SAVONIA
University of Applied Sciences

TYPE OF REPORT – BACHELOR'S DEGREE PROGRAMME
TECHNOLOGY, COMMUNICATION AND TRANSPORT

INTERNET OF THINGS FOR SUSTAINABILITY: PERSPECTIVES IN PRIVACY, CYBERSECURITY, AND FUTURE TRENDS

AUTHOR/S Isa A. Oyedeji

Field of Study Technology, Communication and Transport	
Degree Programme Degree Programme in Information Technology, Internet of Things	
Author(s) Isa A. Oyedeji	
Title of Thesis INTERNET OF THINGS FOR SUSTAINABILITY: PERSPECTIVES IN PRIVACY, CYBERSECURITY, AND FUTURE TRENDS	
Date	Pages/Number of appendices 47
Client Organisation /Partners Veijo pitkänen Markku kellomäki (Savonia University of Applied Science)	

Abstract

The Internet of Things (IoT) has changed our way of life, providing enormous possibilities for sustainability efforts, and causing significant concerns over privacy and cybersecurity. The thesis examined the Internet of Things for sustainability: perspectives in privacy, cybersecurity, and future trends. It analysed the cybersecurity challenges present in IoT networks by focusing on identifying vulnerabilities and suggesting strategies to improve IoT installation protection. Researchers have explored the potential of current IoT developments like artificial intelligence, edge computing, and blockchain technology to revolutionize sustainability efforts.

Also, it examined the global environmental policies and standards that influence the creation and implementation of IoT solutions. From the findings of the thesis, it was discovered that Privacy problems on the Internet of Things (IoT) are wide-ranging, encompassing data protection, user permission, unwanted access, and larger ramifications for personal privacy. These concerns are worsened by the widespread use of IoT devices, which gather, transmit, and frequently keep massive amounts of personal information. Also, sustainability and safeguards of IoT system may be reduced by recognizing possible and executing effective mitigation techniques.

From the findings, it is recommended that by embracing emerging trends and adhering to regulatory frameworks, the Internet of Things has the potential to contribute to positive environmental outcomes and encourage a more sustainable future.

Keywords
Sustainability, Internet of Things, Cybersecurity, Privacy

CONTENTS

LIST OF FIGURES

1 INTRODUCTION

1.1 EVOLUTION AND GROWTH OF INTERNET OF THINGS

The Internet of Things (IoT) has grown significantly since its introduction. Once envisioned as a network of linked gadgets, the Internet of Things (IoT) has fast become a ubiquitous and innovative technological system that has impacted many organizations and industries.

IoT's development was driven by major technological progress in wireless communication, sensor technology, and data analytics. Advancements in low-power, high-performance microcontrollers and sensors have allowed to produce small and energy-efficient IoT devices that can gather and send data instantly. (Atzori et al. 2010.)

Standardization and interoperability were necessary as IoT networks grew. IEEE and the ITU developed standards and protocols to provide seamless communication and interoperability among varied IoT devices and platforms. (ITU-T 2020.)

The growth of IoT technology has led to the emergence of new applications and industries, including Industrial IoT (IIoT) and smart cities. IoT in industrial environments enables predictive maintenance, remote monitoring, and process optimization, leading to enhanced efficiency and cost savings (Gupta et al., 2016). IoT technologies are utilized in smart cities to improve urban infrastructure, enhance public services, and promote sustainability. (Zanella et al. 2014.)

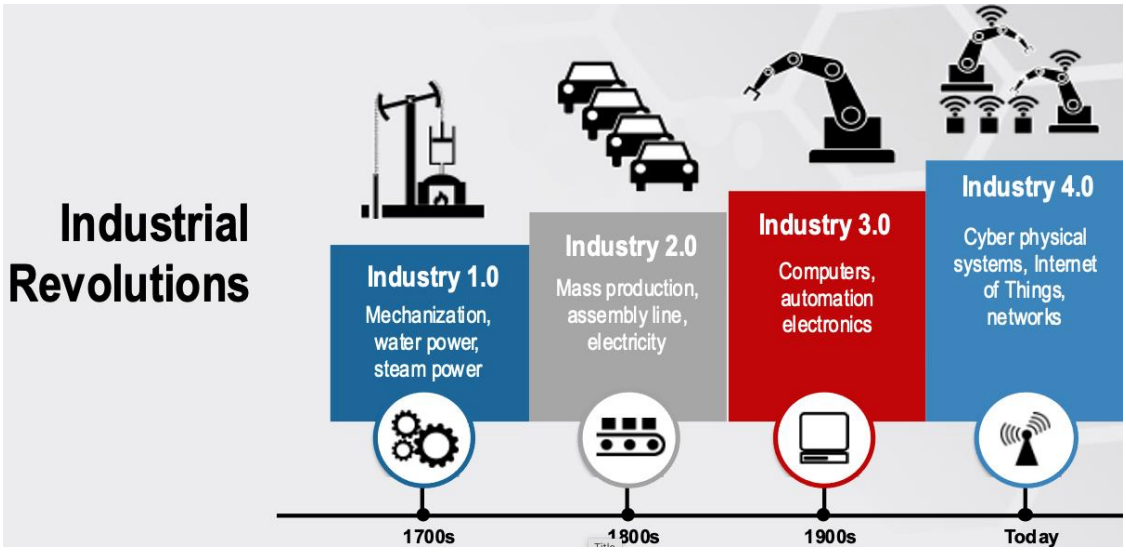


Figure 1. IoT industrial Revolutions (Medium 2023.)

1.2 IMPORTANCE OF SUSTAINABILITY IN INTERNET OF THINGS

The important of IOT is as following:

Environmental Conservation: Sustainable IoT initiatives focus on environmental conservation by reducing the ecological impact of device production, deployment, and disposal. Utilizing sustainable materials, minimizing energy usage, and including recyclable parts are crucial for decreasing environmental harm. (Corchado et al.2019.)

Energy Efficiency: Energy efficiency is essential for sustainable IoT solutions since many IoT devices are battery-powered or utilize energy-harvesting methods. Enhancing device longevity and reducing energy demand in IoT deployments can be achieved by optimizing power consumption through low-power hardware design, effective communication protocols, and cognitive data processing. (Gubbi et al. 2013.)

Resource Optimization: Sustainable IoT practices focus on efficiently managing resources over the whole lifespan of IoT implementations. By limiting resource consumption, improving workflows, and supporting circular economy principles across the design, production, operation, and maintenance processes, more effective utilization of materials and resources can be achieved. (Ilic et al.2020.)

Social and Economic Benefits: Adopting sustainability in IoT offers environmental, social, and economic advantages. Sustainable IoT efforts increase social resilience, economic prosperity, and equitable development by promoting innovation, creating green jobs, and increasing quality of life. (Al-Fuqaha et al. 2015.)

Regulatory Compliance and Corporate Responsibility: The relevance of sustainability in IoT is highlighted by stricter environmental legislation and increasing consumer awareness. Organizations must adhere to regulatory standards, employ transparent supply chain procedures, and embrace corporate social responsibility principles to establish trust, manage risk, and maintain a competitive advantage in the IoT market. (Tully 2019.)

1.3 PRIVACY AND CYBERSECURITY CONCERNS

The Internet of Things (IoT) has transformed technology interaction by allowing smooth communication and intelligent automation in different areas. The increase of IoT devices creates important issues surrounding data privacy and security. With the expansion of IoT ecosystems, it is essential to prioritize addressing privacy concerns to protect sensitive data and uphold user confidence.

Data Collection and Surveillance: IoT devices often collect vast amounts of data about users' behaviors, preferences, and surroundings. From smart home appliances to wearable fitness trackers, these devices continuously gather data, raising concerns about intrusive surveillance and unauthorized data collection (Miorandi et al. 2012).

Data Breaches and Cyberattacks: The interconnectedness of IoT systems creates weaknesses that can be manipulated by nefarious individuals. Security breaches and cyberattacks on IoT devices can lead to unwanted access to critical data, jeopardizing user privacy and security. (Roman et al. 2013).

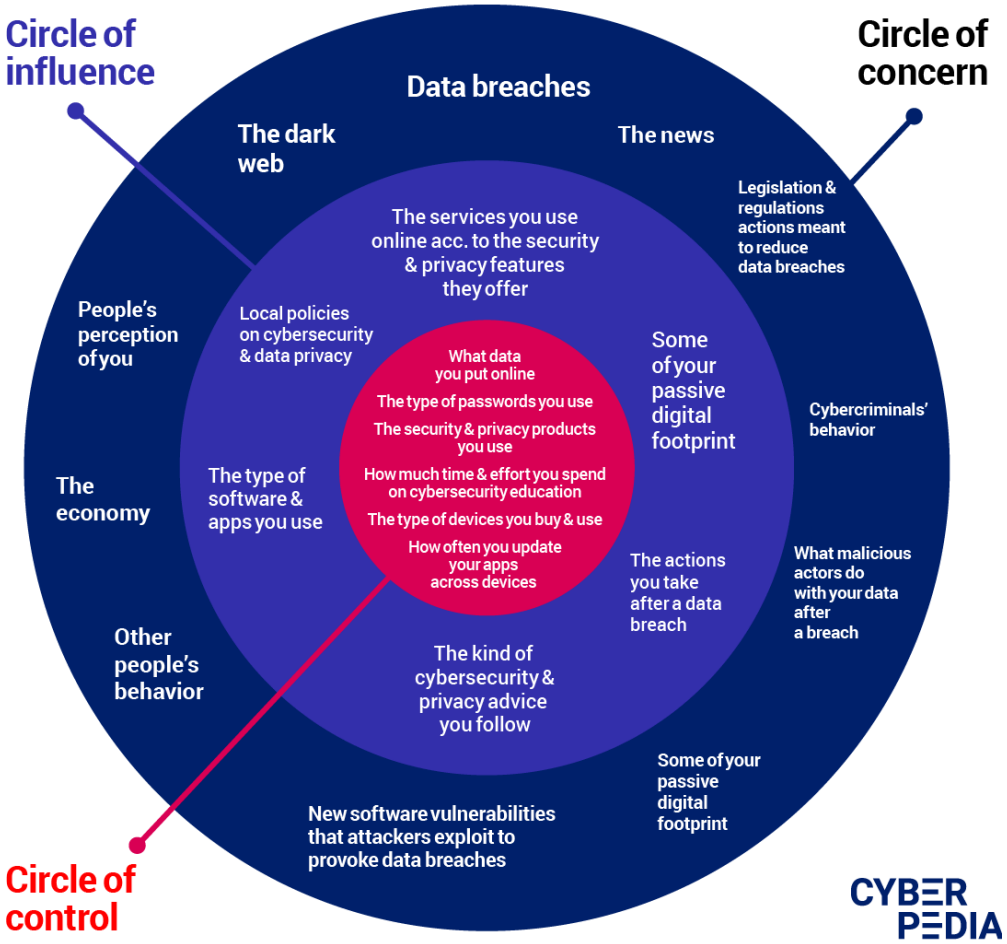


Figure 2. Data breaches and cybersecurity (bitdefender.)

Lack of Transparency and Consent: Several IoT devices function in obscure settings where users have minimal insight into data collection methods and processing algorithms. The absence of clear communication and permission processes worsens privacy worries, diminishing user independence and authority over personal information. (Fernandez- Carames Fraga- Lamas 2018.)

Inadequate Data Protection Measures: IoT devices frequently send data across wireless networks, making information vulnerable to surveillance and eavesdropping. Data is at risk of illegal access and exploitation due to weak encryption, inadequate authentication procedures, and insufficient security processes. (Zhang et al, 2014.)

Regulatory Compliance and Legal Frameworks: The regulations concerning IoT privacy are still developing, with many regions not having thorough laws to deal with new privacy issues. Implementing precise regulatory frameworks, enforcing privacy laws, and ensuring accountability for data breaches are crucial measures to safeguard user privacy in IoT settings. (Bilge et al. 2014.)

2 INTERNET OF THINGS

2.1 IoT TERMS AND CONCEPTS

Internet of things (IoT) comprises of enormous variety of terminology and ideas that act as the basis for development in the field. Acquiring knowledge for these terminologies' is important to understand the complicated nature and potential of IoT technology. The following few essential of internet of things terms and concepts.

Internet of things (IoT) Devices: These are physical objects that have sensors, actuators, and networking features, allowing them to gather, transmit, and receive data over the internet. Illustrations encompass intelligent thermostats, portable fitness trackers, and industrial sensors. (Atzori, Iera, & Morabito 2010.)

Figure 3. Physical IoT Devices (news 2020)

Sensor Networks: Sensor networks are comprised of linked sensors that gather data from the physical world. These sensors can monitor a range of characteristics including temperature, humidity, light, motion, and sound. Sensor networks play a crucial role in IoT applications by supplying

real-time data for analysis and decision-making (Akyildiz, Su, Sankarasubramaniam, & Cayirci,2002).

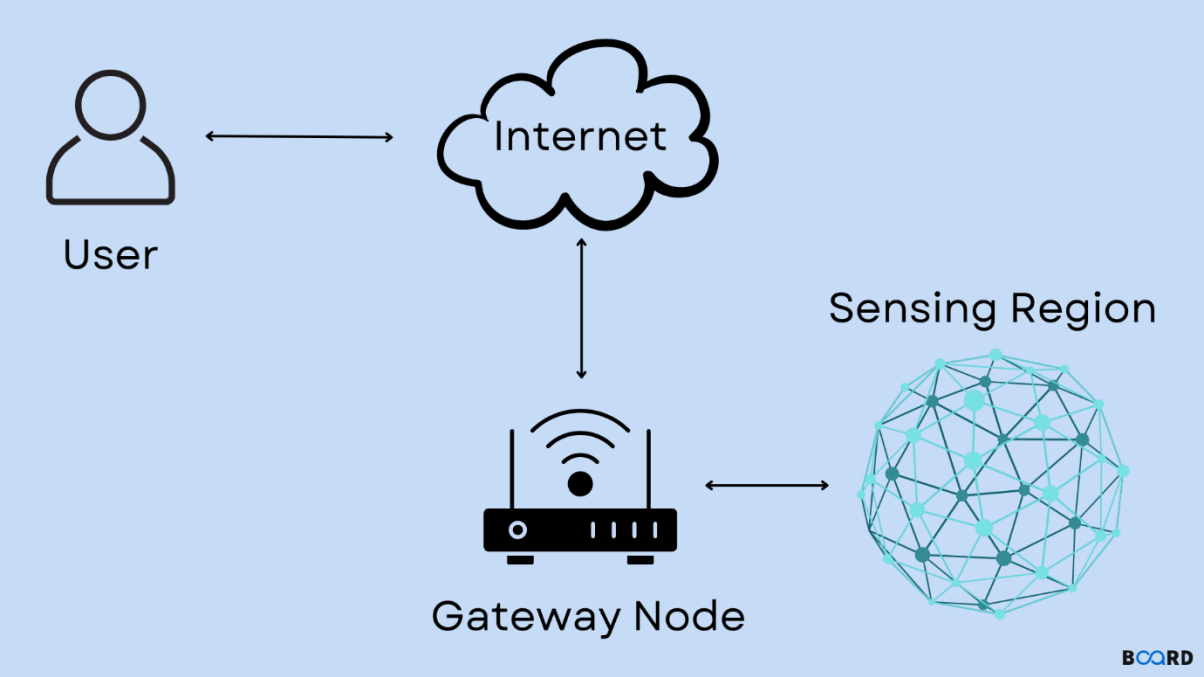


Figure 4. Sensor Networks (boardinfinity.)

