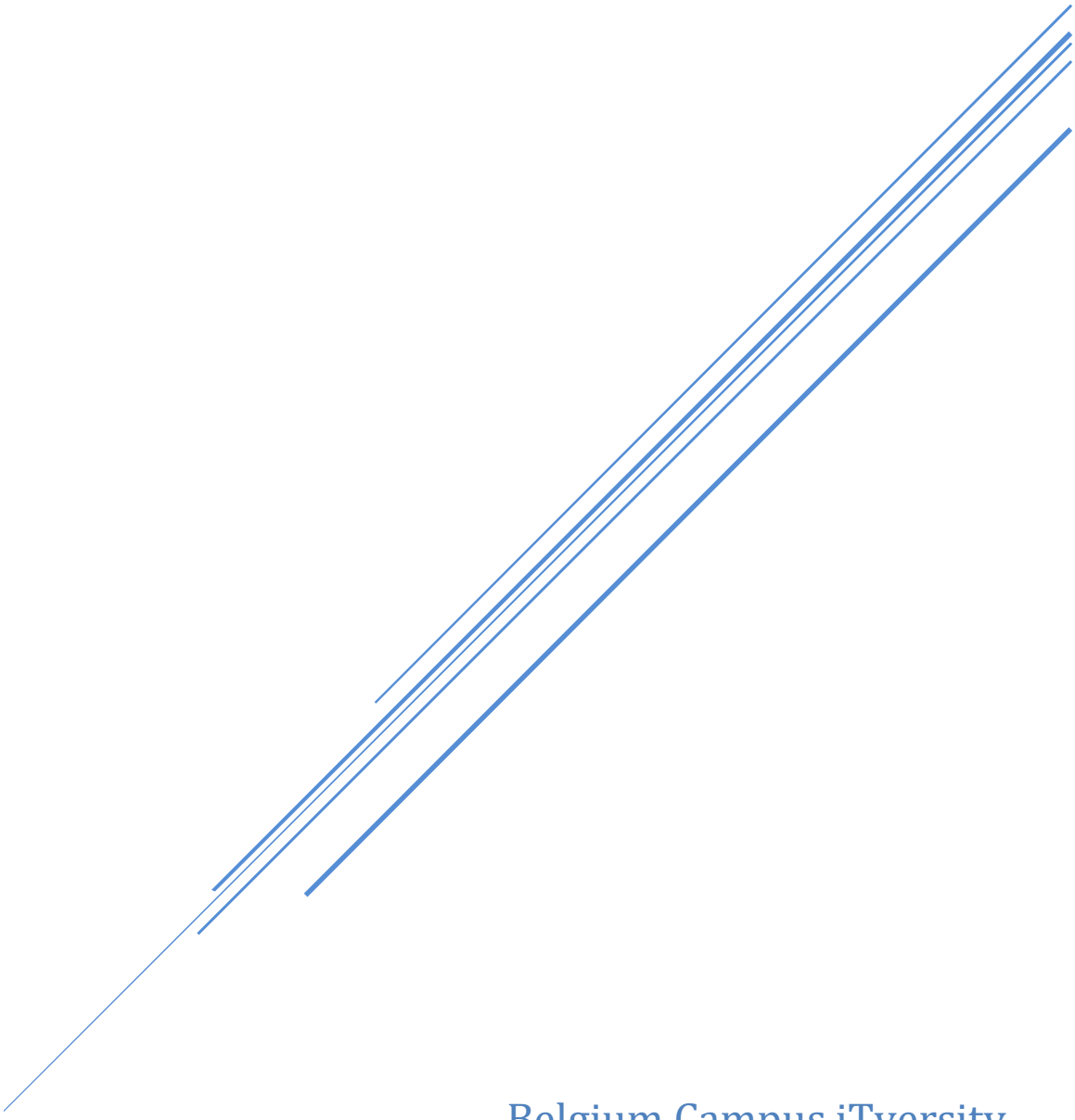
# Cybersecurity for Internet of Things (IoT)

