to Kaspersky, it's getting worse: there were 1.5 billion breaches of IoT devices during the first six months of 202, this is almost double the 639 million for all of 2021. This is largely because IoT security has long been an afterthought for everyone in the landscape. As more IoT devices are being connected in the workplace, they become a potential entry point for cybercriminals. If a hacker can breach the security of a device, they have access to everything it controls. This could lead to high-risk scenarios, such as a hacker accessing the controls of a manufacturing plant's computer system and halting production. This is why it is important for businesses to consider IoT security when purchasing new devices for their workplace. By implementing some basic security measures, such as setting up a strong password on the device, businesses can reduce the risk of a breach.

4.3.1 Product Security and Telecommunications Infrastructure (PSTI) Bill

To improve the security for consumer IoT devices in the U.K. the government introduced a Product Security and Telecommunications Infrastructure bill (PSTI) in Parliament, it is a legislation that states guidelines for IoT manufacturers, importers, and distributors to adhere to.

The bill outlines three key points for security. The first is a ban on easy to guess default passwords. These passwords are often used by devices in factory settings and are easily guessable. The second point mandates manufacturers to provide a public point of contact to make it simpler for anyone from the public to report a security vulnerability. Lastly, it requires that all IoT manufacturers will also have to keep customers updated about the minimum amount of time for which a product will keep on getting latest security updates.

Compliance is also a major factor in proposed bill. Under this bill device manufacturers, importers and all other associated parties will be required to show compliance statements to demonstrate their adherence to security requirements. If they fail to do so, manufacturers, importers, distributors, and retailers will have to report their failure to the relevant authority and take immediate action to remedy the failure. Otherwise, they will not be allowed to sell.

4.3.1.1 Product Security Measures

The first part of the bill proposes product security measures that will:

- Provide government officials with the ability to specify and amend minimum security requirements for consumer products.
- Enforce manufacturers, importers, and distributors to comply with the security requirements.
- Provide powers to allow breaches to be reported and acted against.

4.3.1.2 The Telecommunications Infrastructure measures

The second part 2 of the bill will apply to all parties involved in requests and agreements related to the rights regulated by the Electronic Communications Code of UK. This includes all telecommunications operators, infrastructure providers, landowners and occupiers, as well as professionals like land agents and legal representatives. This part of the bill states:

- Make changes to the already existing Electronic Communications Code to provide the legal reforms to support the government's roadmap to achieve national rollout of 5G networks.
- Encourage negotiations for agreeing upon new and editing of existing agreements requiring telecoms operators to the use Alternative Dispute Resolution ('ADR') instead of legal proceedings in cases where there are disagreements on terms.
- Prior to the 2017 Code reforms, operators were limited to upgrading and sharing equipment on private land. These limitations have been removed, with certain exceptions, to enable operators to share equipment installed before the Code reforms.
- There should be a consistent and equal approach to renewing expired agreements and creating new ones across the UK, enabling operators with existing apparatus to either renew their expired agreement or request a new one.
- To introduce new provisions to enable operators to obtain Code rights over certain types of land quickly if a landowner does not cooperate.

4.3.1.3 Effect on Businesses

The PSTI will have a significant effect on supply chain processes for UK manufacturers, retailers, distributors, and importers. Many connected devices are imported into the UK today, so retailers, distributors, and importers will have to ensure that their suppliers meet the Bill's requirements—which may be in place later this year, with a one-year grace period.

4.4 IoT Security Policies of Russia

4.4.1 Minkomsvyaz Study on Security of IoT

On June 8, 2019, the Ministry of Digital Development, Communications, and Mass Media of the Russian Federation ('Minkomsvyaz') announced a study on the IoT and other cyber-physical systems to resist information security threats [50].

As per their study [50], primary risks to the IoT landscape of Russia are:

- The digitalization of the energy sector leads to greater infrastructure vulnerability.
- In Russian practice, there are no calculated solutions for the success of the implementation of the Internet of Things on a national scale
- The Internet of Things implies new investments, and companies need to recoup the costs already incurred
- New technologies lead to new threats to critical information infrastructure information security.

Since "smart" networks provide for the possibility of remotely limiting the supply or renewal of resources, a computer attack can de-energize a socially significant facility or an entire city. In the case of gas, the consequences can be much more tragic. Therefore, Russia highlights that ensuring maximum security of the critical infrastructure is necessary.

4.4.2 Future for IoT Security

In the future plan to secure the IoT landscape, Russia aims to solve this problem using the Ministry of Energy Ministry of Telecom and Mass Communication. Russia is planning to focus on using predominantly domestic telecommunications equipment and smart metering systems, paying special attention to the use of the Russian component base. According to Russia’s Deputy Head of the Ministry of Telecom and Mass Communication: “We are counting on the allocation of frequency bands for the wireless Internet of things and the use of secure domestic protocols in order to guarantee the stability of the functioning of the infrastructure itself.”

4.5 IoT Security Policies of India

4.5.1 National Digital Communications Policy 2018

In order to unlock the power digital communications and IoT devices the government of India released a National Digital Communications Policy in 2018 which is divided in to three parts. The third part covers the security aspect of digital communications that applies to IoT security as well. The National Digital Communications Policy aims to broaden digital access, increase privacy and data protection, and promote responsible use of digital communications. It also aims to develop the telecommunications market, promote data security and privacy, and advance public interest communications, including e-Governance. The National Digital Communications Policy has also emphasised on the need to develop standards for IoT devices. In order to prevent cyber attacks and data breaches, it is important to have a proper certification system for IoT devices. The policy aims to develop standards for IoT devices. The standards will be determined by the Government of India in consultation with experts and stakeholders. The security strategy has the following salient features:

4.5.1.1 Data Protection

This section states that legal licenses and terms wherever applicable should be amended to incorporate data protection and privacy clauses. It also states that the state should ensure that data protection and security principles are enforced and also promoted by using indigenous communication solutions and devices. The government should encourage citizens to use the state-provided communication services and devices, such as email, chat, and social media. It also says that the government must not use equipment or software that is manufactured outside India. Moreover, the state must promote the use of indigenously developed software and hardware products, instead of using imported products.

4.5.1.2 Provision of Autonomy to Citizens and Enterprises

In this section the state resolves to uphold principles of net neutrality with appropriate exemptions where deemed necessary and ensuring compliance to the principles of net neutrality. With this, the state aims to provide a level playing field for all internet users irrespective of the type of service they are using. This section also allows for restriction of internet usage for the purpose of maintaining public order, preventing crime, or protecting public health. The state should also facilitate the adoption of communication

tools which are safe and secure. Data protection principles should be followed by both the state and citizens. The state must also ensure that citizens have the right to privacy.

4.5.1.3 Security of Digital Communications

This the main section of the security aspect of the policy, it proposes steps that should be taken to ensure the security of digital communication withing the country and applies to IoT devices as well. The main suggestions in this section are as follows:

- Fix security issues across different physical layers
- Develop and implement comprehensive security standards for equipment and devices
- Participation in global standard setting organisations
- Implement and strengthen security testing processes by enhancing capacity to perform testing and establishing comprehensive security certifications based on international standards
- Formulating a policy for encryption and data retention based on international best practices
- Facilitating safety of citizens by introducing interception capabilities in government and increasing awareness about security issues in the general public.
- Establishing a Security Incident Management and Response System for Digital Communications Sector

4.5.2 Code of Practice for Securing Consumer Internet of Things (IoT)

The Telecommunications Engineering Centre (TEC) of India has released a "Code of practice for securing consumer internet of things (IoT)" in 2022 as baseline for IoT device security in the country. The code is aligned with global standards and best practices. The purpose of these guidelines is to secure the IoT ecosystem and manage vulnerabilities. The code is meant to be used by IoT device manufacturers, service providers and application developers to create a secure and productive IoT ecosystem. It is created to ensure that IoT devices and endpoints comply with safety and security guidelines to protect users and networks connected to these devices.

4.5.3 IoT Ecosystem Development Initiatives

The Government of India has allocated a budget of Rs.7060 billion for developing almost 100 IOT-based smart cities in India [51]. In the future, this will lead to a quick and

massive increase in the development of the IoT field in India. Another good step taken by the Government to boost the IoT industry in India is the Digital India Program which will helps to transform the knowledge and the digital empowerment of the Indian society. The initiatives of the Digital India program and the concept of smart IoT-based cities will help improve India's IoT-based technological infrastructure.

For developing the IoT-based ecosystem in India, a detailed draft for IoT-based policies has been formulated [52]. That draft includes different supportive and essential methods and mechanisms that will improve the strength of India in the global service industry. According to the policies mentioned in the draft of the IoT policy [52], there are numerous standards in the IoT-based technologies that India developed. Multiple standards were globally well known, and acceptable related to the process, services, and technology and are like:

- Maintaining the safety and security standards of IoT devices
- Standardizing the IOT technologies
- Developing the Energy consumption standards
- Developing the standards for could communications and outside the cloud communications
- Maintaining the international quality-based standards for creating and tracing
- Providing data integrity, data privacy, data security, and integrity standards
- Using good standards for the protocols of spectrum energy communication

4.6 IoT Security Policies of China

4.3.1 MIIT Guidelines for Security Standard System for IoT

The Ministry of Industry and Information Technology (MIIT) in China publicly released a draft on the "Guidelines for Building Basic Security Standard System for the Internet of Things" on January 15, 2021 to gather public opinions till February 14, 2021 [53]. That open draft received many public suggestions and opinions. After which the Chinese government made updates based on the feedback and formally released the guidelines on 25 October 2021.

Implementation of Guidelines

The primary purpose of this was to design and develop the basic standards for IoT technology. This design was proposed to be implemented in two stages:

1. Almost 10 IOT industry-based standards will be drafted in 2022, and the system will be established according to their specifications, specifying the cleared security requirements in the draft.
2. And having the expectations that more than 30 IOT industry-based standards will be drafted in 2025 would lead to improving the IoT-based cross-industry applications security level.

Proposed Standards and Guidelines

The policy guidelines identified five major areas for standards that needed to be developed and implemented for effective IoT security implementation. Some of the basic IoT-based security standards like the security of gateways, platforms, and IoT terminals are mentioned in this draft and the essential security standards [53]. It also highlights the five most critical security-based standards for IoT systems, which are:

- Security of gateways
- Security of platforms
- Security management
- Security of the terminals
- General security requirements

The directions to follow and the areas for the key standardization are provided to these IoT-based security standards that can be explained as follows:

4.6.1.1 General Security Standards

The general security standards contain the basic security terminologies like Classification of security, security scenarios, integration of protection, security protocols, architectural security models, and application security standards and provides all basic guidelines for the basic IoT-based systems. The following are the highlights of this standard:

- Definition of basic IoT security terms
- The basic IoT security architecture model
- Basic IoT security scenarios
- Basic IoT security classification and application
- Basic IoT security protocol

4.6.1.2 Terminal Security

Terminal security maintains the security of the modules, security of the cards, general security of all terminals equipment, industry terminals and terminal testing, different evaluation standards, and maintaining the security for communication chips and all other measures that apply to the IoT-based security systems. The following are the highlights of this standard:

- Card security
- Module security
- Communication chip security
- General security of terminal equipment
- Industry terminal security
- Terminal test evaluation

4.6.1.3 Gateway Security

It involves the security related to the processing and exchanging the data between different IoT-based gateway devices, security of the physical environment of the gateways, different gateway components security, interface and the gateway communication security, gateway evaluation, and gateway testing. The following are the highlights of this standard:

- Gateway equipment security
- Gateway data exchange and processing security
- Gateway communication and interface security

- Gateway physical environment security
- Gateway component security
- Gateway test and evaluation

4.6.1.4 Platform Security

This security includes the security of general platforms, the interaction between different platforms, different platform evaluations, the security of the business systems platforms, and different platform testing. The following are the highlights of this standard:

- Platform general security
- Platform business system security
- Platform interaction security
- Platform testing and evaluation

4.6.1.5 Security Management

These standards mainly guide maintaining and implementing the industry's safety requirements that involve the standards for certificate management, safety maintenance and safety management, and safety information coordination. The following are the highlights of this standard:

- Security Information collaboration
- Security management and maintenance
- Certificate management

4.6.2 China Standards Plan 2035

China officially launched the 'China Standards 2035' strategy in 2018, aiming to create a blueprint for the Chinese government and leading tech companies to set global standards for emerging technologies, such as 5G, Internet of Things (IoT), and artificial intelligence (AI). With a clear objective to make China a global leader in standards, this strategy aims to make China a standards superpower by 2035. This strategy is expected to transform China into a standards-based society, promote the development of a rules-based economy, and serve as a foundation for the country's international cooperation in standards setting. The launch of this ambitious strategy has primarily been driven by the increasing demand from Chinese industries for standards, growing demand from Chinese consumers for safer and reliable products and services, and the need to upgrade the

standards system to keep pace with the needs of the country's socio-economic and technological development.

These standards will ensure that IoT devices manufactured in China are secure and of the highest quality. The China Standards 2035 plan will likely highlight the importance of setting standards domestically, because in practice there is wide variety of ways in which policies are implemented locally. Hence the govt plans on prioritizing implementing uniform standards across the country.