Wireless Communications Protocols: IoT devices establish wireless communication over a range of protocols which include Wi-Fi, Bluetooth, Zigbee, LoRaWAN, and cellular networks. Every protocol possesses distinct advantages and disadvantages, rendering it appropriate for various IoT applications depending on aspects such as distance coverage, energy use, and data transmission speed (Borgia, 2014).

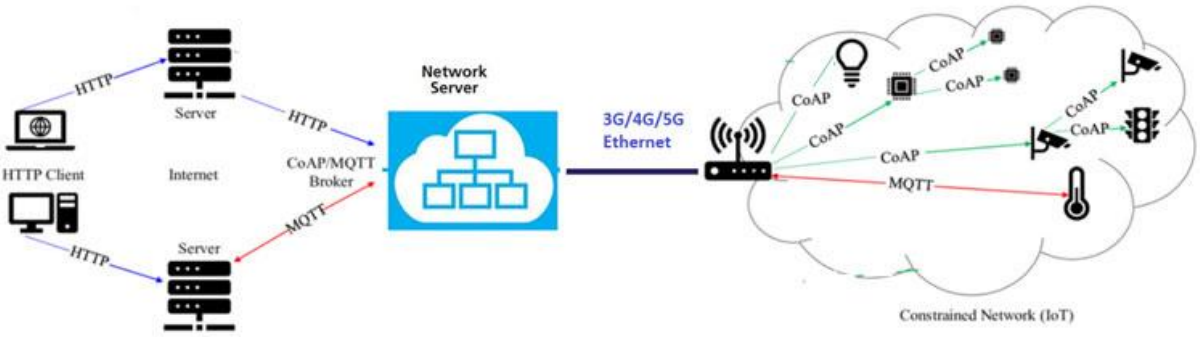


Figure 5. Wireless Network Protocol (Newark.)

Data Analytics: Data analytics is the process of extracting valuable insights and identifying patterns from data generated by the Internet of Things (IoT). These insights are then used to make informed decisions and improve processes. Methods like machine learning, predictive analytics, and anomaly detection are employed to analyse the substantial amount of data produced by IoT devices. (Deng, Xu, & Liu 2019.)

Security and Privacy: Ensuring the utmost security and privacy is of utmost importance when it comes to IoT deployments. This is crucial to safeguard sensitive data and prevent any unauthorized

access. The inclusion of encryption, authentication, access control, and secure bootstrapping is crucial in guaranteeing the confidentiality, integrity, and availability of IoT systems. (Roman, Zhou & Lopez, 2013.)

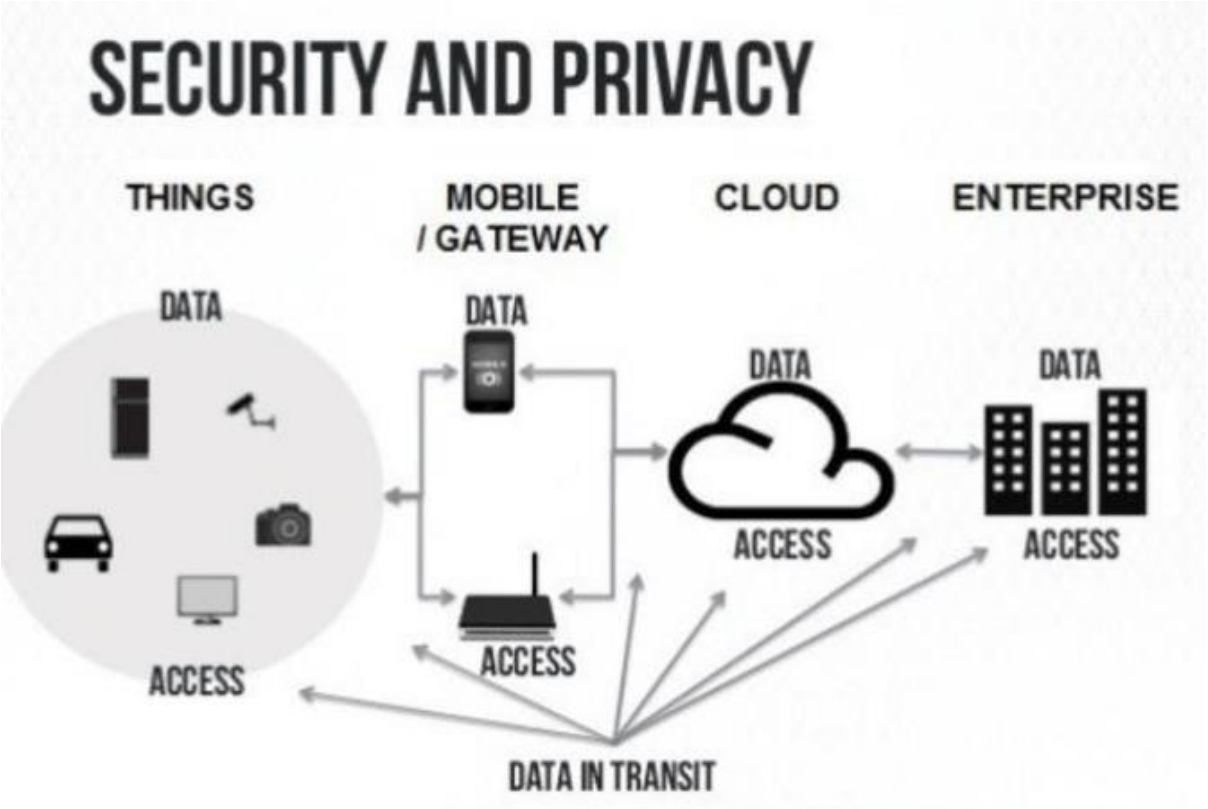


Figure 6. Security and Privacy (Medium 2019.)

2.2 IOT COMMUNICATION PROTOCOLS

MQTT (Message Queuing Telemetry Transport): The communications protocol is specifically intended for small sensors and mobile devices, with a focus on being lightweight. Well-suited for settings with restricted network bandwidth. Highlights the importance of simplicity and efficiency, making it well-suited for IoT applications where minimal power consumption is crucial for long-term viability. (Banks & Gupta 2019.)

CoAP (Constrained Application Protocol): An internet communication protocol designed for use with devices that have limited resources and operate in networks with limited capabilities, such as low power and unreliable connections. The protocols are specifically tailored for machine-to-machine (M2M) applications, including smart energy, and building automation (Shelby, Hartke & Bormann 2014.)

HTTP (Hypertext Transfer Protocol): Although not exclusively an IoT protocol, HTTP is commonly employed for IoT devices that necessitate regular online integration rather than prioritizing low battery usage. Its widespread presence enables seamless integration with web services; however, it is typically less effective than MQTT or CoAP in resource-limited contexts Fielding. (Reschke 2014.)

Security Protocols (TLS/DTLS): Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) are cryptographic protocols designed to provide safe communication across a computer

network. In the realm of Internet of Things (IoT), safeguarding the security and integrity of data sent between devices and services is of utmost importance. (Rescorla 2018.)

3 CYBERSECURITY TERMS AND CONCEPTS

3.1 CYBERSECURITY THREATS IN INTERNET OF THINGS

The Internet of Things (IoT) has revolutionized our technological interactions by linking billions of items to the internet, facilitating smooth communication and automation. The fast increase in IoT devices has brought substantial cybersecurity challenges. IoT ecosystems are vulnerable to many dangers such as data breaches and malicious attacks that can jeopardize the integrity, confidentiality, and availability of linked systems.

Botnets and DDos Attack: Botnets, made up of hacked IoT devices, present a major cybersecurity risk through carrying out extensive Distributed Denial of Service (DDoS) attacks. Malicious individuals might utilize the computational capabilities of IoT devices to coordinate attacks, causing disruptions to essential services and overloading network infrastructure. (Antonakakis et al. 2017.)

Weak Authentication and Credential Management: Several IoT devices have weak authentication systems, often depending on default credentials or insecure authentication protocols. Insufficient authentication methods in IoT systems increase the risk of unwanted access, credential stuffing attacks, and credential leaks, which can jeopardize user privacy and security.(Zhang et al. 2017.)

Firmware and Software Vulnerability: IoT devices often have firmware and software vulnerabilities because of the intricate nature of embedded systems and the absence of consistent updates and fixes. By exploiting these vulnerabilities, criminal actors can carry out remote code execution attacks, insert malware, and compromise device functionality, which poses major dangers to user data and system integrity. (Khan et al. 2019.)

Insecure Communication Channels: Insecured communication lines make IoT data vulnerable to interception, eavesdropping, and man-in-the-middle attacks. Several IoT devices send data across unsecured routes or employ obsolete encryption methods, making sensitive information susceptible to collection and misuse by adversaries. (Al Fuqaha et al. 2015.)

Supply Chain and Third-party Risks: The intricate supply chain network linked to IoT device production brings about extra cybersecurity vulnerabilities. Compromised parts, harmful software updates, and attacks on the supply chain can jeopardize the reliability and trustworthiness of devices, underscoring the significance of supply chain security and managing vendor risks. (O Gorman et al.,2020.)

3.2 CYBERSECURITY CHALLENGES IN INTERNET OF THINGS

The expansion of IoT devices in personal, commercial, and industrial sectors has made cybersecurity concerns on the Internet of Things (IoT) a significant topic of concern. These difficulties originate from the fundamental properties of IoT ecosystems, such as their high interconnectedness, heterogeneity, and sometimes insufficient security capabilities.

The following are some of the challenges cybersecurity in Internet of things.

Heterogeneity and Scalability

The IoT ecosystem includes a wide range of devices with various operating systems, protocols, and security standards. This variation complicates the application of standardized security measures.

With the expansion of IoT networks, there is difficulty in establishing scalable security solutions that can effectively manage a growing number of devices. (Alaba, Granjal & Monteiro 2015; Alaba, Granjal & Monteiro 2017.)

Vulnerability and Attacks

Several Internet of Things (IoT) devices possess constrained processing capabilities and memory, hence limiting the implementation of advanced security techniques. Furthermore, the software and firmware on these devices may lack frequent updates, leaving known vulnerabilities unaddressed. The connection of IoT devices opens new attack surfaces, including device, communication, and application levels, each with its own set of vulnerabilities. (Roman, Lin et al 2013; Roman, Lin et al.2017.)

Data Security and Privacy

The vast quantities of data gathered and communicated by IoT devices provide substantial hazards if accessed or modified by unauthorized individuals, resulting in breaches of privacy and possible monetary harm. (Sicari, Rizzardi et al 2015.)

Legal and Regulatory challenges

Complying with a fragmented set of rules that vary by location and industry presents difficulties for makers and suppliers of IoT devices, which might impede the implementation of worldwide security solutions. The lack of broad global standards for IoT security worsens the challenge of safeguarding IoT ecosystems from cyber-attacks. (Weber, Peppet 2010; Weber Peppet 2014.)

3.3 PRIVACY ISSUES IN INTERNET OF THINGS

Identifying the privacy regulations and concerns is crucial in the context of sustainable IoT because of the very sensitive nature of the data involved. The extensive sensing and data monitoring capabilities of this system result in the generation of a significant quantity of data across several domains, including climate, water, energy, and health. Data privacy and protection are crucial for the effective performance of the system. Nevertheless, various Internet of Things (IoT) devices produce varying quantities of data. One major incentive for safeguarding data is to prevent the disclosure of users' data and to impede the dissemination of protected information. To address the initial scenario, effective screening methods can be employed to mitigate the disclosure of personal information. To safeguard confidential information, it is crucial to establish appropriate training programs to prevent unauthorized disclosure of data.

Privacy problems on the Internet of Things (IoT) are wide-ranging, encompassing data protection, user permission, unwanted access, and larger ramifications for personal privacy. These concerns are worsened by the widespread use of IoT devices, which gather, transmit, and frequently keep massive amounts of personal information.

Figure 7. privacy Issues (resize-ojict.)