By Kamogelo Phiri(577418)



Belgium Campus iTversity
DST481 Dissertation

# Contents


Chapter Outline ..... 2

Chapter 1: Introduction ..... 2

Chapter 2: Research Problem Statement ..... 2

Chapter 3: Research Questions, Objectives and Hypothesis ..... 2

Chapter 4: Significance of Study ..... 2

Chapter 5: Literature Review ..... 2

Chapter 6: Research Methodology ..... 2

Chapter 7: Anticipated results and effects ..... 2

Chapter 8: Moral concerns ..... 3

Chapter 9: Conclusion ..... 3

Introduction and Background ..... 4

Research Problem Statement ..... 6

Research Questions, Objectives, and Hypothesis ..... 8

Research Questions ..... 8

Objectives ..... 8

Hypothesis ..... 8

Significance of Study ..... 8

Literature Review ..... 11

Research Strategy ..... 13

Research Design ..... 13

Data Collection ..... 13

Data Analysis ..... 14

Justification of Method ..... 14

Expected Outcomes and Results ..... 14

Ethical Considerations ..... 15

Conclusion ..... 16

References ..... 16

# Chapter Outline

## Chapter 1: Introduction
The background of IoT technology and its cyber security concerns are covered in this chapter.

## Chapter 2: Research Problem Statement
This chapter will introduce the primary research topic by examining the security problems currently plaguing the Internet of Things (IoT). We'll focus on the limitations of existing security protocols, the increasing number of cyberattacks targeting IoT systems, and the vulnerabilities caused by resource-constrained IoT devices.

## Chapter 3: Research Questions, Objectives and Hypothesis
The objectives of the study will be clearly stated, and it will cover significant subjects like encryption, anomaly detection, and secure communication. The chapter will also include the hypotheses that predicts the findings of the study.

## Chapter 4: Significance of Study
The importance of study from an academic, practical, and technical perspective will be covered in this chapter. It will outline how the insights could contribute to the development of IoT cybersecurity by offering workable, efficient, and scalable solutions.

## Chapter 5: Literature Review
The most pertinent literature and current research on cybersecurity in IoT environments are compiled in this chapter. It discusses the problems, ideas, and current advancements while emphasising the gaps in the literature.

## Chapter 6: Research Methodology
The framework and methodology used during the research are covered in this chapter. It describes the procedures for collecting data, the sources of information, and the methods of analysis that will be applied.

## Chapter 7: Anticipated results and effects
This section describes the study's expected outcomes; like recommendations for workable and scalable cybersecurity solutions for the Internet of Things, evaluations of encryption protocols, and information on how to use secure communication protocols and anomaly detection techniques.

## Chapter 8: Moral concerns

This section covers the ethical issues that are pertinent to the study. Privacy records, informed consent, and the responsible use of data and research findings when working with technologies that track or collect personal data.

## Chapter 9: Conclusion

The final chapter provides a summary of the studies, restates their contributions, and makes recommendations for further research on IoT cybersecurity.

# Introduction and Background

Since technology is now widely accessible everywhere due to internet connectivity it continues to evolve and change daily life. A vast array of devices such as computers, smartphones, network routers and other digital hardware are connected to the internet making the environment increasingly interconnected. Internet of Things (IoT) is a network of physical objects with sensors, software and other technologies that enable them to communicate and share data. (Keyurbhai Arvindbhai Jani (U. V. Patel College of Engineering, 2020).

Industries that have made extensive use of IoT like transit systems, traffic management, home automation, environmental monitoring, healthcare and the defense sectors. These applications frequently use elaborate networks of sensors, actuators, gateways and networked devices that communicate with one another through a combination of wired and wireless technologies (Jaspinder Kaur, 2022).