The setting of such standards in different industries including IoT and IoT device manufacturing will not only allow for the creation of a secure national IoT environment but also make a China a world leader in secure IoT device manufacturing which is huge leap towards economic success in today's world since IoT adoption is the way forward to the future and the time is not far when IoT devices will be present in all areas of our life.

China has also standardized its Belt and Road Initiative and Made in China 2025 strategy in an effort to improve the quality of its standards and make them more in line with the rest of the world. China has already made significant progress towards its goal of setting internationally recognized standards in the manufacturing sector, and the rest of the world has taken note.

4.7 IoT Security Policies of Israel

In Israel, the National Cyber Directorate (INCD) was developed to provide and promote research work in the field of cyber security [54]. INCD provides research, traditional concepts, theories, and approaches to tackling the different mechanisms to improve cyber security in general including IoT security. Israel is considered the most prominent leader across the world in the field of cyber security. [55] That's just because of the INCD efforts because they promote IoT security-related activities in the country and examine the cooperation between the different multinational collaboration. INCD was assigned the tasks of maintaining cyber security and implementing a secure IoT-based environment in the country by the Government of Israel for their cyber defense [56].

For performing these tasks to maintain cyber security, the National Cyber Directorate of Israel (INCD) conducted two primary efforts, which are summarized by [57] as:

- INCD first focuses on the research and development of different cyber security mechanisms, implementations of these mechanisms, exploring different platforms for sharing knowledge and information, and finding other platforms for centralized security services and fast cyber operations.
- INCD secondly focuses on improving the base of national Science and technology in the field of cybersecurity, which is done through different educational research and industrial innovations that helps to boost the security of cyberspace environment in Israel.

4.7.1 The Corporate Defense Methodology

Cyberspace is a major part of our lives, the INCD recognizes this and released a Corporate Defense Methodology to be used by all organizations, it is applicable to all big and small corporations as well as to government organizations. The INCD developed this methodology by combining the world's leading methodologies, with Israeli civil and security experience, adaptation to Israel's environment and adjusting it to the Israeli business culture.

4.7.1.1 Tenets of the Defense Methodology

The defense methodology is very detailed and outlines the procedures that can be adopted to secure the IoT based organizations, but it has the following key tenets:

- The responsibility to defend information rests on the management

- Defense measures should be proportional to the potential that could be caused in case of an attack
- The defense should be tailored to Israeli culture and knowledge
- Proactive defense should be adopted
- Defense should be multi layered

4.7.2 Best Practice Reducing cyber security risks in video surveillance cameras

Data security and privacy concerns are at the forefront of most organizations' and customers' minds as they navigate a world where businesses operate on a global scale and data is stored electronically through IoT devices As the risk of data breaches and cyberattacks continues to grow, businesses must pay careful attention to data security and privacy considerations at every stage of the data supply chain. When sourcing third-party devices, businesses must first verify that vendors are adhering to strict security standards.

The document provides recommendations and key points that should be considered while interacting with system equipment vendors and security/low-voltage consultants who may be involved in installing or setting up video surveillance systems. The document also serves as an standards guide for system personnel responsible for the installation/setting up of these systems to ensure the security of the systems. This document can hence be considered a specialized policy for a particular IoT device which is very commonly used. It also highlights the various benefits offered by video surveillance, how to choose the right video surveillance system for your business, how to conduct a risk assessment, and how to comply with data protection regulations.

The policy takes the following aspects into consideration:

- Pre-acquisition considerations such as data protection including data profiling, data archiving, and migration. Every enterprise should have a data strategy to make sure their data is managed, protected, and leveraged to its full potential. A data strategy should include a data roadmap that outlines the company's data needs over the next one to three years. A data roadmap will also help to identify the company's data sources and use cases, as well as prioritize the data initiatives that will help achieve your business goals. In addition to a data roadmap, every

enterprise should have a device acquisition plan to make sure they are acquiring devices that will be most secure and beneficial for them.

- Before installing the camera and during maintenance processes (if the use of components with Wi-Fi is unavoidable)
- Segregating the camera in a standalone network or in a network by allocation of a dedicated segment.
- Using a segregated network. A segregated network is the safest option when it comes to data security. A segregated network is a network that is completely separated from your main network and only used for storing sensitive data. These networks are often referred to as data segregation or data isolation networks. These networks are completely cut off from your main network and only accessible by a select few people. You can set up a segregated network using either a virtual private network (VPN) or a remote access server.
- Using a dedicated VLAN (after the risk management process). Dedicating a VLAN for critical applications like voice and video has long been a standard practice, but with the increased use of software-defined networking and virtualization, companies may neglect to keep voice and video on its own VLAN.In a virtual environment, it is ideal to set up a VLAN for each application, which means that if you have a UC app on the same network as other non-critical apps, it could be negatively impacted by those other apps. For example, if you're moving data between two VMs on the same network and one is a voice app, the voice app could be negatively impacted by the data movement between the two VMs.
- Security settings for initial operation and general security settings.
- Physical security resources and prevention of access to the cameras and terminal equipment. Cameras and terminal equipment can be used to view confidential information, record meetings, or take pictures of sensitive data. For this reason, it is important to protect terminal equipment and cameras from unauthorized access. To prevent access to the cameras and terminal equipment, you can install a privacy filter or one-way mirror on the camera. It is important to keep physical access to terminal equipment and cameras secure. In addition, you can place the terminal equipment in a locked cabinet or room when it is not in use.

- Reducing cyber risk in maintenance, support and camera handling processes. As organizations move towards embracing the Internet of Things, they also have to be aware of the security risks. In fact, poor security in maintenance and support processes can actually be more dangerous than the product itself. For example, if a manufacturing process involves the handling of sensitive data, the security of the cameras and software used to stream that data also has to be guaranteed. Similarly, the maintenance of critical infrastructure, such as power stations, has to be done in a secure and controlled environment. The information collected by these systems also needs to be protected. In all these cases, a VPN can provide security and privacy for the maintenance team. It can also be used to remotely troubleshoot and monitor these systems.

4.8 Derived Best Practices

The following are the key best practices derived from the IoT policies of different countries:

1. Publish standards and guidelines on the use and management of IoT devices by the federal government, private entities and public use including minimum information security requirements for managing cybersecurity risks associated with IoT devices.
2. Conduct regular reviews federal government's information security policies and make any required changes to ensure they are in line with official recommendations.
3. Update IoT security standards, guidelines and policies at least once in every five years.
4. Stop the procurement of IoT devices by the federal government that do not comply with the above stated security requirements.
5. Publish guidelines for reporting of security vulnerabilities relating to federal agency information systems, including IoT devices.
6. Develop and implement policies that are necessary to address security vulnerabilities relating to federal agency information systems, including IoT devices, consistent with NIST's published guidelines.
7. Contractors providing IoT devices to the government will be required to adopt coordinated vulnerability disclosure policies, so that if a vulnerability is uncovered, that information is duly disclosed.
8. Fix security issues across different physical layers.
9. Develop and implement comprehensive security standards for equipment and devices.
10. Participation in global standard setting organisations.
11. Implement and strengthen security testing processes by enhancing capacity to perform testing and establishing comprehensive security certifications based on international standards.

12. Formulating a policy for encryption and data retention based on international best practices.
13. Facilitating safety of citizens by introducing interception capabilities in government and increasing awareness about security issues in the public.
14. Establishing a Security Incident Management and Response System for Digital Communications Sector.

4.9 Comparative Analysis of Different Country's Policies

Measures	USA	UK	Russia	India	China	Israel
Publish standards and guidelines on the use and management of IoT devices by the federal government, private entities and public use.	✓	✓	×	×	✓	×
Conduct regular reviews federal government's information security policies.	✓	✓	×	×	✓	×
Update IoT security standards, guidelines and policies at least once in every five years.	✓	✓	×	×	✓	×
Stop the procurement of IoT devices by the federal government that do not comply with the above stated security requirements.	✓	✓	×	×	✓	×
Publish guidelines for reporting of security vulnerabilities relating to federal agency information systems.	✓	✓	×	×	✓	×
Develop and implement policies that are necessary to address security vulnerabilities relating to federal agency information systems.	✓	✓	×	×	✓	×
Contractors providing IoT devices to the government will be required to adopt coordinated vulnerability disclosure policies.	✓	✓	×	×	✓	×
Fix security issues across different physical layers.	✓	✓	✓	✓	✓	✓
Develop and implement comprehensive security standards for equipment and devices.	✓	✓	✓	✓	✓	✓
Participation in global standard setting organisations.	✓	✓	×	✓	✓	✓
Implement and strengthen security testing processes by enhancing capacity to perform testing.	✓	✓	✓	✓	✓	✓

Table 2: Comparative Analysis of Different Country's Policies

Formulating a policy for encryption and data retention based on international best practices.	✓	✓	✓	✓	✓	✓
Facilitating safety of citizens by introducing interception capabilities in government and increasing awareness about security issues in the public.	✓	✓	✗	✓	✓	✗
Establishing a Security Incident Management and Response System for Digital Communications Sector.	✓	✓	✗	✓	✓	✗

Chapter 5

Analysis of Security Policies in Pakistan

5.1 National Cyber Security Policy of Pakistan

This section critically evaluates the National Cyber Security Policy of Pakistan. The primary motivation behind this evaluation is to highlight the policy's loopholes in Pakistan's IoT ecosystem. In light of those loopholes in Pakistan's current cyber security policy and the landscape of cybersecurity threats to the IoT ecosystem of Pakistan, the Draft of the National IoT Security Policy of Pakistan will be formulated in the next chapter of this dissertation.

5.1.2 Principles of National Cyber Security Policy of Pakistan

Before analyzing the deliverables of the National Cyber Security Policy of Pakistan, the guiding principle for achieving the objectives of the policy are highlighted below:

- Both private and public organizations are responsible for ensuring and providing cyber security to their ICT products, services, and data delivery simultaneously.
- These guiding principles will be applied to international and national standards and frameworks and provide best practices against national digital sovereignty.
- The purpose of taking all these actions is to enhance public and nationwide prosperity and provide privacy, security, and protection to citizens' online data in the digital domain.
- Protect Pakistan’s CI/ CII from cyber-attacks by taking appropriate measures against national sovereignty.
- With the help of both the private and public sectors, the Government will be responsible for providing a national response during any incidental situations.

5.1.3 Objectives of the National Cyber Security Policy of Pakistan

Overall, there are 16 objectives of the National Cyber Security Policy of Pakistan. Most of the objectives in policy are generic and can be applied to every ICT infrastructure, such as Big Data, Cloud Computing, Private and Public Networks, and Services. However, some objectives in the National Cyber Security Policy of Pakistan are specific

and require considering the functions, operations, and protocols for various ICT infrastructures and services. In this section, the objectives of the National Cyber Security Policy of Pakistan are discussed, which contains loopholes pertaining to the security of the IoT ecosystem of Pakistan.

5.1.3.1 Active Defense

Following are some of the essential actions that the stakeholders will need to take for active defense:

- Understanding and working with the IP routing mechanisms to secure the internet traffic in the Government organizations and departments. IPsec is an internet protocol for data transfer between remote sites or departments. IPsec can secure the voice, video, and data from the public networks like the Internet, private networks, and virtual private networks. It provides end-to-end security by ensuring that only the intended parties receive the information. The Government organizations and departments can use IPsec to secure their data and communications from any malicious attacks to maintain the security of their network and data.
- Detecting the malware attacks and blocking them through working with the Telecom companies and the internet service providers (ISPs). This is done by working together with the ISPs and telecom companies. ISPs are the companies that connect you to the internet. These companies can be your mobile phone provider or your cable provider. These telecom companies have a system that is called the Deep packet inspection. This system can help them to check the content of the data that is being transferred, and if there is any malicious content, then the ISP will block or throttle the connection. There are some other ways through which we can detect the malicious content. If a connection is in use for more than a set time then it can be considered as a malicious connection and can be blocked. There can be some other factors such as the volume of data, the type of data, and even the location.
- Promotion of best security practices with the help of different internet governance organizations like the Internet Governance Forum (IGF) and Asia Pacific Network Information Center (APNIC).
- Protecting the citizens of Pakistan from the different cyber security attacks by working with various international Law enforcement agencies and channels.

- In public networks, the most widely used cyber security attacks are spoofing and email phishing. Thus, it is necessary to protect these public networks.

5.1.3.1.1 Reflection

In this national cyber security policy objective, IoT device manufacturers, operating protocols, and attacks are neglected. The current description of this objective can raise the exceptions in the minds of IoT device manufacturers, distributors, and other relevant stakeholders. They can cover themselves in the shield of this description against any legal actions in the future. Internet of Things doesn't belong to individual users only. This technology covers large public-related application areas. Thus, it is an attractive target for cybercriminals and prone to various cyber threats. The active defense should be available for IoT applications and services as well.