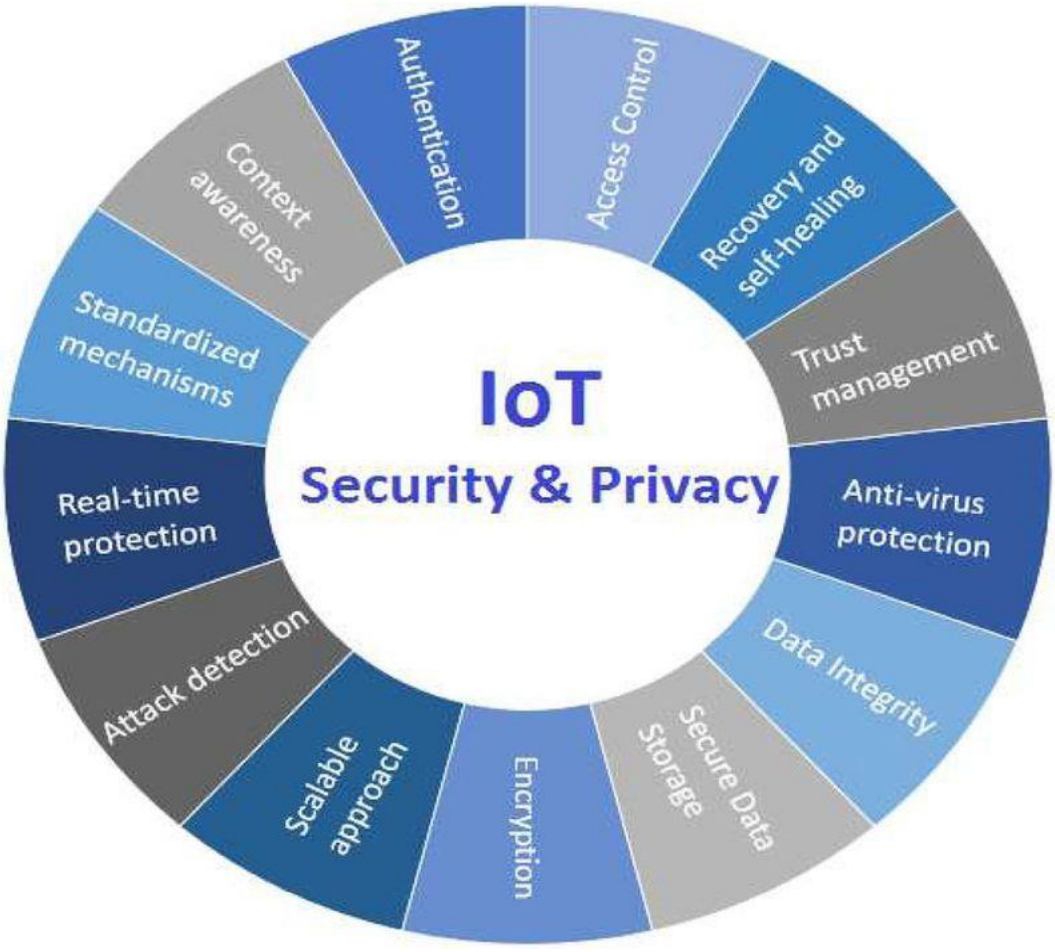


Figure 8. IoT Security and Privacy (resize-ojict.)

3.3.1 DATA PROTECTION AND PRIVACY CONCERN

Personal Data Collection

The Internet of Things (IoT) devices frequently gather copious amounts of personal information, which has raised concerns regarding the data collected, its usage, and the parties with access to it. One of the issues that arouse anxiety is the potential for sensitive data to be collected without the user's explicit consent or awareness. To maintain the level of formality required, please refrain from making any changes to the citation, reference, or in-line citations. Additionally, please ensure that all spelling, specific terms, and phrases adhere strictly to American English. Lastly, please do not alter any numbers in the text. (Weber 2010.)

Consent and Transparency

The complexity and confusion surrounding Internet of Things (IoT) ecosystems often present challenges for users in understanding the data being collected and its intended purpose, which, in turn, raises significant concerns about consent and transparency. (Ziegeldorf, Morchon & Wehrle 2014.)

Data Security and Unauthorized Access

The interconnectivity of IoT devices offers several potential opportunities for exploitation, leading to concerns about data security and the risk of unwanted access. These weaknesses not only endanger personal privacy but also increase the probability of identity theft and fraud. (Roman, Zhou & Lopez 2013.)

3.4 DEVICE COMPROMISE AND DATA THEFT

Description: Hackers leverage weaknesses in IoT devices to obtain unauthorized access, allowing them to steal sensitive data or violate user privacy.

Threat: Device compromise can result in data breaches, which expose personal or private information to unauthorized parties. (Greenberg, A. 2015.)

Malware and Ransomware

Description: Malware particularly designed for IoT devices is employed to remotely infect and manipulate devices or encrypt data in exchange for ransom.

Threat: Malware infestations have the potential to make equipment unusable, undermine the integrity of data, and exploit people for financial profit. (Kolias & Kambourakis 2017.)

3.5 RISK ASSESSMENT AND MITIGATION STRATEGIES IN INTERNET OF THINGS

Conducting risk assessment and implementing mitigation strategies are essential for guaranteeing the security and long-term viability of Internet of Things (IoT) installations. Organizations may reduce vulnerabilities and safeguard IoT systems from security breaches by recognizing possible risks and executing effective mitigation techniques. (Gia et al. 2017.)

3.5.1 Risk Assessment

Prior to deploying Internet of Things (IoT) solutions, businesses should perform thorough risk assessments to identify any risks, vulnerabilities, and repercussions on their systems and operations (Sicari et al. 2015). Risk assessment entails the examination of several elements, including the nature of IoT devices utilized, the data they process, and the communication protocols employed.

The National Institute of Standards and Technology (NIST) Risk Management methodology (RMF) is a widely used methodology for assessing risks on the Internet of Things (IoT) (National Institute of Standards and Technology 2018). The NIST RMF offers a systematic method for recognizing, evaluating, and controlling risks linked to IT systems, including IoT implementations.

3.5.2 Mitigation Strategies

After identifying threats, businesses may employ diverse mitigation measures to decrease the probability and consequences of security breaches in IoT systems.

Secure Device Provisioning: Secure Device Provisioning involves the implementation of secure bootstrapping and device authentication processes. These approaches ensure that only certified devices may access IoT networks (P). (Perera et al. 2014.)

Encryption and Authentication: It is recommended that servers and IoT devices employ secure encryption protocols, including Datagram Transport Layer Security (DTLS) and Transport Layer Security (TLS). Incorporate resilient authentication mechanisms to validate the identities of both users and devices. (Kumar et al. 2017.)

Firmware Update and Patch Management: Ensure the security of IoT devices by upgrading their firmware and software on a regular basis to address known vulnerabilities and security issues. Establish patch management protocols to guarantee prompt installation of security updates. (Alphenaar & Stango 2016.)

Access Control and Least Privilege: Implement access control policies to restrict user and device rights based on the concept of least privilege. Restrict the access to sensitive data and vital system resources only to authorized individuals. (Sicari et al. 2015.)

Monitoring and Incident Response: Implement intrusion detection systems (IDS) and security monitoring tools to promptly identify and address security problems as they occur. Create and implement incident response procedures to swiftly handle security breaches and mitigate their impact on IoT systems. (Gia et al. 2017.)

Organizations can ensure the security, resilience, and sustainability of their IoT ecosystems by integrating risk assessment and mitigation strategies into their IoT deployment processes.

3.6 IMPORTANCE OF SECURE SOFTWARE DEVELOPMENT IN INTERNET OF THINGS

The long-term viability, confidentiality, and safety of IoT systems depend on secure software development techniques. The goal of secure software development is to find security vulnerabilities in software at every stage of its lifetime (SDL) and to fix them or prevent them from happening altogether. (Sommestad et al. 2015.)

Due in large part to the enormous attack surface offered by networked IoT devices, safe software development is of paramount relevance in the IoT. Various devices with different firmware, software stacks, and communication protocols make up most IoT ecosystems (Sicari et al. 2015). Because of this variety, security management becomes more complicated and there are more opportunities for attackers to breach the system.

In addition, there are situations where the processing power, memory, and energy resources of IoT devices are restricted (Roman et al. 2013). Thus, conventional security measures could put a heavy burden on IoT devices, reducing their efficiency and performance. By maximizing security in contexts with limited resources, secure software development approaches aid in overcoming these obstacles.

The possible impact of security breaches on user privacy and safety is another reason why secure software development should be a priority in the IoT. From readings from environmental sensors to private health information, IoT devices gather and handle mountains of sensitive data (Perera et al. 2014). User privacy and trust can be jeopardized if this data is exposed to unapproved access, modification, or theft due to inadequately protected IoT devices.

In addition, public safety, vital infrastructure, and large-scale cyberattacks can all be jeopardized by exploiting vulnerable IoT devices (Kumar et al. 2017). The catastrophic effects of unprotected Internet of Things devices in the hands of malicious actors have been recently shown by events like the Mirai botnet assault. (Antonakakis et al. 2017.)

These risks may be reduced and IoT systems can be built more robust and trustworthy when enterprises include secure software development methods into the IoT development lifecycle. To find and fix security flaws early on in development, it is important to use procedures like code reviews, penetration testing, threat modelling, and secure coding standards. (Alphenaar & Stango 2016.)

Finally, developing safe software for the Internet of Things is crucial. Making security a primary concern from design to deployment and maintenance allows organizations to gain stakeholders' and users' trust and confidence. In the long run, this will make IoT ecosystems more secure, private, and long-lasting.

3.7 PRIVACY PRINCIPLES AND REGULATIONS

Privacy Principles

Data Minimization: Acquire just the essential quantity of personal data required for the intended objective. Minimizing data gathering decreases the likelihood of unwanted access and improper use of personal information. (Cavoukian 2009.)

Purpose Limitation: The principle states that personal data should only be gathered for specific, clear, and lawful objectives, and should not be used in a way that is inconsistent with those aims. Limiting the usage of data to certain objectives promotes openness and ensures that user expectations are fulfilled European Commission. (EU 2016.)

Data Accuracy: it Guarantee that personal data is precise, comprehensive, and current the presence of incorrect data can result in incorrect judgments and erode people's confidence in those who manage the data. (Clarke 2019.)

Privacy Regulations

General Data Protection Regulation (GDPR)

The European Union (EU) implemented regulation to enhance data protection and privacy for its inhabitants. Applicable to global organizations that handle personal data of individuals residing in the European Union. Important provisions include obtaining consent, respecting data subject rights such as access and deletion, notifying individuals in the event of a data breach, and ensuring responsibility. (European Union 2016.)

California Consumer Privacy (CCPA)

The regulation was implemented by the state of California, USA, with the aim of strengthening privacy rights and safeguarding consumer interests. Applicable to enterprises that gather personal information from California citizens, provided that their yearly gross income above a specific level. The key provisions include the right to be informed, the right to have personal data deleted, the right to refuse the sale of personal data, and protection against discriminatory practices. (California Legislative Information 2018.)

Standard for an Architectural Framework for the Internet of Things (IoT)IEEE

IEEE P2413 is an industry standard created by the Institute of Electrical and Electronics Engineers (IEEE) that offers a structured approach for creating Internet of Things (IoT) systems that may operate together and expand in size. IEEE P2413 provides a set of architectural principles, reference models, and interoperability rules to enable smooth integration and communication across different types of IoT devices and platforms (IEEE Standards Association, n.d.). Adhering to IEEE P2413 ensures that IoT installations can work together effectively, are compatible with each other, and can be sustained over time.

Global System for Mobile Communication (GSMA) IoT Security

The GSMA IoT Security Guidelines provides optimal strategies and suggestions for safeguarding IoT devices, networks, and services inside the mobile ecosystem. The standards encompass a wide range of IoT security elements, including as device authentication, data encryption, over-the-air upgrades, and safe bootstrapping (GSMA, 2019). Following the GSMA IoT Security Guidelines assists IoT stakeholders in reducing security risks and safeguarding against cyber-attacks.

Privacy Frameworks

Privacy by Design (PBD)

The framework, created by Ann Cavoukian, focuses on integrating privacy into the design and functioning of systems, processes, and technologies in a proactive manner.

Essential Components: Privacy established as the default option, security that covers the whole communication process, and the ability to see and understand how data is being handled. (Cavoukian 2009.)

National Institute of Standards and Technology (NIST) Privacy Framework

The framework was created by the National Institute of Standards and Technology (NIST) with the purpose of assisting companies in the management of privacy concerns and the establishment of trust among stakeholders.

The system consists of three main components: the core, profiles, and implementation layers. (National Institute of Standards and Technology 2020.)

4 PENETRATION TESTING METHODS AND TOOLS

Penetration testing is a proactive cybersecurity assessment process aimed at discovering vulnerabilities and weaknesses in an organization's IT infrastructure, applications, and network systems. It entails replicating genuine attack situations to assess the security stance and resilience of an organization's digital assets against possible attackers. (Beale 2018.)

Penetration testing is a methodical process that imitates the strategies, methods, and processes used by hostile individuals to breach systems and take advantage of weaknesses. Penetration testing goes beyond vulnerability scanning by actively exploiting vulnerabilities to evaluate their impact and possible hazards, unlike vulnerability scanning which only finds known security problems. (Engebretson 2014.)

4.1 OBJECTIVES OF PENETRATION TESTING

The main goals of penetration testing are:
Identifying security vulnerabilities and weaknesses in the organization's systems, applications, and network infrastructure.
Assessing the efficacy of current security measures, regulations, and protocols in reducing possible risks.
Offering practical insights and suggestions to enhance the organization's security stance and ability to withstand cyber attacks
Complying with regulatory standards and industry criteria for cybersecurity evaluations and audits. (Johnson 2019, 22-23)

Penetration testing adheres to a structured strategy, usually involving the following stages:
Reconnaissance: Gathering information about the target environment, including network topology, system configurations, and potential access points.
Enumeration: It involves identifying active hosts, services, and applications on the target network and collecting further details about their configurations and vulnerabilities.
Vulnerability Analysis: It involves evaluating the security status of target systems by pinpointing recognized vulnerabilities, misconfigurations, and weak spots that may be utilized by attackers.
Exploitation: It involves taking use of known weaknesses to obtain unauthorized access, increase privileges, and compromise targeted systems.
Post-Exploitation: It involves evaluating the consequences of successful assaults, retaining entry to compromised systems, and extracting confidential data.
Reporting: It involves documenting results, such as detected vulnerabilities, exploited holes, and recommendations for fixing them, in a detailed report for stakeholders. (Engebretson 2014, 25-27.)

Penetration testing can be classified into many forms depending on the scope, technique, and objectives of the examination: Penetration testing of networks, Web application penetration testing, wireless penetration testing, social engineering Penetration Testing and Red Team vs. Blue Team Exercise.

4.2 PENETRATION TESTING METHODS

Penetration testing is a critical process in assessing and fortifying the cybersecurity of IoT environments. This approach involves simulating cyberattacks on an IoT system to identify vulnerabilities that malevolent actors could exploit. The realm of penetration testing for IoT is intricate due to the array of devices and technologies that are present.

The following are some penetrations testing methods:

Black Box Testing: Human testers are utilized to evaluate the system's security by simulating an external hacking or cyberattack scenario without any prior knowledge of the system architecture or access credentials. (Weidman 2014.)

White Box Testing: It referred to as clear box testing, this approach grants the tester comprehensive understanding of the system, encompassing its architecture and source code, with the objective of conducting a meticulous and comprehensive security analysis. (Allen, Barnum et al 2008.)