Radio Frequency Identification (RFID), Bluetooth, Low Energy (BLE), Wi-Fi, ZigBee, Near Field Communication (NFC), mobile communication standards (1G–5G), Ethernet and WiMAX are some of the numerous communication technologies that allow IoT devices to connect to each other. Message Queuing Telemetry Transport (MQTT), Constrained Application Protocol (CoAP), HyperText Transfer Protocol (HTTP), web sockets, IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN), and other networking protocols are used by IoT systems. These protocols are necessary for both device interaction and data transfer (Keyurbhai Arvindbhai Jani (U. V. Patel College of Engineering, 2020).

Security threats have significantly escalated as IoT networks are incorporated into both residential and commercial environments. Cyberattacks and other security vulnerabilities are likely to affect these devices because they gather, store and send sensitive data. Assessing the risks connected to IoT environments and putting strong cybersecurity measures in place helps make it possible to find vulnerabilities. (Mohamed Seliem, 2018).

Internet of Things has fundamentally changed how people use technology in both personal and professional environments. Many industries are now "smart" thanks to the internet's ability to connect drones, sensors, wearable technology, surveillance systems, and even medical equipment. Sectors can include urban planning, transportation, energy, and healthcare. But this change has also led to some cybersecurity problems. Although a lot of research has been done on IoT security, there are still gaps in new areas such as lightweight security frameworks, the application of AI and machine learning integrated with cybersecurity, the safe deployment of IoT over 5G networks, and blockchain integration.

IoT devices also show real-time monitoring and data collection, which presents serious privacy and spying concerns. The wide use of cloud-connected devices forces obedience to the Confidentiality, Integrity, and Availability (CIA) security standards. Keeping operational and personal data secure is a major and ongoing concern for researchers and developers (Aejaz Nazir Lone, 2023).

Despite the increased focus on IoT security, many devices remain vulnerable due to design flaws. Traditional, resource-intensive security mechanisms are often impossible to implement due to decentralised systems, low processing power, memory limitations, and short battery life (Usman Tariq, 2023). Many cyberthreats; including distributed denial-of-service (DDoS) attacks, unauthorised access, and data breaches commonly target IoT devices (Andrade, Yoo, Tello-Oquendo, & Ortiz-Garcés, 2020). These vulnerabilities are especially concerning because of the increasing integration of IoT devices into critical infrastructure, which raises the possible consequences of successful hacks.

Given the size and complexity of IoT networks, it is evident that current cybersecurity methods are frequently insufficient. New security solutions that are lightweight, scalable, and device-agnostic are desperately needed. As IoT technologies advance, there is a need for research to create plans to safeguard these ecosystems (Aejaz Nazir Lone, 2023).

Advanced encryption methods, anomaly detection systems, and secure communication protocols (especially those made to function within the resource limitations common to IoT devices) are just a few of the strategies to improve IoT security.

| Security requirements | Vulnerability | Attack vector | IoT Layer | Owasp Classification |
|---|---|---|---|---|
| Authentication | Lack of the implementation of cryptographic algorithms.<br>Lack of password policy management.<br>The average password length on IoT devices is short.<br>Bypassing authentication and authorization.<br>Default passwords and credentials. | Attacker can discover the password using brute force or dictionary attacks.<br>Attacker can eavesdrop the wireless communication.<br>Attacker can gather configuration and authentication credentials from a non-tamper-proofed node, and can replicate it in the network.<br>Impersonation attack in which an adversary is disguised as a legitimate party in the system.<br>Device scanning attack. | Device Layer | Weak, Guessable, or Hard-coded password |
| Access Control | Bypassing access control checks<br>Misconfiguration.<br>Metadata manipulation.<br>Elevation of privilege. | Attacker can emulate the communication behavior of a real IoT node (Spoofing attacks).<br>The attacker can install a malicious firmware on the IoT device and control it remotely. | Device Layer.<br>Network Layer. | Insufficient Authentication or Authorization.<br>Insecure Software and Firmware. |
| Input and Output | Vulnerabilities on HTTP, Telnet and DNS. | DNS Spoofing, DNS cache poisoning, Denial of Service (DoS), Distributed DoS (DDoS) and URL interpretation | Application Layer. | Insecure Network Services. |
| Communications | Vulnerabilities on MQTT, CoAP, UPnP, and HNAP. | MQTT does not provide any data encryption by default. The attacker can sniff the data in transit. | Service Layer. | Insecure Network Services. |
| Cryptographic | Communication protocols do not rely on cryptographic mechanisms. | Eavesdropping attacks allow to analyze plain-text transmissions between IoT nodes. | Network layer. | Lack of Encryption and Integrity Verification. |
| APIs | Security misconfiguration<br>improper asset management<br>security injection<br>access exposure to data<br>broken authentication. | Replay attacks and Cross-Site Request Forgery (CSRF) | Service layer. | Insecure Network Services. |