5.1.3.2 Internet-based Services Protection

Following are some of the most critical actions that the stakeholders will take to protect internet-based services:

- Install different monitoring and security products on the Government organization's networks to ensure the correct functionality of software and services running on critical systems.
- Protect the citizens' online and offline data when sharing their confidential information among private and public organizations.
- Develop an IP reputation service in order to safeguard critical Government services. An IP reputation service will get the information related to the IP addresses connected with a particular digital service. Thus, it will help in real-time and effective risk management and response.
- In digital services, looks for domains other than gov.pk to notify the users still considering outdated technologies in their environments.

5.1.3.2.1 Reflection

Devices communicating over protocols other than Internet Protocol should also be considered in this objective of Pakistan's National Cyber Security Policy. Most IoT devices and other Low Power devices and sensors communicate over channels and protocols such as Bluetooth Low Energy (BLE), Bluetooth, ZigBee, LoRaWAN, Aloha, and so on [58]. Thus, avoiding implementing an effective security strategy for listed

protocols will make the public IoT and wireless networks more vulnerable and prone to cyber-attacks.

5.1.3.3 Regulations

This policy aims to improve the security in cyberspace. It also requires manufacturers of devices to equip them with software updates and security features. These features will secure the devices from being hacked or used maliciously. To achieve this objective, the National Cyber Security Policy of Pakistan states that relevant stakeholders, in conjunction with Government, should:

- Formulate cybersecurity-related laws, rules, and regulations.
- Standardize the network and digital forensics processes and cyber governance infrastructure in synchronization with other relevant laws such as PECA 2016 and this policy.
- Ensure the standards of Cyber Security across Pakistan.
- Empower the law enforcement agencies and legal entities in order to address the rising scope of cybercrimes.

5.1.3.3.1 Reflection

This objective of the National Cyber Security Policy of Pakistan should also emphasize the regulations related to IoT in Pakistan. Currently, no regulatory framework or law is available related to the registration, operations, protocols, bands specification, and so on for IoT devices. This situation leaves the IoT ecosystem of Pakistan unnoticed and insecure.

5.1.3.4 Establishment of Trust in Digital Transactions

This objective guides the stakeholders to maintain trust in the integrity of digital services. In order to achieve this objective, relevant stakeholders are instructed to:

- Implement the digital certifications mechanism to prove the identity and authenticity of users.
- Boost the utilization of scalable Public Key Infrastructure (PKI) to cope with modern business requirements such as e-voting, e-passports, e-governance, e-procurement, e-filling, and other electronic public services.
- Implement the multiple certification services to enhance users' trust in digital services such as Fin-tech, e-commerce, etc.

5.1.3.4.1 Reflection

As described previously, the number of interconnected IoT devices and applications is increasing daily. An IoT device has fewer resources such as power, processing capabilities, and storage than traditional computing devices. Therefore, IoT devices cannot accommodate and operate conventional security measures to ensure safe data transmission and secure digital services. Therefore, low resource-consuming data encryption and validation systems should be focused on by keeping in mind the increasing popularity of IoT.

In order to make Pakistan's IoT ecosystem a healthy, safe, and secure one, the government and regulatory bodies need to come forward and form a regulatory framework for IoT devices. What are the issues? IoT devices are not registered in Pakistan. There are no protocols or standards for manufacturing IoT devices. There is no regulatory framework for security and privacy of IoT devices. There is no standard operating procedure for maintenance and repair of IoT devices. There are no laws and regulations related to data protection and privacy of IoT devices. There is no standard for frequency band for operating IoT devices. There are no laws for data protection and privacy of IoT devices.

In order to overcome this challenge, a dedicated regulatory framework or policy should be developed by the government of Pakistan to provide a secure and trusted IoT ecosystem. This framework should be developed keeping in mind the current status of the country's technology infrastructure and the challenges faced by the existing regulatory frameworks. It should also provide a legal protection to all the stakeholders involved in the implementation of IoT in Pakistan.

5.1.4 Gaps in Terms of IoT Security

Policy Objective	Description	Relevance to IoT Security
Active Defense	Relevant stakeholders at any level should collaborate with ISPs, Internet Governance Organizations, and Law enforcement agencies to ensure the active defense against unwanted cyber security events.	IoT and LPWAN device manufacturers are not listed in the list of stakeholders. They can assume the exception here, which can lead to various risks in the IoT ecosystem of Pakistan.
Protection of Internet-based Services	Relevant stakeholders should initiate actions like developing reputation services, avoid installing programs and applications on Government networks downloaded from third-party unauthentic resources, etc.	The policy should also include protocols other than IP like Bluetooth Low Energy (BLE) Protocol because almost all IoT devices operate over low-energy protocols.
Protection & Resilience of National Critical Information Infrastructure	Relevant stakeholders should operate essential technical platforms to protect critical information infrastructure, ICT, IoT, and Next Generation Mobile Services.	Applicable to the security of the IoT ecosystem as well
Protection of Government's ICT Infrastructure & Information Systems	Relevant stakeholders should take mandatory controls to protect the Government's ICT, such as using the desired access control strategy while accessing government systems, enforcing robust authentication, and performing risk and security assessments periodically.	Applicable to the security of the IoT ecosystem as well
Framework for the Assurance of Information Security	Relevant stakeholders should implement the "Cyber Security by Design Concept" and establish the next-generation national security forensics and screening setups.	Applicable to the security of the IoT ecosystem as well
Public-Private Partnership	Relevant stakeholders like Government, academia, industry, and research centers should cooperate in developing the latest regulations and legislation with privately owned cyber security organizations.	Applicable to the security of the IoT ecosystem as well
Cyber Security Research & Development	Respective stakeholders should consider the importance of active research and development in designing and developing secure solutions, protocols, frameworks, and products.	Applicable to the security of the IoT ecosystem as well
Capacity Building	Relevant stakeholders should produce well-trained human resources.	Applicable to the security of the IoT ecosystem as well
Awareness of National Culture of Cyber Security	Relevant stakeholders should create preventive measures, knowledge on risks, and response to cyber threats via mass awareness efforts.	Applicable to the security of the IoT ecosystem as well
Global Cooperation and Collaborations	Ministry of IT and Telecom should be the central entity between national and international forums for active collaboration and exchange of valuables.	Applicable to the security of the IoT ecosystem as well
Cybercrime Response Mechanism	Relevant stakeholders should embed the effective response mechanism to cybercrimes to strengthen their procedures and processes.	Applicable to the security of the IoT ecosystem as well
Regulations	Effective national cyber security policy implementation should be ensured along with other regulations such as PECA 2016, etc.	No regulation is available related to the registration, operations, protocols, bands specification, and so on for IoT devices. This leaves the IoT ecosystem of Pakistan unnoticed and insecure.
Establishment of Trust in Digital Transactions	Digital certificates, Public Key Infrastructure (PKI), and Certification Services should be applied to ensure the integrity of digital services	Less resource-consuming encryption and integrity services are required to focus on IoT devices.

Table 3: Summary of the objectives of the National Cyber Security Policy of Pakistan and Loopholes Pertaining to IoT Security

5.2 Digital Pakistan Policy

This chapter critically evaluates the Digital Pakistan Policy released by the Ministry of IT and Telecom. The government's initiative has a noble vision of making Pakistan a 'Digital' country by enabling e-governance and facilitating economic and social development. The government has established an extensive plan and strategy to achieve a 'Digital' Pakistan, but how does it measure up to the other countries in the region? What are the key factors that have enabled other countries to be successful in their digital transformation? The primary motivation behind this evaluation is to highlight the policy's gaps in light of Pakistan's IoT ecosystem. Keeping those gaps in mind and Pakistan's current cyber security policy and the landscape of cybersecurity threats to the IoT ecosystem of Pakistan (chapter 3), the Draft of the National IoT Security Policy of Pakistan will be formulated in the next chapter.

5.2.1 Key Objectives of the Digital Pakistan Policy

The Digital Pakistan Policy's vision is to enable a fast-paced digitization eco system to promote economy and socio-economic growth. Here is a brief overview of the objectives of this policy that will later be analyzed on how they are relevant to IoT security in the country.

1. Creating a holistic digital strategy and promoting digitization among all sectors such as education, health, agriculture, and other socio-economic sectors.
2. Promotion of e-commerce by establishing relevant platforms and enabling Payment Service Providers (PSP) and Payment Service Operators (PSO) to function.
3. Encouraging youth and Female empowerment using IT.
4. Promoting innovation and entrepreneurship in the IT sector by enabling tech startups to flourish and scale.
5. Increase the country's software exports as well as promotion of local IT sector.
6. Improve Pakistan's ICT ranking.
7. Promote digital inclusion by bridging the gap between urban and rural population in terms of IT literacy and use.
8. Promote e-governance to facilitate citizens and modernize governance.
9. Increase foreign and domestic investment in the IT sector
10. Reduce barriers to access to IT for people with any kind of disabilities.

11. Start the process for creating standardization by coordinating and supporting standardization efforts to maximize reusability, create credibility and achieve cost effectiveness.

5.2.2 Policy Strategy

In the next part the Digital Pakistan Policy suggests a policy implementation strategy across all sectors in the country. The strategy is divided into four sections, each covering a different area. These sections and their brief details are shared below.

5.2.2.1 Section I: Key Components

This section explains key components of the policy and what areas can be covered to promote a digitization and modernization of systems in the country. Key areas are as following:

1. Legislation
2. Infrastructure Development
3. Human Resource, Entrepreneurship, R&I and Freelancing Development
4. Software Exports
5. ICT for Girls
6. Local Language Content Development
7. Helping Persons with Disabilities
8. Open Source
9. Local Manufacturing of Hardware
10. E-Governance

5.2.2.2 Section-II: Enabling the Digitization of Key Socio-Economic Sectors

This section identifies key government sectors that can benefit from digitization and use of IT in day-to-day operations. The sectors are as following:

1. E-Agriculture
2. E-Health
3. E-Energy
4. E-Commerce
5. E-Justice
6. ICT Education
7. IoT, FinTech, Artificial Intelligence & Robotics

8. Cloud Computing and Big Data

5.2.2.3 Section-III: Fiscal & Non-Fiscal incentives for the IT/ITeS Sector

In order to incentivize the IT sector, the Ministry of IT & Telecom plans a number of fiscal & non-fiscal incentives to create a favorable business environment. This section covers these incentives.

5.2.2.3.1 Fiscal Incentives

- Extension of Income Tax Holiday
- 5% Cash Reward on Export Remittances
- Reduction of Sales Tax on Services to 5%
- Provision of Bank Loans to IT Industry
- Tech Special Economic Zones
- Proliferation of New IT Parks

5.2.2.3.2 Non-Fiscal Incentives

- Reinforcement of the industry status of IT Sector at all levels of government.
- MoIT will work with Ministry of Commerce & other stakeholders for accession to the ITA regime to eliminate tariff barriers on imports of ICT products.
- Increase in the timeframe of initial registration period of call centers with PSEB to 5 years from the one year period.
- Allowing call center certifications to individual/sole proprietors.
- PSEB/PTA to promote work from home facility for the call centers to expand BPO workforce.
- Government of Pakistan will encourage trade delegations comprising of IT/ITeS-BPO to major international markets.

5.2.2.4 Policy Implementation & Reviews

This section states that the implementation of the Digital Pakistan Policy will require constant motoring and collaboration among all stakeholders. It calls for the formation of an ‘Action Plan’ for proper monitoring and evaluation. It also highlights key responsibilities and roles for different govt ministries, details of which are not relevant to this dissertation.

5.2.3 Relevance to IoT Security

The policy is a great roadmap for furthering digital inclusion the country, but it does not contain sufficient provisions for IoT security or even cyber security in general. It is more a general document of what needs to be done and covers less about how it can be done.

Thus, there is a need for a dedicated policy that deals with IoT security, as it is one of the most critical elements of a digital economy. The stakeholders involved in the implementation of IoT-based solutions should be well aware of the risks involved and how to tackle them. A dedicated policy will help in building a framework for risk assessment, identification, and control along with laying down the liability rules for each stakeholder involved in the implementation of IoT-based solutions.

Here is an analysis of the policy objectives in terms of IoT security.

Table 4: Summary of the objectives of the Digital Pakistan Policy and their relevance to IoT Security

Policy Objective	Relevance to IoT Security
Creating a holistic digital strategy and promoting digitization among all sectors such as education, health, agriculture, and other socio-economic sectors.	Can be relevant to IoT security by including relevant considerations
Promotion of e-commerce by establishing relevant platforms and enabling Payment Service Providers (PSP) and Payment Service Operators (PSO) to function.	Can relate to IoT when applied to e-commerce devices
Encouraging youth and Female empowerment using IT.	Not relevant
Promoting innovation and entrepreneurship in the IT sector by enabling tech startups to flourish and scale.	Not relevant
Increase the country's software exports as well as promotion of local IT sector.	Not relevant
Improve Pakistan's ICT ranking.	Not relevant
Promote digital inclusion by bridging the gap between urban and rural population in terms of IT literacy and use.	Not relevant
Promote e-governance to facilitate citizens and modernize governance.	Not relevant
Increase foreign and domestic investment in the IT sector	Not relevant
Reduce barriers to access to IT for people with any kind of disabilities.	Not relevant

Chapter 6

Security Policy for IoT Devices in Pakistan: A Draft

6.1 Introduction

Substantial changes have been observed in the digital space over a recent couple of years and would be most likely to be evolved as per industry experts. The Internet of Things (IoT) is the latest entrant to the digital space. These changes have been mainly attributed to the increasing adoption of smartphones and other IoT devices linked to smartphones and the Internet across generations. It is estimated that there are more than 5.34 billion

active mobile phone users in the world and about 180 million users in Pakistan. The penetration of technology, especially smartphones, across various demographics has brought immense changes in the marketing strategies for businesses. IoT can also be referred to as an interplay for telecom, software and electronic hardware sector and pledges to provide remarkable opportunities for several industries.