Gray Box Testing: The combination of black box and white box testing methodologies, in which the tester is provided with restricted information of the system, is commonly used to imitate the viewpoint of a privileged user. (Arkin & Stender 2005.)

4.3 PENETRATION TESTING TOOLS

Kali Linux: This is a Linux distribution based on Debian that is specifically created for digital forensics and penetration testing purposes. The suite encompasses a wide range of tools for evaluating network security. (Muniz, & Lakhani 2013.)

Metasploit Framework: It is an open-source initiative that offers details on security weaknesses and assists in doing penetration testing and developing IDS signatures. (Kennedy et al. 2011.)

Wireshark: An application that functions as a network protocol analyser, capturing packets in real-time and presenting them in a format that can be easily understood by humans. Understanding the data flow and identifying abnormalities is crucial. (Sanders 2007.)

Nmap: An advanced network scanning and vulnerability assessment tool designed to detect devices operating within a network and uncover exposed ports and services that may pose security risks. (Lyon 2009.)

Zed Attack Proxy (OWASP): A web application security scanner that is open source. Its purpose is to identify weaknesses in online applications. (OWASP 2023.)

4.4 KALI LINUX

Kali Linux, (previously called Backtrack Linux), is a Debian-based Linux system designed for sophisticated Penetration Testing and Security Auditing. It does this by offering standard tools, settings, and automations that let the user to concentrate on the specific work at hand, rather than the peripheral activities.

Kali Linux is a Linux distribution specifically created for the purpose of conducting penetration testing, digital forensics, and security audits. Kali Linux, created by Offensive Security, is a popular tool among security experts, researchers, and ethical hackers for evaluating the security of different systems and networks, especially those on the Internet of Things (IoT) field. (Offensive Security 2022.)

Kali Linux stands out for its comprehensive array of pre-installed tools and utilities that are expressly designed for the purpose of security testing. The tools encompassed in this category consist of network scanners, vulnerability assessment frameworks, password cracking applications, and wireless attack tools, among other options. (Offensive Security 2022.) Kali Linux offers a complete set of security testing tools that allow users to conduct various security assessments on IoT devices and networks.

Kali Linux is compatible with a wide range of hardware platforms and architectures, which makes it well-suited for testing Internet of Things (IoT) devices that have different hardware setups. (Offensive Security 2022.) Security experts can depend on Kali Linux to offer the essential tools and resources for conducting successful testing and analysis on embedded devices, IoT gateways, and IoT endpoints.

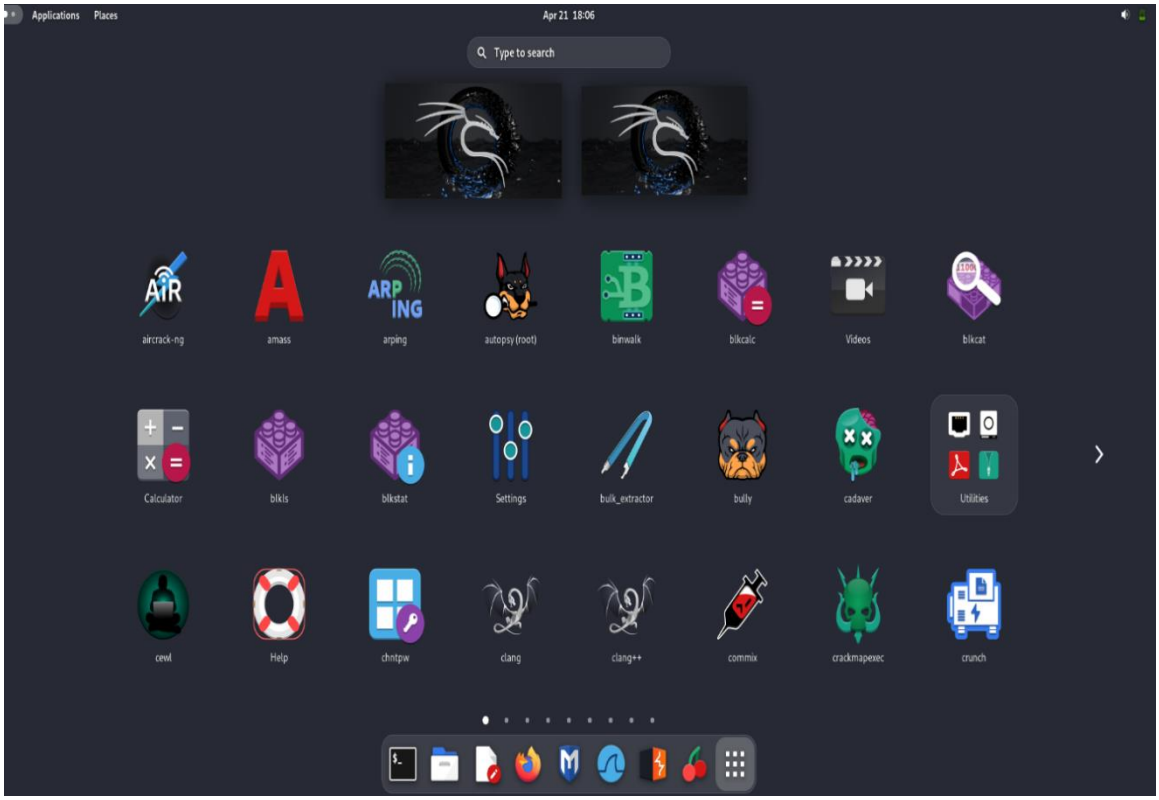


Figure 9. Kali Linux (screenshots.)

4.5 Nmap Scanning Network

Nmap, often known as Network Mapper, is a sophisticated open-source tool that is widely used for network exploration and security evaluation. Nmap, developed by Gordon Lyon (Fyodor), is widely

used by security specialists, network managers, and penetration testers to assess the security of networks, particularly those on the Internet of Things (IoT) space. (Lyon 2022.)

Nmap's versatility and extensive range of capabilities make it perfect for doing security audits, particularly on IoT devices. Nmap's primary objective is to do network scanning by sending packets to specific hosts and evaluating their answers to detect open ports, services, and operating systems. (Lyon 2022.) Nmap is a valuable tool for IoT settings since it can discover IoT devices, visualize their network configuration, and analyse their security risks.

Nmap offers a variety of scanning methods and configurations, allowing users to tailor their scans to individual requirements and goals. Nmap has options for TCP SYN scanning, UDP scanning, version detection, operating system identification, and service listing. (Lyon 2022.) These scanning techniques empower security professionals to gather detailed data on IoT devices and their associated services, facilitating comprehensive security evaluations.

For sustainability, Nmap helps enhance IoT security by allowing security experts to detect and fix security flaws in IoT setups ahead of time. Through utilizing Nmap's network scanning features, companies can increase awareness of their IoT systems, pinpoint security vulnerabilities, and establish suitable security protocols to reduce risks and improve durability.

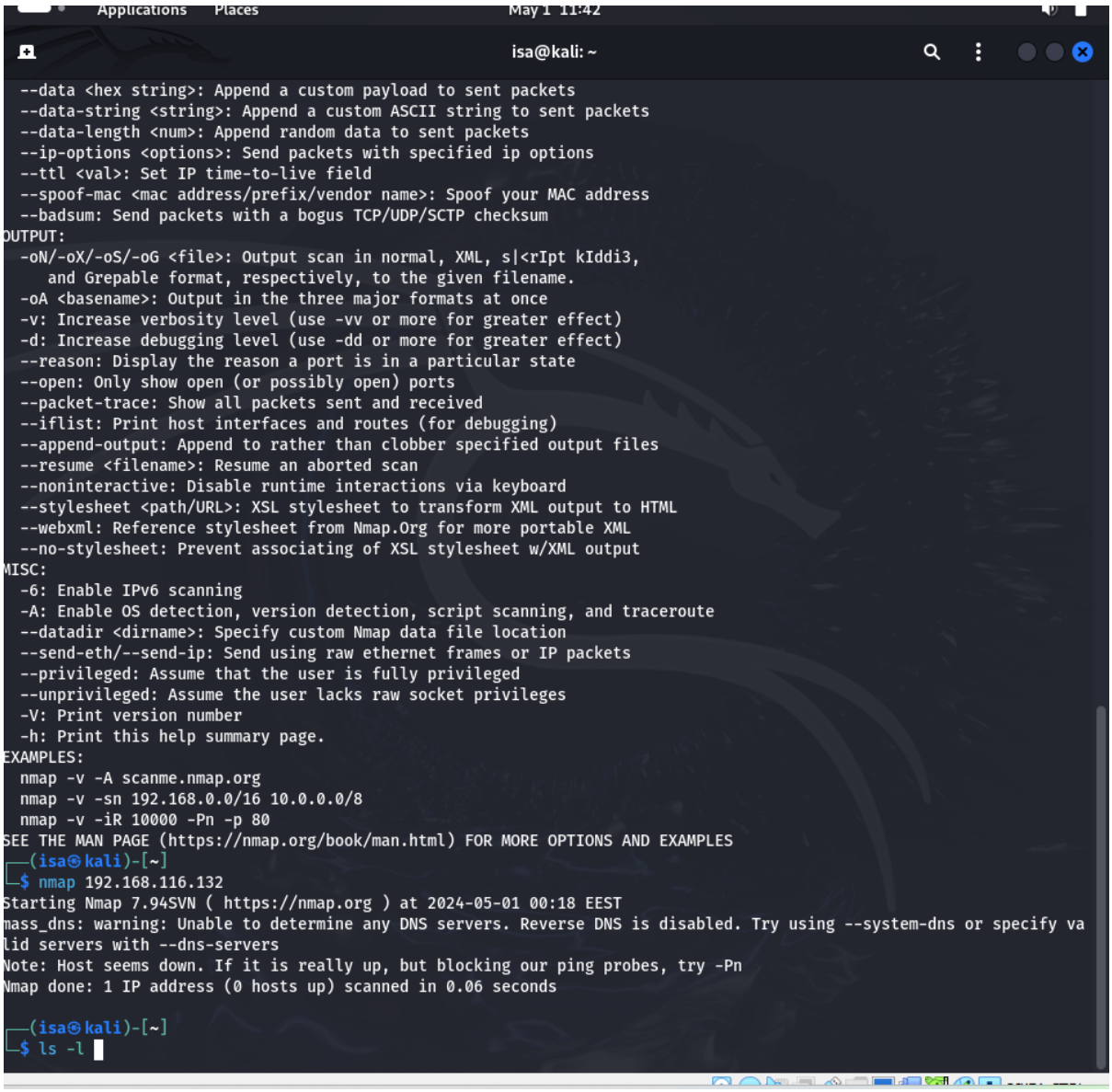


Figure 10. Nmap (screenshot).

4.6 FLIPPER ZERO

Flipper Zero is a little hardware device that has an intriguing personality resembling that of a cybernetic dolphin. It can engage with digital systems in the physical world and increase in size or complexity as it is utilized. Investigate several types of access control systems, such as RFID, radio protocols, and utilize GPIO pins for debugging devices.

Flipper Zero aims to include all the necessary hardware tools for portable exploration and development. Flipper draws inspiration from the pwnagotchi project but distinguishes itself from other DIY boards by prioritizing user-friendly functionality for everyday use.

Flipper Zero operates independently and may be manipulated via a 5-button directional pad, eliminating the need for other devices like computers or smartphone.

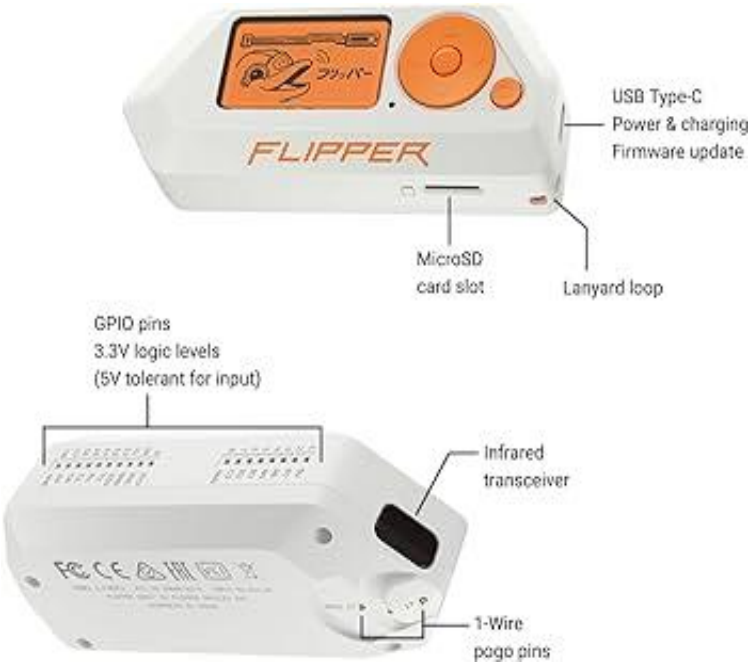


Figure 11.Flipper Zero (Flipper Zero).

Flipper Zero has extensive support for a range of wireless communication protocols typically utilized in IoT devices, including as RFID, NFC, Bluetooth, and Wi-Fi (Flipper Devices, n.d.). This facilitates the examination and engagement of IoT devices that employ these protocols by security researchers and penetration testers, hence enabling thorough security evaluations.

Flipper Zero is supplied with integrated hardware tools including a radio frequency transceiver, an infrared transmitter, and an integrated circuit (IC) programmer (Flipper Devices, n.d.). These technologies let users to conduct activities including intercepting wireless communications, simulating RFID/NFC cards, and updating firmware on specific devices, hence simplifying comprehensive research, and testing of IoT systems.

The specified range pertains to a broad category of wireless devices and access control systems, including but not limited to garage door remotes, boom barriers, IoT sensors, and remote keyless systems. Users may enhance the functionality of their Flipper Zero device by installing supplementary applications that enable the retrieval of data from a diverse range of devices, such as weather stations.

5 IOT FOR SUSTAINABILITY

5.1 IMPORTANCE AND BENEFIT OF TRIPLE BOTTOM LINE (TBL)

The following are some of the importance and benefit TBL.

Impact Assessment: The Triple Bottom Line (TBL) facilitates a comprehensive assessment of an organization's influence on the global world. It transcends the limited boundaries of financial profits and delves into the complex network of social, human, and environmental aspects. This comprehensive assessment offers a subtle comprehension of the organization's function within the larger ecosystem.