(ROBERTO OMAR ANDRADE, 2020, p. 20)

# Research Problem Statement

Protecting devices has become increasingly important as the Internet of Things (IoT) grows. IoT devices are very vulnerable to attacks because of design flaws and a lack of standardised security procedures, even though they have many benefits in a variety of industries (Usman Tariq, 2023). Because these devices regularly collect and transmit

sensitive data like financial, personal and industrial control data, hackers find them appealing. The frequency and complexity of cyberattacks against IoT devices are increasing, endangering not only individuals but also companies and even entire nations.

The primary source of IoT security issues is these devices' limited resources. Traditional security methods often fail to meet the unique requirements of IoT systems. These devices' frequently low processing power, small memory, and short battery life make it impossible to implement resource-intensive encryption techniques, anomaly detection algorithms and secure communication protocols. Resulting in many IoT devices are configured with either no security or very little, leaving them vulnerable to misuse.

There is an urgent need for scalable, lightweight, and specifically tailored security solutions that can handle the demands of Internet of Things devices. Current IoT security research has focused on encryption methods, anomaly detection, secure communication protocols along with other subjects; but a lot of these concepts are still theoretical or haven't been refined for resource-constrained environments yet. Adding these security features to IoT devices usually means sacrificing security and performance in the form of increased power consumption or slower processing speeds.

This study addresses two research issues: first, it examines the lack of the security frameworks that are currently in place for IoT devices; second, it investigates and recommends new security techniques that balance security and performance. This study will specifically focus on the evaluation of lightweight encryption techniques, the application of machine learning-based anomaly detection methods and the optimisation of secure communication protocols to increase the overall security of IoT systems without significantly disturbing device performance.

As IoT devices become more integrated into everyday life and important infrastructure, the risk of cyberattacks increases. Ineffective security solutions may have broader social consequences, including potential disruptions towards national security, healthcare, transportation networks and individual privacy. Closing the knowledge gap and providing practical solutions will be crucial to enhancing IoT security and assisting the safe and secure development of this rapid evolving technology.

# Research Questions, Objectives, and Hypothesis

## Research Questions

1. How can encryption methods be made more secure for IoT without sacrificing functionality?
2. Which anomaly detection techniques are best for finding security threats in IoT systems?
3. Which secure communication protocols may be used to protect data transfers across the IoT?

## Objectives

1. Examine and evaluate current encryption methods that are relevant to IoT systems.
2. Identify and assess efficient anomaly detection algorithms for IoT security.
3. Investigate existing secure communication methods and how they are used in IoT.

## Hypothesis

Overall security of IoT systems may be greatly increased without sacrificing their use by improving communication protocols, anomaly detection, and encryption techniques.

# Significance of Study

This work is significant because it advances the field of cybersecurity, especially by addressing the issues in Internet of Things. As IoT technology continues to advance, there are both major benefits and serious vulnerabilities. Understanding the risks and developing practical, scalable solutions are essential to make sure an IoT ecosystem's ongoing growth and safe operation.