The development of services encompassing the Internet of Things (IoT), network-connected devices and systems generate tremendous opportunities and advantages for Pakistan. These devices require to be more resilient and secure in order to reap the advantages of connected tools and to mitigate the potentially serious threats posed by malevolent intruders trying to exploit them. Unfortunately, the increase in the number of businesses, devices and connected people boosts the potential risk of malicious attacks. Today, the devastating potential of cyber-attacks can enhance sharply when such intrusions or attacks influence huge quantities of affiliated IoT tools.

As threats to the digital ecosystem of the world, comprising IoT, linger on to grow, so does our expectation to rebuild confidence and trust in IoT and connected tools and bigger ecosystems to develop not only safety but innovation and economic growth.

Therefore, the draft IoT Security Policy has been proposed to leverage the strength of Pakistan as a major player in the service industry of the world and to make secure the IoT ecosystem of Pakistan through using supportive techniques and appropriate promotion. Shown below is a high-level overview of the proposed policy.

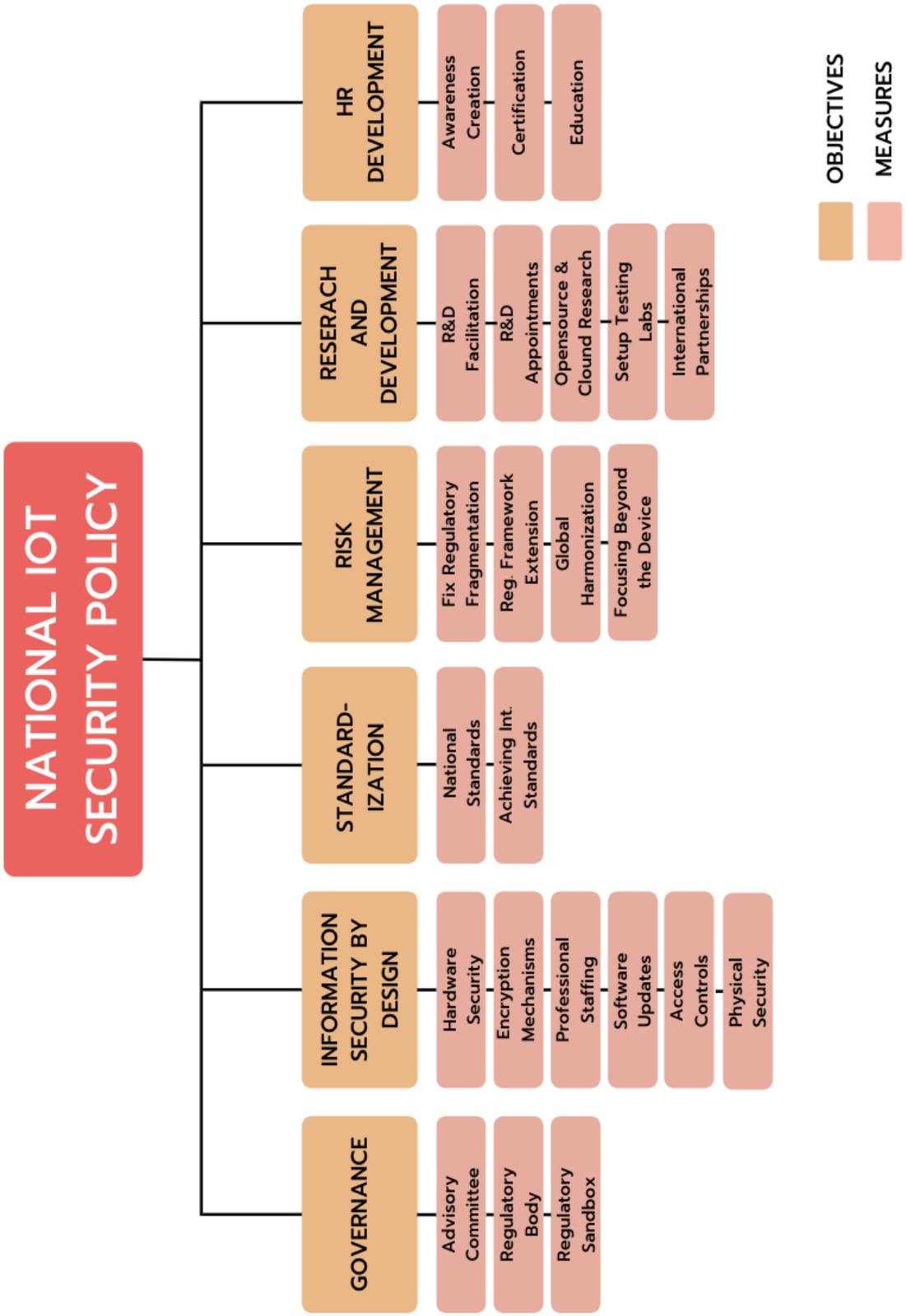

Figure 7: Overview of Proposed National IoT Security Policy

6.2 Vision, Scope & Objectives

6.2.1 Vision

The vision is for Pakistan to have a secure, robust, and continually improving nationwide IoT ecosystem. The goal is to create an environment that enables IoT industry growth, adoption, and implementation of best practices across all economic sectors. The ecosystem will be supported by standards, a common regulatory framework, and incentives for investment, innovation, and adoption of IoT technologies. The ecosystem will be inclusive, open to all stakeholders, and supportive of technological advancements and adoption of best practices. The policies aims to ensure accountability, confidentiality, integrity, and availability of individual users and corporates in order to bring positive improvement in the socio-economic development and national security of Pakistan.

The goal is to narrow the gap between the socio-economic development through digital transformation to build a prosperous and inclusive Pakistan. Providing global and local connectivity to the people of Pakistan through advanced communication networks and Internet Protocol. Providing security, privacy, and protection to the people of Pakistan through advanced technology and government initiatives. Providing opportunities for entrepreneurship, innovation and creativity for people of Pakistan through digital transformation.

6.2.2 Scope

The scope of this draft IoT security policy envisioned to secure the IoT ecosystem of the Pakistan including IoT devices, Short Range Devices (SRDs), data managed, stored, process, and transmitted by IoT devices, and other related IoT services. Scope of this draft IoT security policy also covers the provision of security and assurance of privacy of all public and private sectors organization and industries and citizens of Pakistan.

6.2.3 Objectives

The main objectives of this proposed IoT security policy draft are:

Figure 8: IoT Security Policy Objectives

- **Governance:** Establishment of governance for a secure IoT ecosystem in Pakistan. In order to establish a secure IoT ecosystem in Pakistan, the government will have to make sure that the ecosystem is secure by establishing a sound governance model. Only when the ecosystem has a good governance model will it be possible for the government to make sure that there are no data breaches. The government will also have to make sure that there is a regulatory framework for the Internet of Things. By doing so, it will be possible to make sure that the ecosystem is secure and that regulatory oversight is possible. The government has to make sure that there are systems in place for the monitoring of the IoT devices so that they cannot be used for malicious activities. Only when these things happen will it be possible to establish a secure IoT ecosystem in Pakistan.
- **Information Security by Design:** Ensure security and privacy of information and communication in personal and commercial IoT devices and infrastructure. These regulations will help to protect consumer privacy and data. They will also help

businesses to comply with data protection laws, which will protect them from data breach lawsuits and create a safe national IoT environment.

- **Standardization:** Ensuring security of government, military and all other IoT devices by mandating standards for design, development, acquisition, and operations of IoT devices in Pakistan. Government authorities, military, and all other IoT device manufacturers will be required to buy and use standardized IoT devices. All government authorities, military, and other IoT device manufacturers will be required to abide by standardized IoT device manufacturing procedures. They manufacturers will be required to use standardized IoT device development procedures and will be required to abide by standardized IoT device acquisition procedures.
- **Risk Management:** Collaboration and partnership at national and international level throughout the technical and operational processes to ensure management of risks and ensure the security of IoT ecosystem of Pakistan. IoT devices in Pakistan must include security features like authentication, data integrity, data encryption, device authentication, and others. Developing a national strategy to strengthen cyber security infrastructure and laws. Implementing automated systems and software to reduce the reliance on manual operations and human error. Adopting cloud solutions for critical and sensitive data to avoid the risk of data being stolen if the data is stolen from a server hosting the data.
- **Research and Development:** Involvement of both private and public sectors of Pakistan in active research and development to produce better security solutions for the IoT ecosystem of Pakistan. National and international networking to build capacity in research and development in IoT in the country. Collaborate with the academic institutions and research institutions to develop application-based R&D to solve real-world problems. Collaboration with international bodies to access best practices and new technological innovations in the field of IoT.
- **Human Resource Development:** Building of capacity, development of skills through training and skill development programs nationwide. Also creating awareness about cyber security among the masses. Increasing awareness about protecting data online and how to stay secure online to avoid financial, identity, and reputational risks. Also, working towards the development of a robust cyber

security ecosystem by engaging with stakeholders and partners across the country.

6.2.4 IoT Security Policy Details

The draft IoT Security Policy presents recommendations to support stakeholders and policymakers in better ensuring the security of Pakistan's IoT ecosystem by utilizing the following deliverables as a guide.

6.2.4.1 Governance

The Government of Pakistan needs to adopt an efficient policy to a structure for suitable governance of activities concerned with IoT and its applications. Government departments, autonomous bodies, and private organizations must work in unison to achieve the desired results. Moreover, the government must work with the private sector to create an enabling environment for investment in IoT security. A conducive policy environment will enable the private sector to take up the challenge of deploying IoT security throughout the country.

An independent regulatory body for IoT, a national policy on IoT, a comprehensive regulatory framework for IoT and a dedicated regulatory sandbox for testing of connected devices. These steps will help to create a suitable ecosystem for investment in secure IoT.

6.2.4.1.1 Setting Up an Advisory Committee and Regulatory Body

There is a need to form a high-level advisory committee which will also act a regulatory body with the relevant representations from all sectors of government, and academia. This committee will work towards a shared vision and mission towards building a secure IoT environment. It will help stakeholders to come together and create a conducive environment for the growth. The committee will have the responsibility to review and recommend new regulations, policies, and laws to be enacted. It will also be responsible for making recommendations on existing regulations, policies, and laws to ensure that they are IoT security friendly. It will work towards bringing together all the players of the IoTecosystem at one table. Effective and meaningful guidelines regarding the developing areas of IoT must be provided to this high-level advisory committee. Given below is a proposed structure for this High-Level Advisory Committee.

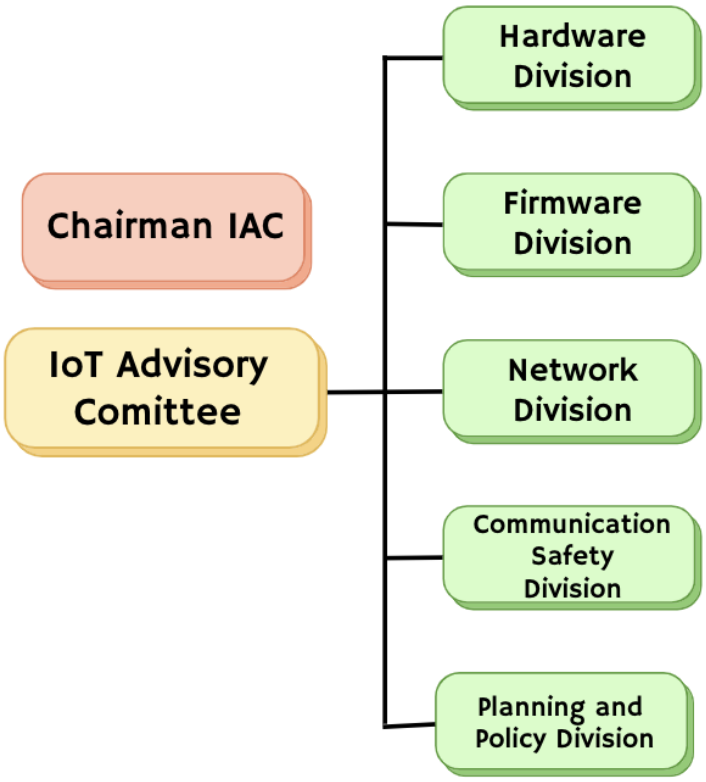

Figure 9: Proposed Structure of IoT Advisory Committee

Government stakeholders capable of handling IoT security moves will represent this committee. The responsibility of the Government will lie in the monitoring of IoT security projects and their progress within the provided time frame. The committee is to meet at least once every quarter and have its inaugural meeting within a period of 60 days from the coming into effect of this Act. The committee shall have the following powers and functions:

- Making recommendations for improving governance in the IoT Sector.
- Making recommendations for attracting investment in the IoT Sector.
- Reviewing regulatory and policy framework for improving governance in the IoT Sector
- Making recommendations for addressing issues of transparency and accountability in the IoT Sector
- Making recommendations for improving consumer protection in the IoT Sector

- Making recommendations for facilitating ease of doing secure business in the IoT Sector

6.2.4.1.2 Setting Up a Dedicated Regulatory Sandbox for Testing of Connected Devices

The regulatory sandbox concept that has been in use in the fintech and blockchain industries can be extended to testing of connected devices as well. The regulatory sandbox concept was first introduced in the United States in 2015. It allows to test a product or service in a live environment, but with a reduced risk of violation of regulations or laws. Setting up a dedicated regulatory sandbox for testing of connected devices is an operational process that will require close coordination and communication between the regulator, sandbox provider, and the government but it is a step that will go a long way in the creation and sustenance of a secure IoT landscape.