Integrating with sustainability goals: Embracing the Triple Bottom Line (TBL) framework places firms as proactive participants in achieving sustainability objectives. Organizations that include social responsibility and environmental stewardship into their core operations are in line with global initiatives to promote a more sustainable future. This alignment is advantageous for the earth and is well received by stakeholders who are placing a growing emphasis on ethical and ecological activities.

Improving long-term sustainability: The Triple Bottom Line (TBL) is more than a theoretical framework; it is a crucial strategy for ensuring the long-term survival and success of an organization. As organizations adapt to a constantly changing environment, those who consider the Triple Bottom Line (TBL) are in a more advantageous position to overcome obstacles. This strategy reduces the potential negative impacts related to shifting cultural norms, unpredictable environmental conditions, and economic instability, promoting the ability to bounce back and adjust.

Societal importance: In along with financial success, the Triple Bottom Line (TBL) enhances an organization's societal relevance. In a time when customers, investors, and workers are becoming more socially aware, firms that prioritize the three Ps (people, planet, and profit) can establish credibility and earn confidence. This societal significance goes beyond financial gains, establishing a favourable reputation that appeals to a wide range of individuals and groups involved.

Multidisciplinary decision-making: TBL promotes a comprehensive approach to decision-making, where the impacts of actions are assessed in terms of their economic, social, and environmental aspects.

Enhanced business reputation: Implementing the Triple Bottom Line (TBL) framework may enhance a company's image by promoting goodwill among communities and environmentally concerned consumers.

Safety mitigation: The Triple Bottom Line (TBL) assists organizations in anticipating and reducing risks related to evolving public expectations and environmental difficulties by considering social and environmental aspects.

5.2 IMPROVING THE TRIPLE BOTTOM LINE WITH SUSTAINABILITY

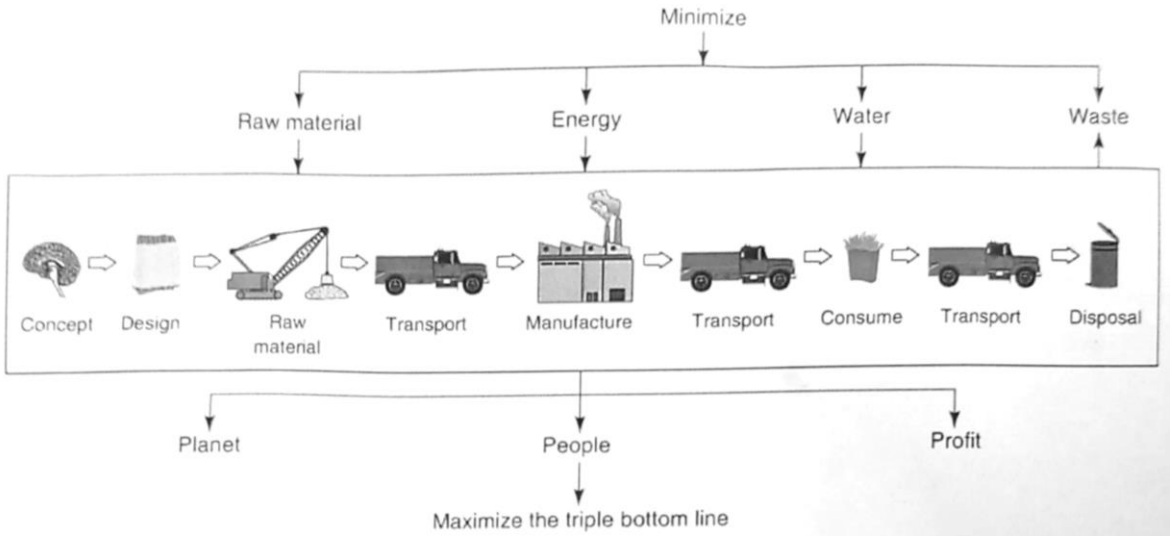


Figure 12. Improving the Triple Bottom Line (Screenshot).

-

Triple bottom describes an approach in business that focuses on three key aspects of sustainability: social, environmental, and financial performance. As an expert in corporate responsibility and sustainable development, the TBL seeks to go beyond traditional profit-focused approaches, encouraging firms to consider a wider range of effects. In contrast to conventional frameworks that focus solely on financial aspects, the Triple Bottom Line (TBL) acknowledges the interdependence of economic prosperity, social accountability, and environmental preservation. The Triple Bottom Line (TBL) incorporates ecological and social factors into the evaluation process, providing a holistic assessment of an organization's global influence.

Triple Bottom Line have three branch which include People, Profit and Planet (3Ps):

People: The social portion, represented by the term 'People', explores multiple dimensions of society. TBL emphasizes a complicated network of human factors is that affect and are impacted by an organization's operations, including unemployment rates, education levels, and health-adjusted life expectancy.

Profit: Within the framework of TBL, profit encompasses not just monetary benefits but also encompasses a wider range of economic factors. It encompasses aspects such as individual earnings, business environmental conditions, and sector-specific revenue distribution, therefore indicating the financial well-being and adaptability of the organization.

Planet: Environmental sustainability is a fundamental principle of the Triple Bottom Line (TBL). This dimension evaluates an organization's influence on the environment, including issues such as air and water quality, energy use, and land utilization. It underscores the obligation of corporations to maintain natural integrity.

5.3 INTERNATIONAL ENVIRONMENTAL POLICIES AND STANDARDS IN IoT FOR SUSTAINABILITY

Global environmental rules and standards have a substantial influence on the development, deployment, and management of Internet of Things (IoT) technology. The policies and guidelines seek to encourage sustainability while mitigating environmental consequences. Here is a comprehensive summary of key global legislation and regulations regarding the Internet of Things (IoT) and its influence on sustainability:

1. Paris Agreement: The Paris Agreement is a global accord ratified by the United Nations Framework Convention on Climate Change (UNFCCC) in 2015. The objective of the agreement is to restrict the rise in global temperatures to a level much lower than 2 degrees Celsius over the levels seen before industrialization, and to actively work towards limiting the temperature increase to 1.5 degrees Celsius. The Paris Agreement promotes the establishment and attainment of nationally determined contributions (NDCs) by nations to decrease greenhouse gas emissions and shift towards low-carbon economies (United Nations, 2015). The utilization of IoT technology can facilitate the attainment of the objectives outlined in the Paris Agreement by enhancing the effectiveness of resource allocation, integrating renewable energy sources, and monitoring emissions.

2. ISO 14000 Series: Environmental Management Standards: The ISO 14000 series is a collection of global standards created by the International Organization for Standardization (ISO) to construct environmental management systems (EMS) and promote the use of best practices for enhancing environmental performance. ISO 14001 is the central standard in the series, including instructions for establishing an Environmental Management System (EMS) to recognize, control, and reduce environmental effects. (ISO, n.d.) Adhering to ISO 14001 standards enables enterprises to guarantee environmental sustainability in their operations, including the use of IoT.

3. Eco-design Directives: The Eco-design law, officially referred to as Directive 2009/125/EC, is an EU law that seeks to foster energy efficiency and environmental sustainability by imposing design criteria on products. The regulation sets down the minimum criteria for energy efficiency and eco-design requirements for energy-related items that are supplied in the EU market, which includes IoT devices (European Commission, n.d.). Adhering to the Eco-design Directive motivates manufacturers to create Internet of Things (IoT) products that are energy-efficient and have a minimal environmental footprint during their entire lifespan.

4. WEEE Directive: The Waste Electrical and Electronic Equipment (WEEE) regulation, specifically Directive 2012/19/EU, is an EU regulation that focuses on the handling and disposal of waste electrical and electronic equipment. The regulation establishes criteria for the gathering, processing, reusing, and discarding of electronic waste to reduce its ecological consequences and encourage the retrieval of valuable resources. (European Commission, n.d.) Manufacturers and stakeholders on the Internet of Things (IoT) market must comply with the Waste Electrical and Electronic Equipment (WEEE) Directive. This directive guarantees that IoT devices that have reached the end of their lifespan are disposed of and recycled in a responsible and ethical way.

5. ITU-T Recommendation on ICT and Climate Change: The International Telecommunication Union (ITU) has created a set of standards and benchmarks for the function of information and communication technologies (ICTs) in reducing the impact of climate change and advancing environmental

sustainability. ITU-T L.1410 offers guidelines for evaluating the ecological consequences of ICTs and implementing energy-efficient ICT solutions. (ITU, n.d.) IoT stakeholders may utilize ITU-T principles to create and implement sustainable IoT solutions that reduce energy usage and carbon emissions.

5.4 ROLE OF IOT IN SUSTAINABILITY EFFORTS

Energy Efficiency: Internet of Things (IoT) devices possess the potential to significantly decrease energy consumption by automating the management of lighting, heating, ventilation, and air conditioning (HVAC) systems in intelligent buildings. By utilizing data analytics, IoT applications can enhance energy efficiency and diminish the environmental impact through decreased carbon emissions. The American English language should be employed, adhering to its spelling, specific terms, and expressions. (Pérez-Lombard, Ortiz & Pout 2008.)

Resource Management: Smart farming employs the Internet of Things (IoT) technology to increase crop production while conserving water resources. This is achieved by monitoring soil moisture levels and adjusting irrigation accordingly. In a similar vein, IoT systems in smart cities can improve waste management by implementing intelligent collection systems that decrease operational expenses and minimize environmental impact. (Wolfert, Ge, Verdouw & Bogaardt 2017.)

Environmental Monitoring: IoT sensors placed throughout ecosystems can monitor environmental factors such as air and water quality in real time, allowing for pollution detection and catastrophe response. This competence is critical for conserving natural resources and maintaining ecosystem health. (Zanella, Bui, Castellani, Vangelista & Zorzi 2014)

Sustainability programs using IoT technology require environmental monitoring. Sensors and IoT devices in environmental monitoring systems provide real-time data gathering, analysis, and administration, improving agricultural, urban planning, and natural resource management decision-making. (NAMIOT 2020.)

IoT-enabled environmental monitoring systems are more accurate, scalable, and cost-effective than traditional techniques. (Elkadeem et al. 2019.) These devices can measure air, water, soil, temperature, and humidity to provide environmental patterns.

IoT sensors in agricultural fields may monitor soil moisture and weather to optimise irrigation schedules, minimize water use, and maximise crop output (Cavalcante et al., 2019). IoT-based air quality monitoring systems can assist urban planners and policymakers detect pollution hotspots, focus actions, and enhance public health. (Palaniappan et al. 2018.)

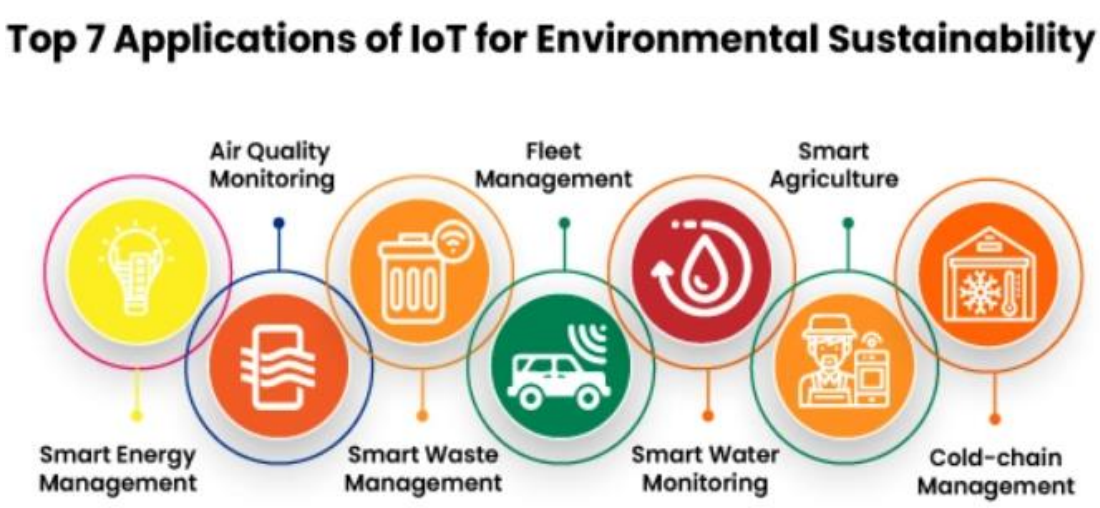
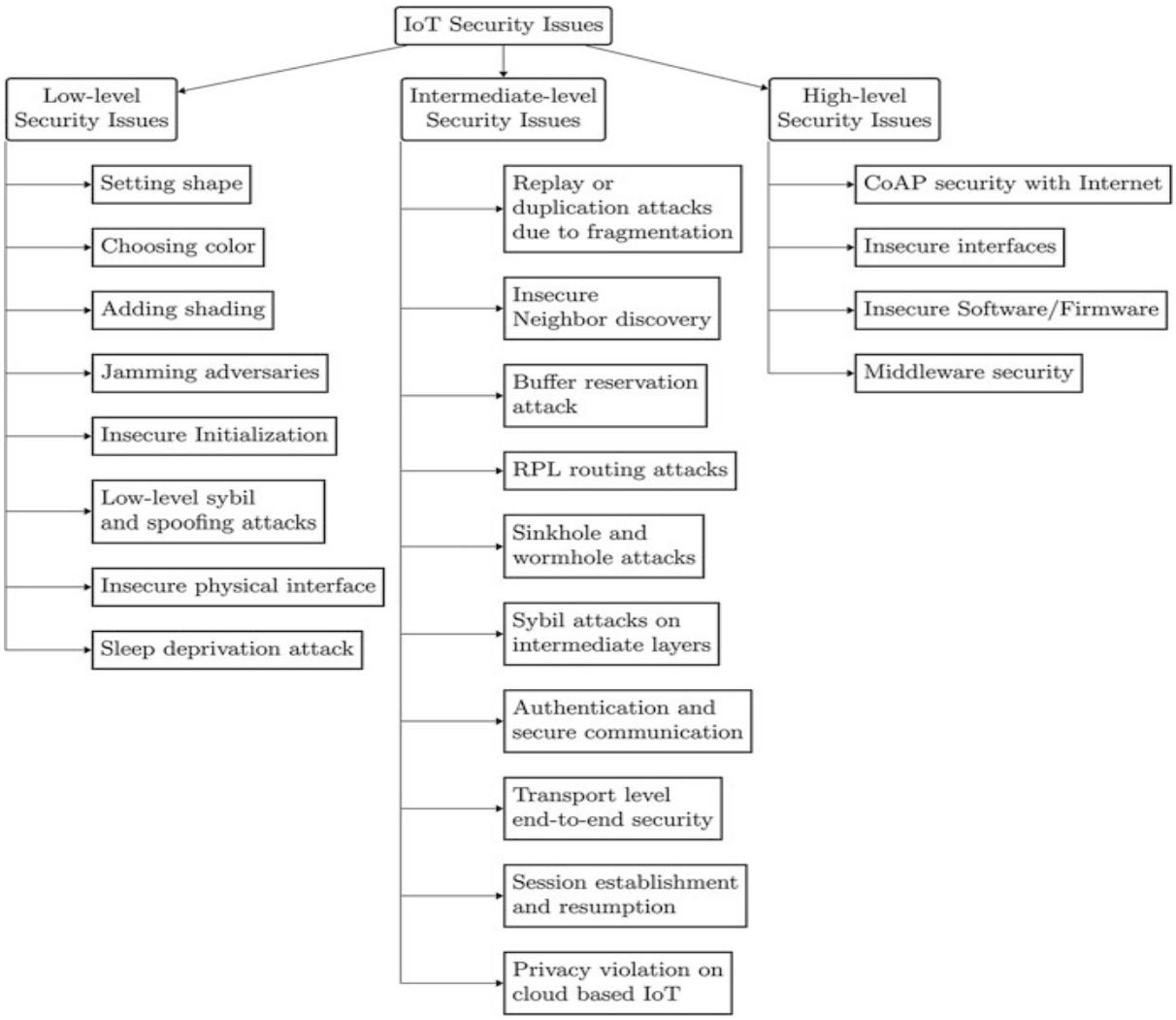


Figure 13. Environmental Sustainability (conurets 2022)

5.5 SECURITY ISSUES IN IoT FOR SUSTAINABILITY



Security issues in IoT. (Khan M. A & Salah K 2018.)