There are several reasons why this study is important.

**1. Resolving the Increasing Danger of IoT Security Flaws**

The more IoT devices there are, the more prone they are to hackers. By exploiting security holes in these devices, cybercriminals can obtain private data, disturb entire networks, or gain unauthorised access. Recent well-known attacks, like the Mirai botnet attack, used infected IoT devices to launch widespread DDoS (Distributed Denial of Service) attacks (Keyurbhai Arvindbhai Jani (U. V. Patel College of Engineering, 2020), demonstrate the potential for IoT vulnerabilities to be destructive.

**2. Creating Security Solutions in an Environment with Limited Resources**

There is a serious security risk because many IoT devices function in environments where traditional cybersecurity solutions (which require a lot of memory and processing power) are not feasible. Current anomaly detection and encryption methods often result in latency, excessive power consumption or hinder the device performance. The goal of this research is to find robust and lightweight solutions that meet the security needs of IoT devices without putting undue strain on their limited resources.

**3. Improving IoT Users' Security and Privacy**

IoT device security vulnerabilities affect not only companies but also individuals whose personal data may be misused or stolen. IoT devices collect and transmit sensitive data such as location information from smart home appliances, financial transactions from smart payment systems, and health information from wearable technology (Ferrag & Shu, 2021). IoT device vulnerabilities expose users to identity theft, privacy invasion, and even physical harm if devices controlling home security or healthcare systems are compromised.

By boosting security of IoT devices with encryption, anomaly detection, and secure communication protocols, this research will greatly improve the privacy and safety of IoT users.

**4. Contribution to the Development of Policies and Regulations**

As IoT devices are integrated into critical infrastructure, the need for strong cybersecurity standards is growing. Governments and regulatory organisations around the world are already creating IoT-specific security standards and regulations (Mikhail Kuznetsov, 2022). But these recommendations usually ignore the challenges posed by resource-constrained IoT devices. The study's conclusions will provide lawmakers with useful data to help them develop practical and effective IoT security regulations.

**5. Useful Implementations in Various IoT Domains**

The results of this study may have suggestions for many industries that heavily depend on IoT technology. From healthcare and manufacturing to driverless cars and smart cities (Jaspinder Kaur, 2022). IoT device security is essential to safeguarding operations and services. For example, healthcare sector and autonomous vehicle breaches could cause accidents or even in one of these areas. Through enhanced encryption or more accurate anomaly detection, the knowledge gained from this study will immediately contribute to making IoT devices in these critical industries safer, more reliable, and better protected against cyber-attacks.

**6. Contributing to the IoT Security Academic Field**

This study will contribute to the growing field of IoT security research in addition to its practical applications. There are still unresolved issues regarding how to effectively secure these devices, despite the importance of IoT and cybersecurity respectively..

# Literature Review

Literature on IoT security shows that there is growing concern about the vulnerabilities brought with the rapid use of IoT. Hackers find IoT devices to be targets because many of them transmit private information over open networks. Examining the literature on cybersecurity technologies from the perspective of IoT may help develop a thorough understanding of IoT cybersecurity. The following are based on Lee's five-layer business IoT architecture (Lee, 2019)

**Cybersecurity at the Perception Layer**

Traditional encryption methods like RSA and AES can usually strain resources for low-power devices, which are common in IoT networks. Due to this, researchers have focused on developing lightweight encryption algorithms balancing security and processing speed (Mishra, 2022). Algorithms like elliptic curve cryptography (ECC) and lightweight AES have gained popularity due to their lower computational cost, making them ideal for resource-constrained situations. An example, RFID tag clones could be used to launch distributed denial-of-service (DDoS) attacks. Physical unclonable functions (PUFs) have been used for identification and authentication also creating cryptographic keys for some semiconductors (Gao, Ranasinghe, Al-Sarawi, Kavehei, & Abbott, 2016). PUF chips enhance security by preventing duplicate devices, provide tamper resistance, device identification alongside authentication. Because IoT device components are often built on resource-constrained platforms, lightweight PUF solutions are needed. PUFs cannot be duplicated, but once a PUF key has been recovered it can be duplicated (Ygal Bendavid, 2018).