Setting up a sandbox environment with a controlled risk exposure is a must for testing of connected devices. The sandbox should have a controlled risk exposure and be highly regulated. A sandbox can be a group of cities, or a single city that enacts legislation to enable testing of connected devices within its boundaries. The sandbox environment should also have an enabling legislative and regulatory framework. The sandbox can be an existing regulation that enables testing of connected devices or can be a new regulation created for the purpose.

6.2.4.2 Information Security by Design

Signing and encrypting data is the best way to secure it, and it is critical that the right type of encryption be used in the right way. For example, engineers designing an IoT system must ensure that the system is using a strong form of encryption that cannot be easily broken. This can be accomplished by using public key infrastructure (PKI) or another form of key management. If a system uses a weak form of encryption or has a single point of failure, it can be hacked. To ensure a cohesive national IoT security environment the most important factor is security through encryption to protect data and communication. Many people do not recognise that everything connected to the Internet is susceptible to cyberattacks. Although IoT devices are typically low-risk, hackers can still utilise them as entrances into your network and do havoc.

- Create technical platforms to protect critical information by ensuring the following measures:

    - Setting up a firewall, encrypting information, creating an inventory of hardware and software, or implementing other protective mechanisms.
    - Make sure hardware is tamper-proof,
    - Provide firmware updates and patches,
    - Perform ongoing device testing
    - Protect data when disposing of devices.
    - Creating a disaster recovery plan.
    - Staffing organizations with professionals who have the necessary skills to protect data.
    - Keeping systems up to date with the latest software releases.
    - Keeping organizational information private by ensuring access control and physical security.
- Create processes to identify, prioritise, assess, and protect critical information.
- Ensure a secure IoT environment through international encryption standards.
- Mandate all operators of national, provincial, and organizational levels to hire qualified Cyber Security individuals.
- Ensure the use of digital certifications and their accreditation in developed, developing, and deployed information in all sectors.

6.2.4.3 Standardization

The government will get involved in the setting up of a National Service Setting Body and facilitate the global participation of SSOs in setting up Service Setting Bodies in Pakistan. The government will also provide attractive incentives and subsidies for setting up of R&D facilities for IoT devices.

The government will provide facilities to research bodies and encourage national and global participation of sector with suitable global Service Setting Organizations (SSOs) to promote standards about the IoT devices originated in Pakistan. It will take assistance from organizations for the sake of designing globally agreeable standards linked with interoperability, technology, services, and processes such as:

- Standardization of IoT safety standards.
- Global integrity/quality standards for traceability and creation of data.
- Communication standards outside and within the cloud.
- Accuracy, Privacy and integrity of the data and security standards.

- The privacy law should be set up to compatible with the emerging IoT ecosystem in Pakistan.

6.2.4.4 Risk Management

Collaboration and partnership at national and international level is necessary to mitigate IoT security risks. The best way to address these issues is to have a multidisciplinary and holistic approach, which includes the involvement of engineers, scientists, and researchers in the process of addressing the challenges. The main goal is to develop the most advanced and secure IoT ecosystem with a focus on the creation of a trustable and risk-free environment for all stakeholders. Smart Risk Management is important for the security of the IoT ecosystem in the country. Government agencies and private enterprises should keep a constant watch on their IoT implementation to guard against cyber threats. To achieve this, they must have a robust risk management framework in place. The risk assessment process starts with an analysis of the risk profile of each IoT implementation. The stakeholders must assess the impact of each implementation on the enterprise or government agency. They must also look at the risk level associated with the implementation. The enterprise or government agency must then identify the risk-mitigating measures for each implementation. To make a risk management framework more effective, enterprises and government agencies must hire risk managers who have the right set of skills and expertise.

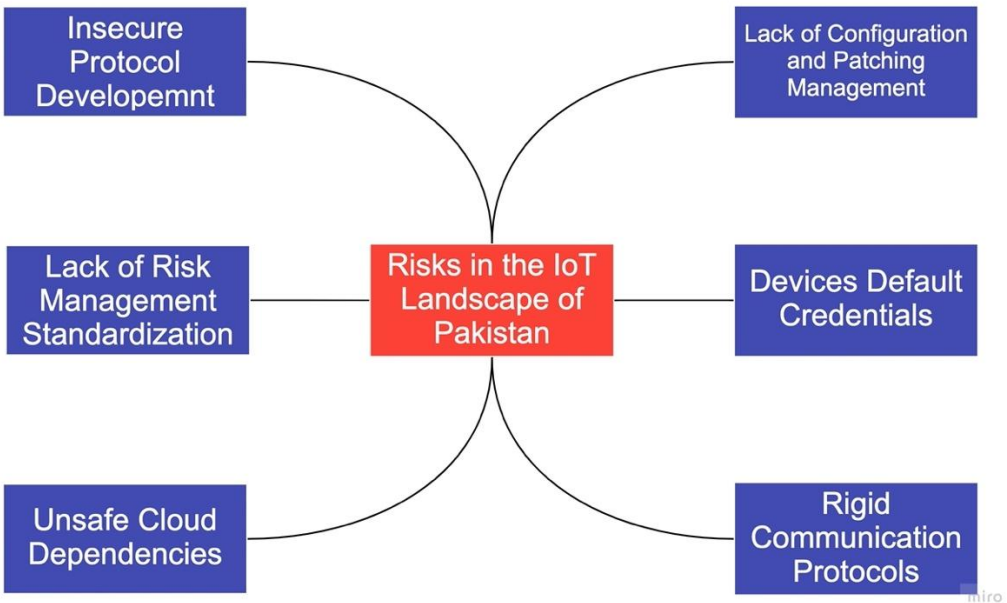

Figure 10: Risks in the IoT Landscape of Pakistan

There is no silver bullet to cybersecurity and the Internet of Things is incredibly complicated, however, the following steps can be taken to reduce risk in the ecosystem:

- Handling cyber threats across the ecosystem of communications and the internet. IoT devices collect and store a lot of sensitive data, and that data can be very valuable to hackers. Smart risk management will help in ensuring that IoT devices are secure and safeguard sensitive data.
- Banning embedded devices with insecure credentials—users may choose default or create insecure credentials that would be collected by hackers when scanning for exposed devices—may lead users to be frustrated with the process of setting credentials, resulting in insecure credentials. Phishing/hacks are easy targets in this area.
- Alleviation of communication protocols– 'man-in-the-middle' attacks on software-based interfaces are possible if they are inflexible, preventing users from applying additional security measures.
- Ensure use of safe dependencies in cloud services – Cloud services' insecure software dependencies—developers frequently rely on existing dependencies to provide functionality to their software, saving time.
- Relevant stakeholders will adhere to the secure development techniques for the development of protocols and services which are to be used in the IoT ecosystem of Pakistan.
- Proper management of configuration, identity, and patching of devices and services. These devices and services, if not properly managed, can be a potential cyber threat to the enterprise network. The right configuration of devices and services is critical to securing the enterprise network. Incorrect configuration can expose vulnerabilities, creating weak spots that hackers can exploit. Similarly, identity management plays an important role in securing the enterprise network. Most enterprises now use a variety of devices and services such as cloud, mobile devices, IoT devices, ERP, POS, etc. to conduct critical business functions. These devices and services, if not properly managed, can be a potential cyber threat to the entire enterprise network.

- Establish and enforce cyber security risk management methodologies according to international standards inter alia ISO/IEC 27005:2008 and ISACA RISK IT etc.

Policy Measure	Details
Mitigation of Regulatory Fragmentation	Examine areas requiring regulatory efforts. Encourage private-public cooperation through regulation. Boost IoT market through clear regulations.
IoT and SRD Regulatory Framework Extension	Government will work on an extension of the current IoT and SRD regulatory framework and include clauses related to IoT security.
Efforts for Global Harmonization	Adopt a holistic and international approach regarding the use of IoT devices. Global harmonization and cooperation for regulation will be prioritized by stakeholders.
Device Security	Implement of an endpoint Trusted Computing Base. Ensure that default or hard-coded passwords are not used. The device must verify the integrity of its own platform and authenticate the identities of its peers using trusted certificates. Anomalies in behaviour must be detected by modelling endpoint behaviour in IoT security. To ensure the connected object's robustness, both its hardware and its software must be resistant to attack.
Focusing Beyond the Device	Secure the different elements of networks and complicated ecosystems that design the IoT The focus of an inclusive process will be on end-to-end security, involving safe progress lifecycles and security-by-design methods. Major challenges concerning securing the Pakistan ecosystem instead of concentrating just on security products of IoT will be prioritized by the concerned stakeholders. The concerned stakeholders will give attention to the IoT ecosystem security entirely instead of loosely concentrating on individual elements of the ecosystem.

Table 5: Risk Management Overview

6.2.4.4.1 Mitigation of Regulatory Fragmentation

As the adoption of IoT grows, so will the responsibility of governments to ensure a safe and secure environment for its citizens. The government will encourage policies that have the potential to break down the challenges of connected devices and associating data while taking care of security and privacy to fully gain the advantages offered by IoT.

Some of the expected policy changes include mandatory data breach notifications, data protection laws, and increased awareness around data usage. Additionally, governments will focus on improving access to public data, open sourced data, and data analytics to drive economic growth. To reap benefits:

- The examination of technologies comprising IoT and assessment where oversight, regulation and current authority already exist and prevent siloed, sector-specific regulatory approaches will be made by the Government of Pakistan in collaboration with concerned bodies.
- Private-public cooperation on Internet of Things challenges will be implemented by regulators and policymakers to support exploring solutions for cybersecurity and effectively coordinate the several efforts for IoT security-related policy currently in the way across Pakistan.
- Relevant and clear information on important security elements in IoT tools will be provided to consumers by concerned stakeholders that may boost market competition through building confidence and trust in the products of IoT and supporting consumers satisfy their role in managing security.

6.2.4.4.2 IoT and SRD Regulatory Framework Extension

In Pakistan, IoT and SRD regulatory framework proposed by the Ministry of Information Technology and Telecommunication, indicates growth and interest towards IoT devices in the country. However, the framework currently only covers licensing details and does not have any provisions for ensuring security in IoT devices. This policy proposes that the government will work on an extension of the current IoT and SRD regulatory framework and include clauses related to security. By doing so, the government can ensure that when a device is manufactured or procured there is a comprehensive framework controlling the mandated security regulations that it must satisfy before it is available for either government, public or private use.

6.2.4.4.3 Efforts for Global Harmonization

The global IoT security landscape is fragmented by mandatory IoT needs proposed by municipalities, individual states, countries, and sector-specific bodies. For example, the European Union is working on a law that requires all car manufacturers to equip new cars with a "Black Box" data recorder. The United States Federal Communications Commission (FCC) has also proposed a rule that would require internet-connected

devices to be equipped with " software code that can be updated remotely in order to maintain compatibility with new technology standards." The legislative fragmentation of the IoT security landscape makes it difficult for everyone to manage compliance.

The emergence of such fragmentation may result in limiting the production of a secure IoT by mitigating the performances of scale in progress, support, assessment, production, training, and examination of secure items of IoT. The industry will also face difficulty in complying with such divergent needs, hampering trade and business of the world. To prevent this:

- It is required for the Pakistan IoT ecosystem to adopt a holistic and international approach encircling the use of baseline activities of security by stakeholders in several countries, parts of the ecosystem and sectors. It is imperative that Pakistan's IoT ecosystem adopts international standards and best practices for security to protect itself from cyber-attacks and other security risks. In this regard, the Government of Pakistan shall adopt best practices from other countries to secure its IoT ecosystem and can also work towards forming an international consortium of governments that are working towards forming a secure and interconnected IoT ecosystem for the benefit of their citizens.
- Global harmonization and cooperation for regulation will be prioritized by concerned stakeholders to confront an emerging divergent policy culture and to help a voluntary, and sector-driven consensus around the baseline abilities for the security of IoT that are embedded with global standards.
- Stakeholders must be aware of the thing that linking IoT tools or devices to the Internet is not a one-time structure and involves a one-time production cost but a long-term commitment. In a scenario where the Internet of Things is being implemented in an enterprise setting, the stakeholders must be aware of the fact that connecting IoT tools or devices to the Internet is not a one-time process and involves a one-time production cost. In fact, it is a long-term commitment that needs to be undertaken with utmost care and responsibility. Before you decide to go for the Internet of Things, you must have a clear understanding of the benefits that it is going to offer to your business. After that, you will have to choose the right vendor for the implementation. It is very important that the vendor you choose should be experienced and have a proven track record in this domain. After the implementation is done, you will have to keep in mind that these things

are connected to the Internet and are open to cyber threats. You must have a detailed plan in place to address any sort of cyber security issue that might crop up.