The following are some of the Security of Issues for Internet of things.

Vulnerability in IOT Devices

Limited processing power and Memory: IoT devices with limited resources are vulnerable to assaults like buffer overflows and denial-of-service (DoS) attacks. (Ray 2017.)

Insecure Communication Protocols: Insufficiently protected communication protocols can make IoT devices vulnerable to interception and modification of data, which can compromise the integrity and confidentiality of information. (Hossain & Muhammad 2016.)

Inadequate Authentication: A significant number of IoT devices lack strong authentication measures, rendering them susceptible to unwanted access and control. (Al-Fuqaha, et al 2015.)

Weak Encryption: The encryption used in IoT devices is sometimes inadequate or absent, which makes data transfer susceptible to surveillance and manipulation. (Roman 2013.)

Privacy Concerns in IOT Systems

Data privacy Risks: Internet of Things (IoT) systems gather vast quantities of personal and sensitive information, which gives rise to worries over illegal entry, improper usage, and breaches of data security. (Atzori, et al. 2010.)

Lack of User Awareness: Users may lack sufficient awareness regarding the data gathered by IoT devices and the possible privacy consequences, resulting in inadvertent exposure of confidential information. (Al-Fuqaha, et al. 2015.)

Security Frameworks for Sustainable IOT

End-to-End Encryption: By using end-to-end encryption, data is kept secret and safe during transmission and storage, reducing the chances of interception and eavesdropping. (Chowdhury, et al. 2017.)

Blockchain Technology: Blockchain offers a distributed and unalterable framework for guaranteeing the authenticity and traceability of information in IoT systems, improving security and visibility. (Dorri, et al. 2017.)

Lack of updatability and Patch Management

Limited Updatability: A significant number of IoT devices do not have the necessary procedures to receive and install security updates, which means they remain constantly susceptible to known vulnerabilities. (Sheng, 2016.)

Patch Management: Despite the presence of updates, IoT ecosystems sometimes lack centralized management mechanisms to effectively distribute fixes across a substantial number of devices.

Interoperability and Standards

Interoperability Issues: The diversity of IoT devices and protocols poses difficulties for smooth integration and the establishment of standardized security measures. (Sicari, Rizzardi, et al. 2015.)

Lack of Security Standards: The lack of globally recognized security standards for IoT worsens interoperability problems and impedes the advancement of secure IoT solutions. (Gubbi, Buyya 2013.)

5.6 REGULATORY AND ETHICAL CONSIDERATIONS

Regulatory Framework

The current regulatory frameworks, such as the General Data Protection Regulation (GDPR) in the European Union, aim to address certain privacy concerns related to the Internet of Things (IoT) by imposing stricter consent requirements and allowing individuals to have greater control over their personal data. However, the global and heterogeneous nature of the IoT presents challenges for the effective implementation and adequacy of these regulations. (Peppet 2014.)

Ethical Considerations

The use of Internet of Things (IoT) technologies raises important ethical considerations beyond legal obligations. These include ensuring user privacy, obtaining informed consent, and minimizing potential harm. Ethical principles and guidelines are essential in guiding developers and manufacturers to adopt responsible data practices. (Wright & Raab 2014.)

5.7 SECURITY STANDARDS AND PROTOCOLS IN INTERNET OF THINGS FOR SUSTAINABILITY

Establishing stringent security standards and protocols is essential for the long-term use of Internet of Things (IoT) technology. Various organizations and consortia have created standards and protocols to tackle the distinct security concerns presented by IoT ecosystems. (Perera et al. 2014.)

The ISO/IEC 27001 series is a well-known security standard for the Internet of Things that provides a thorough framework for creating, executing, maintaining, and enhancing an information security management system. ISO/IEC 27001 assists enterprises in recognizing and minimizing security vulnerabilities, especially those pertaining to Internet of Things (IoT) devices and systems. (ISO/IEC 2013.)

The NIST Cybersecurity Framework, established by the National Institute of Standards and Technology (NIST) in the United States, is a significant security standard for IoT. The NIST framework offers a collection of rules, optimal methods, and concepts for managing risks and improving the ability of critical infrastructure sectors, including IoT, to withstand and recover from cybersecurity threats.

Various security procedures are utilized alongside standards to ensure the security of communication and data sharing in IoT contexts. Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) are commonly used protocols to ensure the security of communication between Internet of Things (IoT) devices and servers. (Kumar et al. 2017.) TLS and DTLS offer cryptographic protocols that safeguard sensitive data by providing encryption, authentication, and data integrity procedures, preventing unauthorized access and manipulation.

In addition, resource constrained IoT devices commonly utilize lightweight cryptographic methods such as Elliptic Curve Cryptography (ECC) and Symmetric Encryption to reduce computational overhead and memory usage. (Roman et al. 2013.) These algorithms guarantee both efficient and secure communication while also preserving device resources.

In IoT ecosystems, it is crucial to strictly follow security standards and protocols to establish trust, promote compatibility, and reduce security threats. By adhering to established standards such as ISO/IEC 27001 and utilizing suggested security protocols like TLS and DTLS, stakeholders may improve the security of IoT installations and support long-term development.

5.8 PRIVACY RISKS IN INTERNET OF THINGS DEVICES AND SERVICES FOR SUSTAINABILITY

Data Collection and Usage Risks

Excessive Data Collection Issue:

IoT devices could gather excessive data beyond what is required for their intended function, which might result in privacy violations. Excessive accumulation of data raises the likelihood of unlawful entry, misuse, and profiling. (Sicari & Rizzardi 2015.)

Secondary Use of Data

There is a risk that personal data acquired by IoT devices may be used for different purposes or shared with third parties without the explicit agreement of the users. Secondary utilization of data gives rise to worries over privacy infringements and the relinquishment of authority over personal information. (Kosta, Pierson & Kalloniatis 2019.)

Security Vulnerabilities

Lack of Encryption Issue:

Insufficient encryption may result in the interception or alteration of data during transmission between IoT devices and cloud services. Without encryption, sensitive information, such as environmental sensor data and user preferences, is susceptible to interception and unauthorized access. (Roman, Zhou & Lopez 2013.)

Weak Authentication

IoT devices that use weak, or default passwords are vulnerable to unauthorized access, which can lead to privacy breaches by malevolent individuals. Weak authentication techniques enable unlawful manipulation of equipment and unauthorized entry into sensitive data. (Al-Fuqaha & Guizani 2015.)

Data Security Breaches

Data Breaches

There is a possibility of data breaches in IoT devices and services, which might lead to the disclosure of sensitive personal information.

Data breaches undermine user privacy, diminish confidence in IoT ecosystems, and can result in significant legal and financial ramifications. (Dhillon & Moores 2001.)

5.9 PRIVACY-PRESERVING TECHNIQUES FOR SUSTAINABILITY

Data minimization objective: Reduce privacy concerns by minimizing the acquisition and keeping personally identifiable information (PII).

Methods: Employ data anonymization, aggregation, and pseudonymization to decrease the level of detail in the gathered data (European Union Agency for Cybersecurity. (ENISA 2015.)

Differential Privacy

Description: The purpose is to provide noise or disturbances to query results to safeguard individual privacy while yet enabling valuable data analysis.

Methods: Utilize differential privacy strategies such as the insertion of Laplace noise or randomized response approaches. (Dwork 2011.)

Secure Multiparty Computation (SMC)

Purpose: Enable many entities to collaboratively perform a computation on their respective inputs while maintaining the privacy of those inputs.

Methods: Utilize cryptographic techniques such as homomorphic encryption or secure function evaluation. (Lindell & Pinkas 2008.)

Privacy-Preserving Authentication

Description: Verify the identity of users without disclosing confidential authentication information.

Techniques: Utilize cryptographic techniques such as zero-knowledge proofs or identity-based encryption.

Federated Learning

Purpose: Facilitate the training of machine learning models on numerous decentralized edge devices without the need to share raw data.

Methods: Utilize strategies such as combining models, implementing secure aggregation procedures, and incorporating differential privacy. (Kairouz, et al. 2019.)

5.10 HEALTH AND CYBERSECURITY FOR SUSTAINABILITY

Cybersecurity weakness and attacks have the potential to adversely affect the accessibility of essential life- saving healthcare supplies and data. Cybersecurity risk can cause bodily harm to patients and disturb the regular operations of hospitals, making them incompetent of providing health for humans. Hence, attaining the maximum level of cybersecurity in the medical field is important to ensure patient safety. Identify theft, ransomware and target patient hacking are among the security holes. (Cauteruccio et al. 2019.)

5.10.1 SOME MAJOR FACTORS AFFECTING HEALTHCARE CYBERSECURITY

The problem face by the healthcare sectors in Cybersecurity has follows.

In the healthcare sector is experiencing a shortage of trained security experts.

The equipment consists of ancient or depreciated hardware and equipped with insecure operating systems.

The frequent occurrence of patient care failures, including being locked by ransomware, offers significant challenges to the healthcare sector. (Brewcznska et al. 2019.)

Resistance to recognize and resolved identified weakness. (Kapellmann & Washburn 2019.)

The lack of financing enables the operation of equipment without any assistance. The network architecture emphasizes hyper connection over security indication. (Fredette et al. 2012.)

Case studies

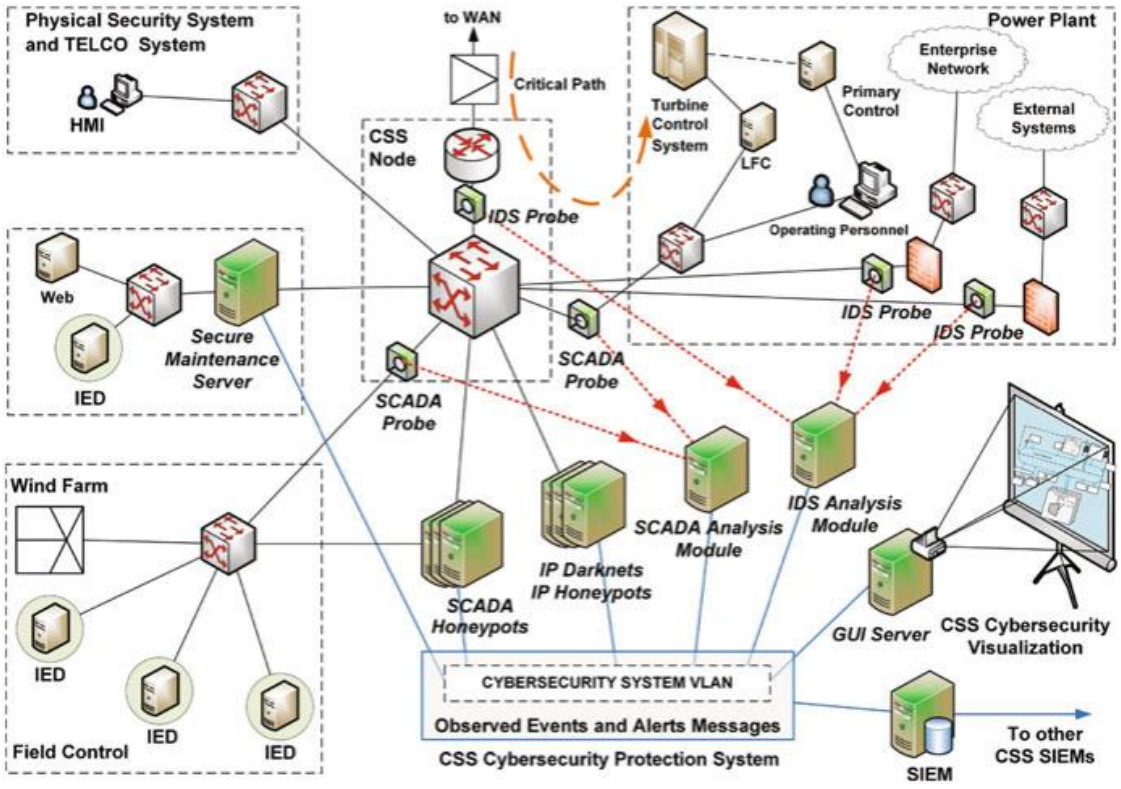


Figure 14.Cybersecurity Protection System (Jarmakiewicz 2017.)