**Cybersecurity at the Network Layer**

This network layer is essential to the overall security performance of the IoT system since devices, processing stations and the entire system depend on secure data transmission across the network (Qureshi, Qureshi, Haider, & Khawaja, 2020). Anomaly detection is necessary for identifying malicious activity in IoT networks. By continuously monitoring device behaviour and network traffic, anomaly detection systems can find odd behavior from routine operations, which often indicate a potential security breach. Many techniques such as machine learning-based methods like support vector machines

(SVMs), neural networks, and clustering that can detect complex patterns of malicious behaviour (Ahmed, 2022).

**Cybersecurity at the Processing Layer**

For processing and storing large data streams generated by multiple IoT devices simultaneously, cloud computing and fog computing are becoming standard technologies. In fog computing, intrusion detection systems (IDS) can be used to detect disturbances on a fog node. A hybrid approach combining IDS, Virtual Honeypot Devices (VHD), and Markov models shows promising results in fog computing when detecting hostile (Amandeep Singh Sohal, 2018).

**Cybersecurity at the Application Layer**

Smart grids, smart homes, smart transportation, and smart health are just a few of the application domains that require different security management techniques. For example, because smart health works with highly personalised data, it requires high security and privacy protection. Attacks on IoT applications could affect the security of other connected apps because many of them might be managed by third-party service providers.

Secure communication protocols ensure the integrity and confidentiality of data transferred between IoT devices. IoT networks, which are often decentralised, need safe and efficient communication protocols. Protocols designed for different tiers to meet these requirements include MQTT (Message Queuing Telemetry Transport) and CoAP (Constrained Application Protocol) (Apostolos Gerodimos, 2023).

**Cybersecurity at the Service Management Layer**

At the service management layer, cybersecurity's primary focus is on its human and business aspects. Trust and privacy issues are relevant to IoT service management because they affect how IoT services and apps are used. When processing personally identifiable information (PII), safeguarding devices and data is important to maintaining

people's privacy. Early in the development process, privacy protection measures must be included to promote trust when using of IoT devices (Katie Boeckl, 2019).

# Research Strategy

Using a qualitative comparative research approach based on a careful analysis of secondary sources; the goal of this study is to identify, evaluate, and compare methods to enhance security in Internet of Things (IoT) systems.

## Research Design

The nature of the study is exploratory and descriptive, aiming to provide a comprehensive understanding of current IoT security practices. Analysing and producing findings from technical white papers, case studies, academic publications, and industry standards will be done. Current improvement techniques will be examined, existing vulnerabilities will be found, and suitable security solutions that consider the limitations of typical IoT devices will be recommended.

## Data Collection

The data for this study will be from sources like cybersecurity technical reports, IEEE conference journals/articles, and/or peer-reviewed journals. Cybersecurity and IoT jargon such as "resource-constrained cybersecurity," "secure IoT protocols," "IoT anomaly detection," and "lightweight encryption for IoT" will be used during the search.

To guarantee excellence and relevance:

- Priority will be given to research published within the last five to seven years (2018–2024).
- Sources must specifically address IoT security or provide solutions for scenarios.
- The methodology, scope, creativity, and relevance of the findings of each selected study will be looked at closely.

### Data Analysis

The thematic analysis will involve looking at IoT security issues and trying to find common patterns.

Comparison of encryption methods, anomaly detection models, and communication protocols based on factors like:

- Process overhead and Memory usage
- Energy consumption and Detection precision
- Protocol latency and Resilience

Where appropriate, quantitative measurements from existing benchmark tests will be used to support evaluation (examples being; encryption time in milliseconds, detection rate %, packet loss during secure transmission, etc.). Findings will be put into comparison tables and graphics to highlight performance trade-offs and use-case applicability.