6.2.4.4.4 Device Security

Securing the device itself is the most critical aspect of IoT security. Hence the following steps should be undertaken:

- Implement of an endpoint Trusted Computing Base. A TCB is a hardware, software, and protocol suite that enforces computer system security policies. It is a crucial part of an endpoint. The trusted certificate stores and processes cryptographic secrets such as pre-shared Keys (PSKs) and asymmetric keys.
- Devices that have user interfaces must be capable of managing passwords effectively. Ensure that default or hard-coded passwords are not used.
- The device must verify the integrity of its own platform and authenticate the identities of its peers using trusted certificates.
- Anomalies in behaviour must be detected by modelling endpoint behaviour in IoT security. To detect hacked devices, certain behaviours must be recorded.
- Attackers may gain unauthorized access to a connected object by attacking the device's hardware or software. To ensure the connected object's robustness, both its hardware and its software must be resistant to attack.

6.2.4.4.5 Focusing Beyond the Device

To create a secure ecosystem, we need to go beyond the individual IoT devices and work on securing the whole ecosystem. This will ensure that the devices are connected to a secure network and are protected from external threats. There are a few ways to do this - One way is to have a proxy or firewall that controls the traffic between the internet and the IoT devices. Another way is to use trusted software on each device, which enables secure connections. These devices should also be upgraded with security patches when they are released. This will help to protect the ecosystem from external threats. A combination of all these methods will create a secure ecosystem. This will not only help in safeguarding the sensitive information of the customers, but also enable these devices to communicate with each other and exchange data securely. To do so, the manufacturers have to work towards a common standard. A standardised ecosystem will help to create a secure environment for data exchange, data integrity, and data privacy. We are already

seeing a lot of efforts being made towards this globally. For instance, in the case of 5G, due to its low latency and high bandwidth, it is expected to be used widely for connected cars. It's being designed to accommodate millions of connections from IoT devices, which will make it a very important part of the ecosystem. Similarly, efforts are being made to standardise the cloud infrastructure as well. These are some of the ways in which we can create a secure ecosystem for the Internet of Things:

- Collaboration among all stakeholders will be made to adopt a holistic and meaningful approach to securing the different elements of networks and complicated ecosystems that design the IoT.
- The focus of an inclusive process will be on end-to-end security, involving safe progress lifecycles and security-by-design methods. It will be essential that the development teams integrate security into their software development lifecycles, rather than implementing a one-off approach at the end of the project. This will enable the software to remain secure, even as new features and functionalities are added. In order to guarantee data security, the process must be monitored throughout, and the development team must be trained in security-by-design principles. Inclusivity of the process means engaging all stakeholders at every stage. This includes staff members responsible for information security, but also those who will be using the new software. The teams must collaborate closely to identify any areas of vulnerability and must be open to feedback.
- Major challenges concerning securing the Pakistan ecosystem instead of concentrating just on security products of IoT will be prioritized by the concerned stakeholders. As international concerns about IoT safety including concerns regarding distributed risk like botnets that maneuver and sophisticated automated, insecure IoT tools have continued to develop.
- The concerned stakeholders will give attention to the IoT ecosystem security entirely instead of loosely concentrating on individual elements of the ecosystem.

In case of addressing the elements of the ecosystem including security steps taken at the network, level of software and device in isolation, the results will ultimately be a failure. Adopting a holistic perception is therefore will a superior approach.

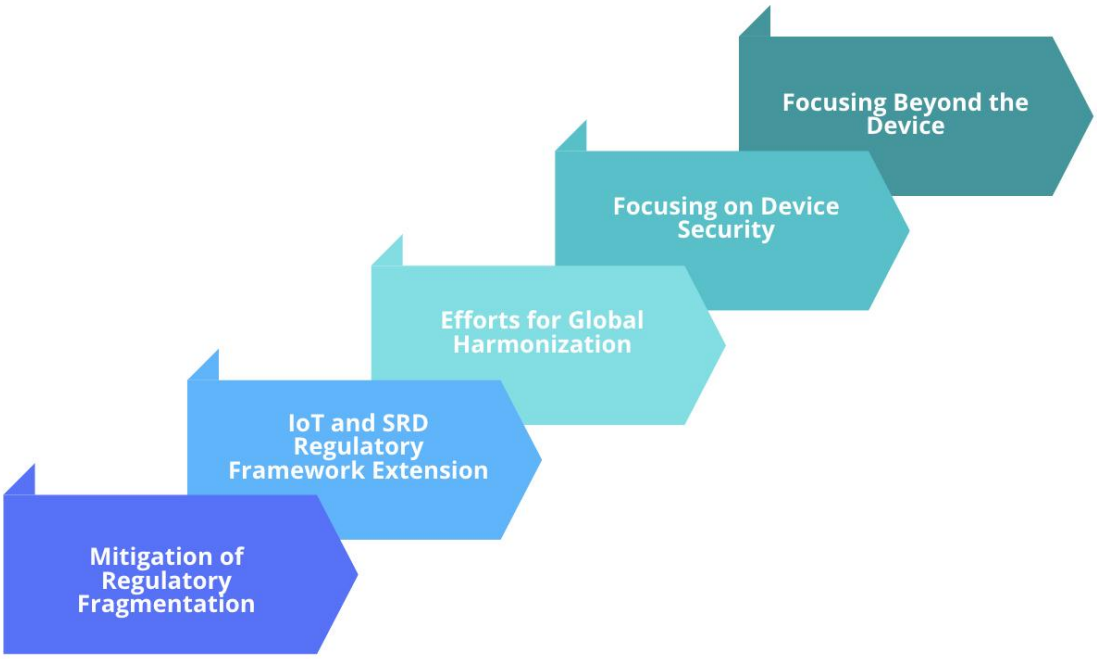

Figure 11: Risk Management in the IoT Ecosystem

6.2.4.5 Research and Development

The increasing number of connected devices and the growing reliance on cloud-based services have significantly increased the risk of cyberattacks. These factors have turned technological innovation into a double-edged sword, increasing the risk of cyber-attacks and data breaches. The ever-increasing connectivity of devices and massive amounts of data flowing through networks is creating new potential targets for cybercriminals. The Internet of Things is creating a vast and ever-growing network of devices, many of which were not initially built with security in mind. Many of these devices have very limited processing capabilities and memory, which makes it difficult to install security software. These devices are often designed with a relatively short lifespan in mind, which makes it difficult to upgrade the software. And, of course, many of these devices are manufactured by third-party vendors with no connection to the company using them. Even when we're talking about appliances, many of them are controlled via mobile apps or websites, which only makes security issues more critical. The IoT industry is growing at a rapid pace, and with it comes new challenges and risks for businesses. As more devices join the network, the risk of cyber attacks rises. To stay ahead of the competition, businesses must invest in research and development to stay at the forefront of IoT security. Investing in R&D

allows organizations to stay ahead of the curve, stay one step ahead of cyber criminals, and stay ahead of the competition.

- Facilitate research and development (R&D) in IoT for implementations of common good via call for proposals. By providing a platform for researchers and technologists to pitch their ideas, the aim is to drive innovation and accelerate the development of the Internet of Things for the common good. The IoT R&D efforts will receive and review proposals from researchers, developers and entrepreneurs with a focus on solving societal challenges.
- Appoint R&D core members connected with each field of technology which manages IoT. The team members must be experts who can predict the future of the technology. The R&D team must work in close collaboration with all other teams and monitor and study international best practices and the market to suggest innovative ideas to improve IoT security. They must have a thorough knowledge of the technological developments, vendor products and standards. The team members must be experts in working with different technologies.
- Introduce open-source cloud-based projects for creating cooperative and incessant research and development. This will offer a common space for researchers and developers to work together towards a common goal. The introduction of open-source projects will also have a positive impact on the rate of software development. Collaborative software development will result in quicker software development. The open-source model is beneficial as it reduces costs and increases the speed of software development. This will lead to faster and better quality software being developed. The open-source model will also improve the knowledge base of researchers. Researchers will be able to access and use the code of other researchers for their own research. This will lead to better and faster research.
- Establish test labs for hardware to software and hardware to hardware integration. The benefits of creating a test lab are multifold. Not only will this integrate testing earlier in the process, but it can also create a library of test cases that can be used to determine the best way to set up production environments. These labs can also set up replication capabilities so that if a production environment is ever compromised, it can recover from the test lab.

- Encourage international partners for undertaking IoT-related projects of R&D and stimulate private sector investment. The Government can also set up public–private partnerships (PPP) for setting up of innovation parks for encouraging R&D activities and start-ups focused on IoT. It can also facilitate setting up of venture capital funds and angel network to support start-ups. The Government can also set up incubators and accelerators for start-ups, facilitate setting up of exchange-traded funds (ETF) and mutual funds focused on IoT, and create infrastructure and business environment to support private investment in secure IoT.

6.2.4.6 Human Resources Development

Starting from awareness about IoT to the implementation of standards for its safety. At every stage, there is a need for a dedicated skill set. Pakistan with its huge potential in the field of IoT can become a global leader in the next few years if the right steps are taken at the right time. The IoT awareness program will highlight the importance of the technology, its usage, and the risk associated with it. The program will also help in creating a culture around IoT, where people will be more aware of security risks and responsibilities of the technology. The program will be hosted on Government and Private websites, as well as social media. Various activities will be carried out to create awareness among people about the usage of IoT, its benefits and its associated risk. People will be educated about the fact that why is IoT important, how to use this technology, the potential risk associated with it and what will be their responsibilities when using this technology. Government bodies and Private sector companies will be expected to have a framework in place to ensure compliance with the principles of the Policy and its Annexes. To initiate an awareness program and IoT Security Education in Pakistan for creating sets of skills for IoT safety at all stages. The following would the objectives of this program:

6.2.4.6.1 Awareness Creation

The proposed awareness program will focus on making the masses aware of the IoT technologies and its usage and how it can be used to improve the quality of life. Once the public is educated and aware of the IoT technology and its benefits, they can be assured that the technology is being used in a secure manner and they are safe. This will help in creating an overall positive impact on the economy of the country. It is expected that the proposed program will create at least 10,000 new jobs in the country.

- Generate video and audio content for promotion and awareness via social media. This includes a variety of materials, from basic explainer videos to live-streamed events. The benefit of video and audio is that it allows us to go into greater detail than a few paragraphs of text.
- Compile and publish blogs and articles in popular newspapers and journals. This is an excellent way to reach a large audience and push your message even further.
- Encourage workshops for high level executives from faculty and sector from academic institutions.
- Take part in and hold conferences and trainings in educational institutions and other sectors to raise awareness about IoT security.

6.2.4.6.2 Certifications and Education

In order to ensure that new generations of engineers and computer scientists receive the proper training in IoT security, governments must incorporate these topics into their curricula.

- Universities to offer master's degrees in IoT security and require students to conduct their own research. Therefore, these students must select a topic of interest and then conduct extensive research to discover any information that is relevant to their field of study. Some graduate students may not even realize that their area of interest falls under the category of IoT security. Therefore, it is up to faculty members to encourage students to explore these topics and discover how they can contribute to the field.
- In institutions which are supported by Government like TEVTA, introduction of a two to six weeks training program and IoT security-related certificate course.
- IoT security curriculum's introduction at Bachelors, Masters, and PhD level. Similar to universities in Asia like Nankai University, Beijing Normal University, Tsinghua University, Shanghai Jiao Tong University, and Wuhan University who have introduced IoT and cyber security topics in their degree programs.

Chapter 7

Policy Implementation Framework

7.1 Introduction

An IoT Security policy must be a living document that adapts to changing technology and trends, and addresses new challenges as they arise. In this section we discuss how the National IoT security policy can be implemented and propose a strategy or framework to materialize the policy on ground divided into different phases. The implementation strategy is divided into three main phases: Short-term, long-term and ongoing efforts. This policy implementation strategy can be used as the basis for an 'Action Plan' by the federal government to coordinate with relevant ministries and lead a consolidated IoT security effort in the country.