6 FUTURE VISIONS

6.1 TRENDS IN IoT FOR SUSTAINABILITY

The Internet of Things (IoT) has been experiencing fast evolution, and emerging trends are changing the way IoT technologies are used to promote sustainability. These developments involve advancements in other fields, such as energy management, environmental monitoring, smart agriculture, and urban planning. (Gubbi et al. 2013.)

Edge Computing : The importance of edge computing in the context of the Internet of Things (IoT) has increased due to its pivotal role in advancing sustainability. Data analysis and processing can take place near IoT devices, namely at the network edge. Edge computing improves the effectiveness of Internet of Things (IoT) systems in environments that have restricted resources, such as rural agricultural regions and industrial sites. To accomplish this goal, a successful strategy is to reduce both the quantity of data delivered and the time delay. (Mouradian et al. 2019.)

Artificial Intelligence (AI) and Machine Learning (ML): Artificial intelligence (AI) and machine learning (ML) are gaining significance in Internet of Things (IoT) applications focused on sustainability. Artificial intelligence algorithms have the capability to analyze vast quantities of Internet of Things (IoT) data to identify trends, optimize the utilization of resources, and predict changes in the environment. Artificial intelligence-powered predictive maintenance systems could identify equipment issues in industrial Internet of Things (IoT) configurations, resulting in reduced periods of inactivity and enhanced use of resources. (Atzori et al. 2010.)

Blockchain Technology: Blockchain is being developed to enhance the security, transparency, and accountability of IoT networks, with the aim of fostering sustainability. Blockchain facilitates safe and verifiable transactions across IoT devices and stakeholders by offering a tamper-resistant distributed ledger. Blockchain technology in supply chain management enables the tracing of the origin of goods, verification of their sustainability credentials, and mitigation of the risk of fraudulent activities or counterfeiting. (Dorri et al. 2017.)

5G Connectivity :5G networks are expected to speed up the use of IoT technologies for sustainability by providing faster, more reliable, and low-latency connection. 5G enables real-time communication between Internet of Things (IoT) devices and cloud platforms, allowing for the creation of applications like smart grids, intelligent transportation systems, and remote healthcare monitoring. 5G networks offer enough bandwidth and little latency, making them well-suited for emerging IoT applications such as augmented reality (AR) and virtual reality (VR) applications for environmental education and awareness. (Li et al. 2017.)

Circular Economy Initiatives: The adoption of Internet of Things (IoT) technology is becoming more prevalent in supporting circular economy projects. The initiatives aim to minimize waste, save resources, and promote sustainable habits in consumption and production. Intelligent waste management systems, which make use of Internet of Things (IoT) technology, enhance garbage collection routes, offer real-time monitoring of waste levels, and improve recycling and composting operations. Moreover, the use of Internet of Things (IoT) technology enables manufacturers to sell products through a product-as-a-service (PaaS) model, where products are provided on a subscription basis.

This method promotes the adoption of reusing, repairing, and remanufacturing techniques, which are considered more advantageous when compared to conventional ownership models. (Geissdoerfer et al. 2017.)

6.2 FUTURE CHALLENGES AND OPPORTUNITIES ON THE INTERNET OF THINGS FOR SUSTAINABILITY

As the Internet of Things (IoT) develops, there are numerous challenges and opportunities that need to be tackled with the aim to accomplish sustainability. To fully harness the potential of IoT in promoting sustainability in many areas, it is essential to tackle these problems and take advantage of the opportunities.

Interoperability and Standards: Establishing compatibility across various devices and systems is essential for the sustained existence of the Internet of Things (IoT). To ensure smooth communication and integration across many devices and platforms in the increasingly complex and diverse IoT ecosystems, it is crucial to establish accessibility standards. (Gubbi et al. 2013.) By incorporating standardized data formats, communication protocols, and device compatibility, the development of scalable and interoperable Internet of Things (IoT) solutions for sustainability will be streamlined.

Data Privacy and Security: The future of IoT for sustainability depends extensively on addressing and prioritizing privacy and security concerns. With the expansion and diversification of IoT projects, the amount of confidential information gathered and transferred by IoT devices grows rapidly, leading to issues over the protection of data privacy, confidentiality, and integrity. (Sicari et al. 2015.) To tackle these concerns, it is necessary to use strong security measures, encryption methods, and privacy-preserving approaches to protect sensitive information and reduce the likelihood of data breaches and assaults.

Energy Efficiency and Resource Optimization: To accomplish sustainability in IoT installations, it is crucial to prioritize energy efficiency and optimize resource utilization. Several IoT devices function in regions with restricted resources and a limited power supply. Hence, it is imperative to utilize energy-efficient designs and optimization methods to extend battery life and reduce energy usage. (Jennings et al. 2015.) Furthermore, it is important to optimize the consumption of resources such as water, energy, and raw materials to reduce the environmental effect and foster sustainable growth.

Ethical and Social Implication: The widespread implementation of IoT technology gives rise to ethical and societal concerns that need to be resolved to achieve sustainability. The ethical concerns for IoT installations involving personal or sensitive information, such as data ownership, permission, and responsibility, are of great importance. (Miorandi et al. 2012.) Furthermore, it is crucial to develop Internet of Things (IoT) solutions that give high importance to social inclusion and equality. This involves ensuring that underprivileged people have fair and impartial access to technology and may fully benefit from the favourable results it offers.

Regulatory and Policy Framework: Establishing strong regulatory and policy frameworks will be crucial in guiding the responsible implementation and management of IoT technologies for sustainability purposes. It is crucial for governments and regulatory bodies to work together with industry

stakeholders to develop and enforce standards, regulations, and guidelines that encourage innovation while also protecting public interests, privacy rights, and environmental sustainability. (Fortino et al. 2017.) Regulations encompass data protection, cybersecurity, environmental standards, and ethical guidelines for IoT deployments.

6.3 RECOMMENDATIONS FOR IMPROVING PRIVACY AND CYBERSECURITY

The governments agency should ensure that the security of data should protected when is being transferred between the IoT devices and the backend servers and when it being stored on devices or cloud, encryption of protocols such as Advance Encryption Standard (AES) and Transport Layer Security (TLS) must be used.

The used of robust authentication mechanisms such as multi-factor authentication (MFA) and biometric authentication are used to make sure that only authorized users and devices should have access to IoT system.

The used of systematic approach for regularly updating the software and firmware on IoT devices is important for minimizing security threat and reduce vulnerability.

The introduction of policies control to limited user and device is rights according to the concept of least privilege guarantee the only essential permission are given to do some certain activities.

The used of intrusion detection system (IDS), network monitoring tools to identify and get abnormal network traffic patterns that may give unauthorised access to IoT devices.

Internet of things (IOT) technology has become a vital part of our everyday systems, lifestyle and business which needs to sustain and protected from cyber-attack. In other to prevent malicious attack on our database, cybersecurity and privacy on database need to be sustained.

Cybersecurity in internet of things for sustainability is the process of protecting the systems, sensors, and wireless communication from digital attacks. (Abdul Salam Purdue University). It is also important to ensure that the sustainable Internet of things (IOT) paradigm will operate in safe and secure environment to achieve sustainability goals using system, which is dependable, reliable, and trustworthy. (Brass et al. 2018.) Cybersecurity risk for systems monitoring and sensors are different from the traditional networking systems in the following ways:

The sensing data in some of the sustainability tradition takes more time to accumulate such as education, Health, Agriculture and Climate which prolong exposure related security problems. (Salam & Shah et al. 2017; Salam & Shah 2019.)

Sustainable development demands a holistic strategy that recognizes sustainability issues alongside with economic growth. Sustainability may be described as the act of providing the current demands without compromising the ability of future generations to fulfil their own requirements. Currently, there are about 140 developing nations worldwide that are actively searching for strategies to address their development requirements. However, due to the growing menace of climate change, it is imperative to take decisive actions to guarantee that present-day growth does not have adverse consequences for future generations. (United Nation 1987.)

The concept of sustainability is not recent. Indigenous communities have long engaged in sustainable living practices by closely aligning themselves with the natural environment and its boundaries, cycles, and fluctuations. This comprehension is commonly known as traditional ecological knowledge, or the profound understanding and convictions regarding the connections between individuals, flora, fauna, natural occurrences, environments, and the timing of events in a particular ecosystem.

Figure 15.Sustainable development Goals (climateposition, 2017.)

The scale of internet of things (IOT) for sustainable community development expand beyond cities, to the global scale including oceans, climate, and water monitoring applications. Therefore, the diverse medium of communications is involved such as wide area networks (WAN), terrestrial air, cellular and satellite. (Shridhar 2019.)

The require on of the security features on these sustainability internet of things (IOT) devices requires well thought design keeping in view its integration in the holistic traditional and novel insight and innovation into the potential risks that can comprise information. (Frustaci et al. 2017; Frustaci et al. 2018.)

Figure 16. Sustainability Human Goal (researchgate 2018.)

The interaction of sustainability internet of things with physical world phenomena such as water, weather, climate ocean is generally not found in the modern information technology systems. The actuation is based on sensing and monitoring, requires special attention in term of privacy and security. Therefore, more energy efficiency, safety, power, performance requirements of these devices distinguish them from computers. (Sengupta, Lessatapornwongsa, Ardekani, & Stuardo 2019.)

In IoT for sustainable community advancement, it is crucial to recognize that supportability things don't work in a vacuum, maybe these are part of the whole ecosystem. Subsequently, rather than the person-based security, the all-encompassing approach is of most extreme importance. The all-encompassing approach ought to take end-to-end procedure for cybersecurity over the whole maintainability scene. (Frustaci, et al. 2016; Frustaci, et al. 2017.)

Sustainable development provides businesses with a wide range of strategic options.

Sustainability offers several benefits, including effective human resource use, employment retention, cost efficiency, pollution reduction, and energy conservation. Businesses may enhance their ties with shareholders by implementing sustainable practices in their organizations. (Molamohamadi & Ismail 2013, 3.)

7 SUMMARY

The Internet of Things (IoT) is a technology revolution that play significant rule in implication for sustainability, privacy, cybersecurity and future, this thesis studies the convergence of IoT and sustainability, concentrating on the various challenges and opportunities given by adoption of IoT technologies throughout the various fields.

The privacy and cybersecurity have grown as a crucial factor for sustainability, the project studies the privacy challenges raises by the development of IoT devices and stressing the importance for strong privacy preserving methods and legislative structures to protect personal data and privacy. The cybersecurity concern on IoT ecosystem have been addressed, which include vulnerabilities in IoT devices, network infrastructure and cloud computing platforms and solutions to improve IoT security architecture.

IoT trends for sustainability have examined improvements in edge computing, blockchain technology artificial intelligence and 5G connection, these have potential to change the way IoT technology are used to solve sustainability problems and increase development in the sectors which include smart health, smart cities, energy conservation and agricultural precision.

Regulations and industry standards affect the growth and implementation of IoT systems for sustainability. The thesis examines importance of world environmental legislation and standards, which include Paris Agreement, Eco-design Directives, and these give guide to improve environmental sustainability and decreasing the environmental effect on IoT installations.

8 REFERENCES

ChatGPT 2023. OpenAI. GPT-3.5. Accessed for language check, May 2024. https://chat.openai.com

Akyildiz, I. F. Su W. Sankarasubramaniam, Y. & Cayirci, E. 2002. A survey on sensor networks. IEEE Communications Magazine, 40(8), 102-114. Accessed 10.02.2024.

Alaba, F. A. Othman, M. Hashem, I. A. T. & Alotaibi, F. 2017. Internet of Things security: A survey. Journal of Network and Computer Applications. 88, 10-28. doi:10.1016/j.jnca.2017.04.002 12.02.2024.

Al-Fuqaha, A. Guizani, M. Mohammadi, M. Aledhari, M. & Ayyash, M. 2015. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. IEEE Communications Surveys & Tutorials, 17(4), 2347-2376. doi:10.1109/COMST.2015.244. Accessed 14.02.2024.

Alphenaar, R. & Stango, A. 2016. Internet of Things (IoT) Security—Potential Risk of Attacks. Procedia Engineering, 149, 324-329 and multi-parameterized edit distance. Information Fusion, 52, 13–30. Accessed 14.02.2024.

Antonakakis, M. April,T. Bailey, M. Bernhard, M. Bursztein, E. Cochran, J. & Zhou Y. 2017. Understanding the Mirai Botnet. In Proceedings of the 26th USENIX Security Symposium (pp. 1092-1110). USENIX Association. Accessed 14.02.2024.

Atzori, L. Iera, A. & Morabito, G. 2010. The Internet of Things: A Survey. Computer Networks, 54(15), 2787-2805. doi:10.1016/j.comnet.2010.05.010 Accessed 15.02.2024.

Banks, A. & Gupta, R. 2019. MQTT Version 5.0. OASIS Standard. Accessed 25.03.2024.

Beale, J. 2018. The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws (2nd ed.). Wiley. Accessed 17.02.2024.

Bilge, L. Balzarotti, D. Robertson, W. & Kirda, E. 2014. Disclosure: Detecting Botnet Command and Control Servers Through Large-Scale NetFlow Analysis. In NDSS (Vol. 14, pp. 1-16). Accessed 20.02.2024.

bitdefender, n.d. What are data Breaches. https://blogapp.bitdefender.com/cyberpedia/content/images/size/w1000/2021/11/Data-Breaches.png Accessed 25.03.2024.

Boardinfinity n.d. Wireless sensor networks. https://www.boardinfinity.com/blog/content/images/2023/03/Copy-of-Copy-of-Copy-of-Copy-of-Copy-of-Untitled-Design.png Accessed 25.04.2024.

Borgia, E. 2014. The Internet of Things vision: Key features, applications, and open issues. Computer Communications, 54, 1-31. Accessed 20.02.2024.

Broad, M. 2014. Mastering Kali Linux for Advanced Penetration Testing. Packt Publishing. Accessed 20.02.2024.

California Legislative Information. 2018. California Consumer Privacy Act of 2018. Accessed 22.02.2024.

California Legislative Information. (n.d.). California Consumer Privacy Act of 2018. Retrieved from https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180AB375 Accessed 22.04.2024.

Care industry cybersecurity task force, H.: Report on improving cybersecurity in the health care industry. https://www.phe.gov/preparedness/planning/cybertf/documents/ Accessed 22.02.2024.

Cauteruccio, F. Fortino G. Guerrieri A. Liotta A. Mocanu D. C. Perra C. et al. 2019. Accessed 22.04.2024.