### Justification of Method

A qualitative, literature-driven approach is justified by the study's broad technical scope and objective of knowledge production and practical guidance. Because IoT security is a rapidly evolving field with numerous ongoing advancements, this approach allows for comprehensive, up-to-date coverage of current solutions and implementation.

## Expected Outcomes and Results

Given the constraints of IoT devices, emphasis will be placed on security solutions that are effective while requiring the fewest resources possible.

The research is expected to deliver the following key results:

1. **Recommendations for Lightweight Encryption**
   Part of goal of this study is to find efficient encryption methods suitable for IoT devices with low power consumption. This will provide practical guidance for selecting encryption techniques in a range of use cases, such as smart homes, healthcare, and industrial IoT.

2. **Comparison of Anomaly Detection Techniques**
   The study will compare machine learning methods (like SVM, Random Forest, and k-means) with traditional rule-based systems to detect anomalies in IoT networks. It will check each method's precision, resource usage, and flexibility in constrained environments.
3. **Assessment of Secure Communication Protocols**
   Lastly, the study will evaluate IoT-friendly protocols such as lightweight HTTPS, MQTT, and CoAP. It will analyse their security, scalability, and speed, with a focus on enhancements like mutual authentication and end-to-end encryption for devices with constrained resources.

The research aims to produce these findings to contribute valuable insights to the field of IoT cybersecurity. The findings will enhance the overall security of IoT ecosystems; assisting manufacturers, policymakers and device developers in picking and implementing appropriate security solutions that are viable and efficient.

## Ethical Considerations

IoT cybersecurity research must effectively take ethical issues like data security, privacy, and suitable risk management into account. Since IoT devices frequently handle sensitive personal data, any proposed security enhancements should put user privacy protection first.

Getting users' informed consent and guaranteeing data ownership are essential ethical considerations. Despite being theoretical and devoid of real-world experiments, this study obeys with ethical standards that place a high value on transparency when gathering, sharing, and protecting data. Priorities remain high for preserving user independence and ensuring that individuals are aware of and in control of their data.

Another important consideration is reporting vulnerabilities that are discovered. Since pointing out security flaws without offering solutions could increase system risk, ethical responsibility entails taking steps to mitigate known risks. Additionally, recommended security solutions need to be inclusive so that users from a variety of socioeconomic backgrounds can benefit from them.

# Conclusion

The quick expansion of IoT has greatly benefited many sectors, but it has also raised serious cybersecurity concerns. IoT devices are difficult to secure with traditional methods because of their extensive distribution and resource constraints.

This research proposal highlights the need for practical and lightweight security solutions with a focus on encryption techniques, anomaly detection, and secure communication protocols. Through a comparative and literature-based approach, this aims to identify strategies that are effective and feasible for real-world IoT contexts.

# References

Jani, K.A. and Nirbhay Chaubey (2020). IoT and Cyber Security. *IGI Global eBooks*, pp.203–235. doi: https://doi.org/10.4018/978-1-7998-2253-0.ch010

Lone, A.N., Mustajab, S. and Alam, M. (2023). A comprehensive study on cybersecurity challenges and opportunities in the IoT world. *SECURITY AND PRIVACY*, 6(6). doi: https://doi.org/10.1002/spy2.318

Seliem, M., Elgazzar, K. and Khalil, K. (2018). Towards Privacy Preserving IoT Environments: A Survey. *Wireless Communications and Mobile Computing*, [online] 2018, pp.1–15. Doi: https://doi.org/10.1155/2018/1032761

Kaur, J., Jaskaran, Nidhi Sindhwani, Anand, R. and Pandey, D. (2022). Implementation of IoT in Various Domains. *Springer eBooks*, pp.165–178. doi: https://doi.org/10.1007/978-3-031-04524-0_10