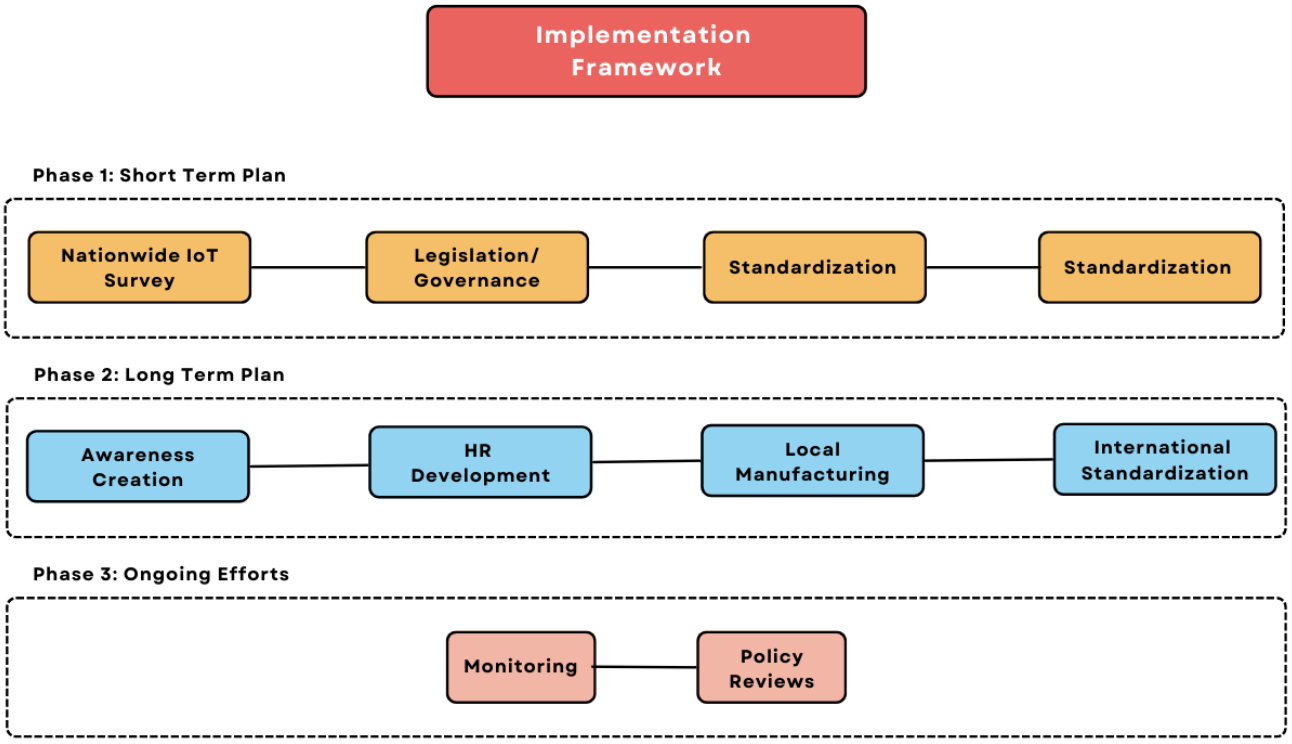

Figure 12: IoT Security Implementation Framework

7.2 Phase 1: Short Term Plan

This section outlines the efforts that can be started immediately by bringing together all stakeholders to begin a national IoT security plan and begin creating a secure IoT environment.

7.2.1 Nationwide IoT Survey

In the initial stage, the government should conduct a country-wide IoT survey to identify vulnerable areas and create awareness among citizens about the benefits of using secure IoT devices. IoT devices with minimum security features will be imported and distributed in the country. The government should set up IoT testing infrastructure in every state to test imported IoT devices and certify those that meet the standards. In the next stage, the government should set up a cyber observatory to monitor country's cyberspace and detect malicious activities. Government should also introduce cyber-education in schools and colleges to create awareness among the new generation about the importance of cybersecurity. It is important to note that the timeline of the implementation of the policy on ground can change according to the country's situation and needs. For example, the Information Gathering and Data Analysis phase may take more or less time depending on the country's situation and needs.

7.2.2 Governance/Legislation

Governments around the world are considering legislative action to make IoT devices safer for consumers. In the U.S., the Federal Trade Commission (FTC) is considering new regulations that would require companies that make IoT devices to disclose any security vulnerabilities to the FTC so that consumers can make informed purchasing decisions. The European Union is also considering legislation that would require manufacturers to maintain logs of software updates for certain types of IoT devices. Countries like Japan and Australia are also working on various legislative initiatives that would help to ensure the security of IoT devices for consumers. Similarly, Pakistan should also start with the following steps:

1. The government would legislate necessary policy frameworks, laws, and rules to enable creation of a secure IoT environment including enactment of data protection laws.
2. Legislation to ensure protection of personal data and security of sensitive and confidential information utilized in IoT devices

3. Developing a framework for cloud based services and its regulation which include data classification mechanism, standards for access, data privacy & transparency, ownership and security to promote the adoption of cloud based services.

7.2.3 Standardization

It is not possible to create a safe IoT environment without setting a baseline standard for security. Setting a standard for security and maintaining it will go a long way in helping to keep IoT devices safe. On the other hand, a lack of a security standard will open devices up to hackers who can exploit any vulnerabilities they find. A good example of a baseline standard for IoT security is the implementation of cryptographic controls and key management. These controls help mitigate a variety of threats, including data breach, device usurpation, and unauthorised access. Setting the right standards will not only make the IoT environment more secure and reliable, but will also make it easier to implement security at each stage of the IoT lifecycle. There are different standards that govern the creation, implementation, and operation of an IoT environment. Even though every standard has its own pros and cons, they all have one thing in common — they are essential for a secure IoT environment. In this blog post, we will explore the most important standards that are necessary to make an IoT environment secure. Therefore,

1. The government would come up with IoT security standards at par with international standards.
2. Ensure compliance with national standards across the board.
3. Ensure that all IoT devices in public and private sectors comply with the set standards.
4. Ensure compliance with set standards when procuring IoT devices.

7.2.4 Infrastructure Development

The Internet of Things is a network of physical devices that are connected to the internet. IoT devices are used for a variety of applications, such as monitoring climate conditions, tracking inventory in real time, or managing power grids. It is necessary to adopt a holistic approach to develop the IoT infrastructure in the country in a manner which is both beneficial to business as well as secure. To achieve this the government of Pakistan shall:

1. Enable cross sector collaboration to enable IoT development in all sectors while still ensuring security measures.

2. Create a central authority only meant to ensure that IoT security laws are being followed.
3. Setup departments specializing in securing IoT devices in all government and private organizations.
4. Develop an infrastructure where all devices that are procured or already exist are thoroughly tested to ensure security.
5. Provide subsidized access to secure devices for all those who are interested.

7.3 Phase 2: Long Term Plan

This section outlines the long-term future efforts that would be started by all stakeholders to continue creation of a secure IoT environment and in time strengthen that environment as well.

7.3.1 Creating Awareness

Mass awareness effort is of utmost importance to create knowledge about relevant IoT risks and best practices to ensure IoT devices are used safely by everyone. In the coming years, awareness training for IoT users will be vital for businesses and consumers alike, as these devices become more widely used. For businesses, it is important to train their employees to use IoT devices safely and securely. For consumers, it is vital to be aware of the risks associated with using IoT devices and to exercise caution when using them.

It is necessary to mitigate IoT threats in both public and private domains. In this regard the policy proposes that all stakeholders will:

1. Plan and implement education programs on IoT security customized for every relevant sector of society.
2. Encourage the corporate sector to protect the IoT space by maintaining a baseline desired level of IoT security in their offered and acquired products .
3. Preparation and execution of national awareness program to educate general users.
4. Implementation of a IoT Security Awareness program for government systems and officials.
5. Add IoT Security Awareness to the national education curriculum at school, college and university levels.

7.3.2 Human Resource Development

With the ever-growing need for enhanced IoT Security measures, it is integral to have a trained workforce that is ready to effectively utilize these secure devices while adhering to security standards. It is essential to spread awareness about IoT risks among the stakeholders to minimize the impact of such risks. It is also critical to provide information on how to avoid such risks through best practices. The stakeholders who are likely to be affected by IoT risks should be made aware of such risks and how they can be avoided. In the process of creating awareness among stakeholders, it is important to identify the right people to engage with. This can be done through profiling the risk group. The stakeholders who are likely to be affected by IoT risks should be made aware of such risks and how they can be avoided. Therefore, in this phase all stakeholders will:

1. Establish IoT Security Centers to educate and train human resources in IoT Security to strengthen and uplift the human support base.
2. Formulate and implement customized human resource development programs to fulfill the IoT Security needs of both public and private sectors.
3. Increase IoT Security research and development (R&D) budget for the development of indigenous IoT devices and security solutions to minimize dependencies.
4. Include IoT related courses in curriculums in the graduate and postgraduate Engineering and Law related degrees, training of prosecutors, lawyers and judges, etc.

7.3.3 Adoption of Local Manufacturing

True independence in terms of IoT security can-not be achieved unless we start manufacturing our IoT devices ourselves. The only way to make sure that your IoT device is not going to be a part of some botnet is to start from the very beginning with the hardware and software. You can't secure a device that is already manufactured. IoT manufacturers must make sure that they are not using software or hardware that can be hijacked and used as a weapon. The only way to do this is to start from the ground up.

At least on a government level all devices should be locally manufactured to minimize risk and ensure device security. As capacity to manufacture locally is built further, the private sector can also be made to shift towards local devices. This is an easier solution since it is more practical to manufacture devices according to our security standards

ourselves instead of having to rely on imports. Public and private sectors will be encouraged and incentivized to collaborate to bridge the manufacturing gaps in the industry. We can no longer rely on Chinese manufacturing for our smart devices. Companies such as Amazon, Apple, Google, and Microsoft are working on creating their own private clouds for their AI systems. This is the only way to ensure that data is kept secure. We need to do the same with our IoT devices.

7.3.4 International Standardization

Lastly, once a sufficient level of IoT security is achieved in the country, the government and concerned authorities shall work with international entities to bring Pakistani IoT security standards at par with international standards and make them acceptable worldwide so that in the future we may start exporting locally manufactured devices as well. Pakistan shall form a task force comprising of government officials, technologists, and other stakeholders to study the legal framework of data protection and privacy laws with regards to IoT and recommend improvements. A National Cyber Security Framework, as recommended by the International Telecommunication Union, shall be adopted. The government shall form a task force with participation of all stakeholders, including academia, to study the legal framework of data protection and privacy laws, and recommend improvements.

7.4 Phase 3: Ongoing Efforts

Once the plan is in action, it will be an ongoing effort to make sure that things are going smoothly and efficiently. While the short term and long-term plan are things that can be implemented in phases some other measures will need to be constantly undertaken as ongoing efforts to ensure a secure IoT environment.

7.4.1 Monitoring

To ensure adherence to plans set forth by the government there should be constant monitoring and check and balance. This can be achieved by setting up a feedback mechanism within the government. There must be systems in place to collect data and receive feedback from its citizens on how it is performing. This will help the government to identify gaps in its functioning and take corrective action. Setting up a feedback mechanism will also help in increasing trust among the people towards the government.

1. Creation of an IoT security governing body that is responsible for ensuring adherence to IoT rules.
2. The governing body shall be responsible to monitor and evaluate the level of adherence to IoT security laws across the board. It shall be an independent body.
3. The body shall evaluate and report any discrepancies it notices in terms of IoT security.
4. To avoid any suspicion of corruption or malpractices, the government can partner with a reputed organization to conduct regular audits of its projects. Partnerships like these will also help the government in obtaining technical know-how and expertise to execute its plans.

7.4.2 Reviews

An IoT Security Policy must be dynamic to keep up with changes in the environment and keep the organization protected from emerging security threats. Regular review of the policy is important to ensure that it stays current and relevant to the country's needs. The policy needs to be benchmarked with that of other leading nations to help identify areas of improvement.

- The IoT Security Policy shall be reviewed after a period of every one year initially to keep up with changes in the IoT environment and make necessary amendments.
- The review process shall be documented with the inputs and recommendations received from stakeholders. It shall be communicated to the stakeholders when it is updated with the change log. The policy shall be kept up to date with regard to the technological developments in the IoT environment.
- After 5 years this period will be reduced once every two years.

Chapter 8

Conclusion and Future Work

8.1 Background Study

In this dissertation it was established that IoT security is an essential need for the country. For the purpose of developing a comprehensive IoT security policy for the country we first studied the IoT security landscape of Pakistan to gain a thorough understanding of the country's IoT security situation. After this I identified the gaps within the country in terms of IoT security so that later we can propose a solution through the IoT security policy to mitigate those risks and gaps. To create a policy that is holistic and at par with international standards and best, the IoT security practices of different countries like India, China, Russia, USA and Israel were studied and analyzed to identify what they are doing in terms of IoT security and which of their practices we can adopt in Pakistan, whether as it is or by molding them a bit to better suit our IoT security landscape. A comprehensive overview was given of the security issues for the stakeholders of the IoT ecosystem. The policy will help the stakeholders to make informed decisions about the security of their products, services, and infrastructure. It will cover the responsibilities of government agencies and private sector companies to ensure the security of the IoT ecosystem.

It was identified that all the previously mentioned countries have made significant leaps in terms of IoT security, and we need to pick up pace to match their speed and become at par. If not, then Pakistan will be left at a disadvantage since in today's world IoT is the way forward. It is future of all industries and is making its way very rapidly into our everyday lives as well. In such an environment it is impossible to progress in terms of digitization without adequate considerations for IoT security on a national level with government facilitation and interest.

8.2 Policies Analyzed

The 'National Cyber Security Policy' and 'Digital Pakistan Policy and were analyzed in depth to identify whether they fulfill the need to create a secure IoT environment provide solutions to mitigate IoT risks in the country. Based on this analysis, it was observed that

the security aspect of IoT devices and related services is not appropriately considered in both these policies. IoT technology has already proven its worth in almost all application areas of Pakistan, including health, education, agriculture, public services, defense, and so on. However, per the analyzed threat landscape to this emerging technology, the security of the IoT ecosystem in Pakistan is at risk.

8.3 Proposed Solution/Policy

Therefore, this dissertation proposes a draft for the IoT security policy for Pakistan. The proposed IoT Security Policy draft covers all significant aspects of the desired security for the IoT ecosystem. This policy is a combination of existing IoT security policies of other countries and the requirements of the local IoT ecosystem. The draft policy includes all the aspects of security in the IoT ecosystem such as Network Security, Device Security, Data Security, Cyber Security, and Physical Security. The policy will be helpful for IoT Manufacturers, IoT Service Providers, and Government to meet the desired security in the IoT Ecosystem. The research has tried to incorporate the best practices from different countries in the form of a draft policy as a solution to the IoT security problem. This policy if adopted by the government of Pakistan can help in combating the security issues and can make the country a better place to live, work, and do business.

The main strategies suggested in the proposed IoT security policy draft include governance, risk management, avoidance of regulatory fragmentation, promotion of global harmonization, focus beyond the devices, research and development, and human resources development.

8.4 Implementation Strategy

Afterwards the dissertation also proposes an implementation strategy for the policy so that it can rolled out effectively to ensure proper adaptation to ensure IoT security in the country. The implementation strategy is an important part of a dissertation because it tells the reader how the policy will be rolled out and implemented, what challenges will be faced, and how they will be overcome. It is believed that the collective adoption of all proposed strategies in the IoT ecosystem of Pakistan could harden its security posture, as mentioned in this dissertation's vision and objectives of the proposed draft of the IoT security policy. It is hoped that the adaptation of this policy will address the rise in incidents related to malicious use of IoT devices which is affecting the integrity and the civil rights protections guaranteed by the state. It is important to note that these

recommendations are not a silver bullet, and no strategy is guaranteed to be 100% effective. In order to deal with the ever-changing landscape of security threats, all stakeholders in the IoT ecosystem of Pakistan should continuously evolve their risk management plans.

8.5 Future Work

In the future this draft can be reviewed and further refined by outlining the policy measures in much more detail and considering relevant authorities that can be made to work on the policy measures. There is a need for a dedicated policy that deals with IoT security, as it is one of the most critical elements of a digital economy. The stakeholders involved in the implementation of IoT-based solutions should be well aware of the risks involved and how to tackle them. A dedicated policy will help in building a framework for risk assessment, identification, and control along with laying down the liability rules for each stakeholder involved in the implementation of IoT-based solutions.

References

[1] Montori, F., Bedogni, L., Di Felice, M. and Bononi, L, "Machine-to-machine wireless communication technologies for the Internet of Things: Taxonomy, comparison and open issues," *Pervasive and Mobile Computing,* vol. 50, pp. 56-81, 2018.

[2] A. a. M. A. S. Zahra, IoT based ransomware growth rate evaluation and detection using command and control blacklisting, IEEE, 2017.

[3] Stead, "Spimes: A Multidimensional Lens for Designing Future Sustainable Internet Connected Devices," Lancaster University , United Kingdom, 2020.

[4] Rizvi, S.S.H., Zubair, M., Ahmad, J., Hashmani, M. and Khan, "Wireless Communication as a Reshaping Tool for Internet of Things (IoT) and Internet of Underwater Things (IoUT) Business in Pakistan: A Technical and Financial Review," *Wireless Personal Communications,* vol. 116, no. 2, pp. 1087-1105, 2021.

[5] P. M. a. M. S. K. Chanal, Security and privacy in IOT: a survey, Wireless Personal Communications, 2020.

[6] H. Z. Z. a. T. T. Wang, Special issue on security and privacy of IoT, World Wide Web 21.1, 2018.

[7] N. e. a. Waheed, Security and privacy in IoT using machine learning and blockchain: Threats and countermeasures, ACM Computing Surveys (CSUR), 2020.

[8] S. U. R. e. a. Aqeel-ur-Rehman, Security and privacy issues in IoT, International Journal of Communication Networks and Information Security (IJCNIS), 2016.

[9] Mazhelis, O., Luoma, E. and Warma, "Defining an internet-of-things ecosystem," in *In Internet of things, smart spaces, and next generation networking*, Springer, Berlin, Heidelberg, 2012.

[10] Trappey, A.J., Trappey, C.V., Govindarajan, U.H., Chuang, A.C. and Sun, "A review of essential standards and patent landscapes for the Internet of Things: A key enabler for Industry 4.0," *Advanced Engineering Informatics*, vol. 33, pp. 208-229, 2017.

[11] Shin, D.H. and Park, "Understanding the Internet of Things ecosystem: multi-level analysis of users, society, and ecology.," Digital Policy, Regulation and Governance, 2017.

[12] I. a. K. L. Lee, The Internet of Things (IoT): Applications, investments, and challenges for enterprises, Business horizons 58.4, 2015.

[13] F. e. a. Wen, Advances in chemical sensing technology for enabling the next-generation self-sustainable integrated wearable system in the IoT era, Nano Energy, 2020.

[14] T. e. a. Poongodi, Wearable devices and IoT, A handbook of Internet of Things in biomedical and cyber physical system, 2020.

[15] L. P. e. a. Rondon, Survey on enterprise Internet-of-Things systems (E-IoT): A security perspective, Ad Hoc Networks, 2022.

[16] H. e. a. Arasteh, Iot-based smart cities: A survey, IEEE 16th international conference on environment and electrical engineering (EEEIC, 2016.

[17] H. a. T. C. Rajab, IoT based smart cities, IEEE, 2018 international symposium on networks, computers and communications (ISNCC), 2018.

[18] A. S. e. a. Syed, oT in smart cities: a survey of technologies, practices and challenges, Smart Cities 4.2, 2021.

[19] Agrawal, P. and Narain, "Analysis of enablers for the digitalization of supply chain using an interpretive structural modelling approach," *International Journal of Productivity and Performance* , 2021.

[20] A. e. a. Aryal, The emerging big data analytics and IoT in supply chain management: a systematic review, Supply Chain Management: An International Journal , 2018.

[21] A. a. T. H. Chacko, "Security and privacy issues with IoT in healthcare." EAI Endorsed Transactions on Pervasive Health and Technology, 2018.

[22] Ahuja, K. and Khosla, "Network selection criterion for ubiquitous communication provisioning in smart cities for smart energy system," *Journal of Network and Computer Applications*, vol. 127, pp. 82-91, 2019.

[23] M. A. e. a. Razzaq, Security issues in the Internet of Things (IoT): A comprehensive study, nternational Journal of Advanced Computer Science and Applications 8.6, 2017.

[24] N. e. a. Almolhis, The security issues in IoT-cloud: a review, 16th IEEE International Colloquium on Signal Processing & Its Applications (CSPA), 2020.

[25] N. N. Thilakarathne, Security and privacy issues in iot environment, International Journal of Engineering and Management Research 10, 2020.

[26] Shad, "Cyber threat landscape and readiness challenge of Pakistan," *Strategic Studies*, vol. 39, no. 1, pp. 1-19, 2019.

[27] J. A. Lewis, Assessing the risks of cyber terrorism, cyber war and other cyber threats, Washington, DC: Center for Strategic & International Studies, 2002.

[28] L. a. A. C. e. Janczewski, Cyber warfare and cyber terrorism, IGI Global, 2007.

[29] J. a. S. B. Hua, he economic impact of cyber terrorism, The Journal of Strategic Information Systems 22.2, 2013.

[30] M. K. J. a. H. J. Robinson, Cyber warfare: Issues and challenges, Computers & security, 2015.

[31] S. Rasool, Cyber security threat in Pakistan: Causes, Challenges and Way forward, International Scientific Online Journal, 2015.

[32] Z.-K. M. C. Y. C. a. S. S. Zhang, Emerging security threats and countermeasures in IoT, Proceedings of the 10th ACM symposium on information, computer and communications security, 2015.

[33] Saleem, J., Adebisi, B., Ande, R. and Hammoudeh, "A state of the art survey-Impact of cyber-attacks on SME's," in *In Proceedings of the International Conference on Future Networks and Distributed Systems.*, 2017.

[34] Kolias, C., Kambourakis, G., Stavrou, A. and Voas, "DDoS in the IoT: Mirai and other botnets," *Computer* , vol. 50, no. 7, pp. 80-84, 2017.

[35] E. a. N. I. Bertino, Botnets and internet of things security, Computer 50.2, 2017.

[36] R. J. A. a. M. J. J. J. Vogt, Army of Botnets, NDSS, 2007.

[37] G. Cox, Managing the risks of shadow IoT, Network Security, 2019.

[38] Alt, F., Schneegass, S., Shirazi, A.S., Hassib, M. and Bulling, "Graphical passwords in the wild: Understanding how users choose pictures and passwords in image-based authentication schemes.," in *In Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services*, 2015.

[39] Franco da Silva, A.C. and Hirmer, "Models for internet of things environments a survey," *Information* , vol. 11, no. 10, 2020.

[40] M. Murphy, he Internet of Things and the threat it poses to DNS, Network Security 2017, 2017.

[41] B. R. Chandavarkar, Hardcoded credentials and insecure data transfer in IoT: National and international status, 11th International Conference on Computing, Communication and Networking Technologies, IEEE, 2020.

[42] M. e. a. Fagan, IoT Non-Technical Supporting Capability Core Baseline., 2021.

[43] C. M. M. e. a. Otalvaro, IoT Best Practices and their components: A Systematic Literature Review, EEE Latin America Transactions, 2022.

[44] R. e. a. Bruggemann, Global cybersecurity index (GCI) and the role of its 5 pillars, Social Indicators Research, 2022.

[45] N. a. A. M. Shafqat, Comparative analysis of various national cyber security strategies, International Journal of Computer Science and Information Security , 2016.

[46] Dawson, M., Bacius, R., Gouveia, L.B. and Vassilakos, "Understanding the challenge of cybersecurity in critical infrastructure sectors," *Land Forces Academy Review,* vol. 26, no. 1, pp. 69-75, 2021.

[47] T. G. Lewis, Critical infrastructure protection in homeland security: defending a networked nation., 2019.

[48] Lawson, C., Bersin, A. and Kayyem, " Beyond 9/11: Homeland Security for the Twenty-First Century," MIT Press, USA, 2020.

[49] I. Lee, Internet of Things (IoT) cybersecurity: Literature review and IoT cyber risk management, Future Internet, 2020.

[50] S. A. Valerievich, "The Ministry of Telecom and Mass Communications of Russia will study the security of the Internet of things," St. Petersburg International Economic Forum, 2019.

[51] Vijai, P. and Sivakumar, "Design of IoT systems and analytics in the context of smart city initiatives in India," *Procedia Computer Science,* vol. 92, pp. 583-588, 2016.

[52] Govt. of India, "Draft Policy on IoT," Department of Electronics & Information Technology (Deity), Ministry of Communication and Information Technology, India, 2015.

[53] Kosajan, V., Wen, Z., Zheng, K., Fei, F., Wang, Z. and Tian, "Municipal solid waste (MSW) co-processing in cement kiln to relieve China's Msw treatment capacity pressure," *Resources, Conservation and Recycling,* vol. 167, 2021.

[54] Sabillon, R., Cavaller, V. and Cano, "National cyber security strategies: global trends in Cyberspace," *International Journal of Computer Science and Software Engineering*, vol. 5, no. 5, 2016.

[55] B. Ben-Atar, Cyber security developments in Israel, Journal of Data Protection & Privacy, 2018.

[56] Adamsky, "The Israeli Odyssey toward Its National Cyber Security Strategy," *The Washington Quarterly*, vol. 40, no. 2, pp. 113-127, 2017.

[57] Cristiano, "Israel: Cyber defense and security as national trademarks of international legitimacy," *Routledge companion to global cyber-security strategy*, pp. 409-417, 2021.

[58] Meneghello, F., Calore, M., Zucchetto, D., Polese, M. and Zanella, "Internet of threats? A survey of practical security vulnerabilities in real IoT devices," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8182-8201, 2019.

[59] Y. e. a. ". s. v. A. c. s. o. a. W. c. 2. 2. I. C. o. A. C. T. (. I. 2. Seralathan.

[60] Y. e. a. Seralathan, IoT security vulnerability: A case study of a Web camera, IEEE, 2018.

[61] R. . Neisse, G. . Steri and G. . Baldini, "Enforcement of security policy rules for the Internet of Things," , 2014. [Online]. Available: http://publications.jrc.ec.europa.eu/repository/handle/jrc91395. [Accessed 1 9 2022].