Tariq, U., Ahmed, I., Bashir, A.K. and Shaukat, K. (2023). A critical cybersecurity analysis and future research directions for the internet of things: A comprehensive review. *Sensors*, [online] 23(8). doi: https://doi.org/10.3390/s23084117

Andrade, R.O., Yoo, S.G., Tello-Oquendo, L. and Ortiz-Garces, I. (2020). A Comprehensive Study of the IoT Cybersecurity in Smart Cities. *IEEE Access*, 8, pp.228922–228941. doi: https://doi.org/10.1109/access.2020.3046442

Andrade, R.O., Yoo, S.G., Tello-Oquendo, L. and Ortiz-Garces, I. (2020). A Comprehensive Study of the IoT Cybersecurity in Smart Cities. *IEEE Access*, 8, pp.228922–228941. doi: https://doi.org/10.1109/access.2020.3046442

Kuznetsov, M., Novikova, E., Kotenko, I. and Doynikova, E. (2022). Privacy Policies of IoT Devices: Collection and Analysis. *Sensors*, 22(5), p.1838. doi: https://doi.org/10.3390/s22051838

Rameez Raja Kureshi and Bhupesh Kumar Mishra (2022). A Comparative Study of Data Encryption Techniques for Data Security in the IoT Device. *Lecture notes in electrical engineering*, pp.451–460. doi: https://doi.org/10.1007/978-981-16-7637-6_40

Chatterjee, A. and Ahmed, B.S. (2022). IoT anomaly detection methods and applications: A survey. *Internet of Things*, [online] 19, p.100568. doi: https://doi.org/10.1016/j.iot.2022.100568

Gerodimos, A., Maglaras, L., Ferrag, M.A., Ayres, N. and Kantzavelou, I. (2023). IoT: Communication protocols and security threats. *Internet of Things and Cyber-Physical Systems*, [online] 3. Doi: https://doi.org/10.1016/j.iotcps.2022.12.003

Lee, I. (2019). The Internet of Things for enterprises: An ecosystem, architecture, and IoT service business model. *Internet of Things*, 7, p.100078. doi: https://doi.org/10.1016/j.iot.2019.100078

Mollah, M.B., Azad, Md.A.K. and Vasilakos, A. (2017). Security and privacy challenges in mobile cloud computing: Survey and way ahead. *Journal of Network and Computer Applications*, [online] 84, pp.38–54. doi: https://doi.org/10.1016/j.jnca.2017.02.001

Bendavid, Y., Bagheri, N., Safkhani, M. and Rostampour, S. (2018). IoT Device Security: Challenging 'A Lightweight RFID Mutual Authentication Protocol Based on Physical Unclonable Function'. *Sensors*, 18(12), p.4444. doi: https://doi.org/10.3390/s18124444

Qureshi, A., Qureshi, M.A., Haider, H.A. and Khawaja, R. (2020). *A review on machine learning techniques for secure IoT networks*. [online] IEEE Xplore. doi: https://doi.org/10.1109/INMIC50486.2020.9318092

Boeckl, K., Fagan, M., Fisher, W., Lefkovitz, N., Megas, K.N., Nadeau, E., O'Rourke, D.G., Piccarreta, B. and Scarfone, K. (2019). Considerations for managing Internet of Things (IoT) cybersecurity and privacy risks. *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks*. [online] doi: https://doi.org/10.6028/nist.ir.8228

Lee, I. (2020). Internet of Things (IoT) Cybersecurity: Literature Review and IoT Cyber Risk Management. *Future Internet*, 12(9), p.157. doi: https://doi.org/10.3390/fi12090157

Sohal, A.S., Sandhu, R., Sood, S.K. and Chang, V. (2018). A cybersecurity framework to identify malicious edge device in fog computing and cloud-of-things environments. *Computers & Security*, 74, pp.340–354. doi: https://doi.org/10.1016/j.cose.2017.08.016