Cavalcante, R. C. Alves J. P. Aguiar R. S. & Sadok D. 2019. IoT-Based Environmental Monitoring Systems: A Survey. IEEE Access, 7, 98109-98128. 23.02.2024.

Cavoukian, A. 2009. Privacy by Design: The 7 Foundational Principles. Information and Privacy Commissioner of Ontario, Canada. challenges. Future Generation Computer Systems, 82, 395–411. Accessed 24.02.2024.

Clarke, R. 2019. The Right to Accuracy in Data Privacy Law. University of New South Wales Law Research Series. 24.02.2024.

Climatepositions, 26.09.2017, UN Sustainable Development Goals and greenhouse gas emissions, https://climatepositions.com/un-sustainable-development-goals-global-goals-and-greenhouse-gas-emissions/

Conuret, 8.3.2022, Top Applications of IoT for Environmental Sustainability https://www.conurets.com/top-7-applications-of-iot-for-environmental-sustainability/

Corchado, J. M. Bajo, J. Abraham, A. & De Paz, J. F. 2019. Towards Sustainable Smart Cities: A Review of Trends, Architectures, Components, and Open Challenges in Smart Cities. Sustainability, 11(7), 1881. Accessed 24.02.2024.

Deng, Z. Xu, X. & Liu, Y. 2019. Deep Learning for IoT Big Data and Streaming Analytics: A Survey. IEEE Communications Surveys & Tutorials, 21(4), 3462-3491. 24.02.2024.

Dhillon, G. & Moores, T. 2001. Internet Banking Security: A Comparative Study of Recent Technological Developments. Information Management & Computer Security, 9(1), 24-31. 25.02.2024.

Dorri, A. Kanhere, S. S. Jurdak, R. & Gauravaram P. 2017. Blockchain for IoT Security and Privacy: The Case Study of a Smart Home. In Proceedings of the 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops) (pp. 618-623). IEEE. Accessed 26.02.2024.

Elkadeem, M. R. Badawy, A. & Zoriel, A. M. 2019. IoT-Based Environmental Monitoring Systems: Design, Implementation, and Security Challenges. IEEE Access, 7, 63540-63558. 26.02.2024.

Engebretson, P. 2014. The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy (2nd ed.). Syngress. Accessed 26.02.2024.

European Commission. 2018. General Data Protection Regulation (GDPR). Retrieved from https://eur-lex.europa.eu/eli/reg/2016/679/oj Accessed 27.02.2024.

European Union. 2016. General Data Protection Regulation. Official Journal of the European Union, L119, 1-88. Accessed 28.02.2024.

European Union. 2016. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons Regarding the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union, L119, 1-88. Accessed 28.02.2024.

Fernandez-Carames, T. M. & Fraga-Lamas, P. 2018. A Review on the Use of Blockchain for the Internet of Things. IEEE Access, 6, 32979-33001. Accessed 01.03.2024.

Fielding, R. & Reschke, J. 2014. Hypertext Transfer Protocol (HTTP/1.1): Messaging and Semantics. RFC 7231. Retrieved from [URL] Accessed 01.03.2024.

Fortino, G. Trunfio, P. & Liotta, A. 2017. Internet of Things: Architectures, Protocols, and Applications. Wireless Communications and Mobile Computing, 2017, 1-2. Accessed 01.03.2024.

Geissdoerfer, M. Savaget, P. Bocken, N. M. & Hultink, E. J. 2017. The Circular Economy—A new sustainability paradigm? Journal of Cleaner Production, 143, 757-768. Accessed 04.03.2024.

Gia, T. N., Jiang, M. Rahmani, A. M. Westerlund, T. Liljeberg, P. & Tenhunen H. 2017. Internet of Things for Smart Cities: A Survey. IEEE Internet of Things Journal, 4(6), 1802-1819.Accessed 04.03.2024.

Granjal, J. Monteiro, E. & Silva,J. S. 2015. Security for the Internet of Things: A survey of existing protocols and open research issues. IEEE Communications Surveys & Tutorials, 17(3), 1294-1312. doi:10.1109/COMST.2015.2394421 04.03.2024.

Greenberg, A. 2015. Hackers Remotely Kill a Jeep on the Highway—With Me in It. Wired. Accessed 05.03.2024.

GSMA. 2019. GSMA IoT Security Guidelines. https://www.gsma.com/iot/iot-security-guidelines/ Accessed 05.03.2024.

Gubbi, J. Buyya, R. Marusic, S. & Palaniswami M. 2013. Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems, 29(7), 1645-1660.Accessed 05.03.2024.

Hong, J. I. & Landay, J. A. 2019. Privacy Issues in Sustainability Systems. ACM Transactions on Computer-Human Interaction (TOCHI), 26(5), 1-42. doi:10.1145/3364994 Accessed 06.03.2024.

Hossain, M. S. & Muhammad, G. 2016. Cloud-Assisted Industrial Internet of Things (IIoT) – Enabled Framework for Health Monitoring. Future Generation Computer Systems, 56, 471-484. doi:10.1016/j.future.2015.08.012 16.03.2024.

IEEE Standards Association. (n.d.). IEEE P2413: Standard for an Architectural Framework for the Internet of Things (IoT). Retrieved from https://standards.ieee.org/standard/2413-2019.html Accessed 14.03.2024.

Ilic, A. Despotovic D. & Bajic E. 2020. Sustainable smart solutions based on IoT and big data paradigm. Sustainable Cities and Society, 60, 102243. Accessed 16.03.2024.

International Organization for Standardization. 2013. ISO/IEC 27001:2013 Information technology—Security techniques—Information security management systems—Requirements. Accessed 17.03.2024.

ISO. (2013). ISO/IEC 27001:2013 - Information Security Management System (ISMS) https://www.iso.org/standard/54534.html Accessed 23.04.2024.

Jara, A. J. Moreno-Sanchez, P. & Skarmeta, A. F. 2014. Internet of Things in Smart Cities: A Survey. IEEE Internet of Things Journal, 1(1), 22-32. 24.03.2024.

Jarmakiewicz, J. Parobczak, K. & slanka K. 2017. Cybersecurity protection for power grid control infrastructures. International Journal of Critical Infrastructure Protection, 18, 20–33 Accessed 14.03.2024.

Jennings, N. R. Sycara, K. & Wooldridge, M. 2015. A Roadmap of Agent Research and Development. Autonomous Agents and Multi-Agent Systems, 1(1), 7-38. Accessed 15.04.2024.

Jensen, M. C. & Meckling W. H. 1976. Theory of the Firm: Managerial Behavior, Agency Costs and Ownership Structure. Journal of Financial Economics, 3(4), 305-360. Accessed 30.03.2024.

Johnson, S. 2019. The Hacker Playbook 3: Practical Guide to Penetration Testing. Independent. Accessed 30.03.2024.

Kali Linux Documentation. (n.d.). https://www.kali.org/docs/ Accessed 24.03.2024.

Kali Linux. (n.d.). https://www.kali.org/ Accessed 27.03.2024.

Khan M. A. & Salah K. 2018. IoT security: Review, blockchain solutions, Accessed 6.03.2024.

Khan, S. Yaqoob, I. Hashem I. A. T. Inayat Z. Ali W. K. Alam M. ... & Ahmed E. 2019. A privacy-preserving and secure framework for IoT-based healthcare. IEEE Access, 7, 116786-116800. Accessed 20.03.2024.

Kolias, C. Kambourakis, G. Stavrou, A. & Voas, J. 2017. DDoS in the IoT: Mirai and Other Botnets. Computer, 50(7), 80-84.Accessed 25.04.2024.

Kosta, E. Pierson, J. & Kalloniatis, C. 2019. Privacy Risks in Smart Environments: A Survey. ACM Computing Surveys (CSUR), 52(5), 1-38. Accessed 30.03.2024.

Kumar, N. Al-Fuqaha, A. Guizani, M. & Rayes, A. 2017. Security in Internet of Things: Opportunities and Challenges. In 2017 IEEE Wireless Communications and Networking Conference Workshops (WCNCW) (pp. 1-6). IEEE. Accessed 20.04.2024.

Li, S. Da, I. Xu, L. & Zhao, S. 2017. The Internet of Things: A survey. Information Systems Frontiers, 17(2), 243-259. Accessed 15.04.2024.

Lin, J. Yu, W. Zhang, N. Yang, X. Zhang,H. & Zhao, W. 2017. A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. IEEE Internet of Things Journal, 4(5), 1125-1142. doi:10.1109/JIOT.2017.2683200 Accessed 24.04.2024.

Luthra, S. & Mangla, S. K. 2018. Evaluating challenges to Industry 4.0 initiatives for supply chain sustainability in emerging economies. Process Safety and Environmental Protection, 117, 168-179. doi:10.1016/j.psep.2018.04.018 Accessed 15.04.2024.

Lyon, G. 2022. Nmap. Retrieved from https://nmap.org/ Accessed 27.03.2024.

Medium, 16.03.2023, Cybersecurity in Industrial 4.0, https://medium.com/@so-ham.sattigeri20/cyber-security-in-industry-4-0-c410ba38167 Accessed 16.04.2024.

Medium, 8.5.2019, Internet of Things (IoT) Security, Privacy, Application & Trends https://www.researchgate.net/profile/Gursharan-Banger/publication/338288885/figure/fig2/AS:842350368677889@1577843386247/Security-and-privacy-of-data-in-IoT-51.png

Accessed 18.04.2024.

Messier, D. 2016. Penetration Testing Basics: A Quick-Start Guide to Breaking into Systems. O'Reilly Media Accessed 27.04.2024.

Miorandi, D. Sicari, S. De Pellegrini, F. & Chlamtac, I. 2012. Internet of things: Vision, applications and research challenges. Ad Hoc Networks, 10(7), 1497-1516. Accessed 29.03.2024.

Mouradian, C. Naboulsi, D. Yangui, S. Glitho, R. H. & Morrow, M. J. 2019. A comprehensive survey on fog computing: State-of-the-art and research challenges. IEEE Communications Surveys & Tutorials, 20(1), 416-464. 01.04.2024.

NAMIOT. 2020. Environmental Monitoring Using IoT Sensors. Retrieved from https://www.namiot.com/environmental-monitoring-using-iot-sensors/ Accessed 03.04.2024.

National Institute of Standards and Technology. 2018. Framework for Improving Critical Infrastructure Cybersecurity. Accessed 18.04.2024.

National Institute of Standards and Technology. 2020. NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management. Accessed 30.04.2024.

Newark, n.d. IoT Wireless Network Protocols https://www.newark.com/wcsstore/ExtendedSitesCatalogAssetStore/cms/asset/images/common/technology/articles/2434360/2434360-iot-protocol-network.jpg Accessed 10.05.2024.

News, 13.11.2020, System brings deep learning to internet of things devices. https://news.mit.edu/sites/default/files/styles/news_article__image_gallery/public/images/202011/MIT-Tiny-AI-01_0.jpg?itok=chf7f8K1 Accessed 10.05.2024.

Offensive Security. 2022. Kali Linux. Retrieved from https://www.kali.org/ 01.04.2024.

OffSec Resources. (n.d.). https://www.offensive-security.com/kali-linux-vm-vmware-virtualbox-image-download/ 26.04.2024.

O'Gorman, G. Meyer, C. M. Collier, M. Kott, A. & Spring J. 2020. Supply chain security in the internet of things: A review. Computers & Security, 101948. Accessed 30.04.2024.

Ohm, P. 2010. Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. UCLA Law Review, 57, 1701. Accessed 19.04.2024.

Palaniappan, R. Omkar, S. N. & Kumar, M. 2018. IoT-Based Air Pollution Monitoring System. In Proceedings of the International Conference on Intelligent Systems Design and Applications (pp. 167-172). Springer, Cham. Accessed 28.02.2024.

Peppet, S. R. 2014. Regulating the Internet of Things: First steps toward managing discrimination, privacy, security, and consent. Texas Law Review, 93, 85. Available at SSRN: https://ssrn.com/abstract=2409074w Accessed 15.03.2024.

Perera, C. Zaslavsky, A. Christen, P. & Georgakopoulos, D. 2014. Sensing as a Service Model for Smart Cities Supported by Internet of Things. Transactions on Emerging Telecommunications Technologies, 25(1), 81-93. Accessed 21.03.2024.

Pérez-Lombard, L. Ortiz, J. & Pout, C. 2008. A review on buildings energy consumption information. Energy and Buildings, 40(3), 394-398. doi:10.1016/j.enbuild.2007.03.007 Accessed 21.04.2024.

Ray, P. P. (2017). Internet of Things for Sustainable Community Development. Computers in Human Behavior, 76, 224-235. doi:10.1016/j.chb.2017.07.003
report2017.pdf. Accessed 23.04.2024.

Rescorla, E. (2018). The Transport Layer Security (TLS) Protocol Version 1.3. RFC 8446. Accessed 20.03.2024.

Researchgate, 11.2018, Comparison Study of Big Data Processing Systems for IoT Cloud Environment, https://www.researchgate.net/publication/331353248_Comparison_Study_of_Big_Data_Processing_Systems_for_IoT_Cloud_Environment Accessed 25.03.2024.

resize-ojict, n.d. Security and Privacy Issues in the Internet of Things https://resizev3.pubpub.org/eyJidWNrZXQiOiJhc3NldHMucHVicHViLm9yZyIsImtleSI6ImhoNzdhaXFoLzIxNjA5MDg0ODkzMTM1LnBuZyIsImVkaXRzIjp7InJlc2l6ZSI6eyJ3aWR0aCI6ODAwLCJmaXQiOiJpbnNpZGUiLCJ3aXRob3V0RW5sYXJnZW1lbnQiOnRydWV9fX0= Accessed 05.05.2024.

Roman, R., Zhou, J., & Lopez, J. 2013. On the features and challenges of security and privacy in distributed internet of things. Computer Networks, 57(10), 2266-2279. doi:10.1016/j.comnet.2012.12.018 Accessed 25.04.2024.

Sharif, M., Ahmed, K., & Saha, S. 2019. Cyber Security Threats and Solutions in IoT. In Proceedings of the 10th International Conference on Ambient Systems, Networks and Technologies (pp. 170-177). Springer, Cham. Accessed 25.03.2024.

Shelby, Z., Hartke, K., & Bormann, C. 2014. The Constrained Application Protocol (CoAP). RFC 7252. Retrieved from [URL] Accessed 25.02.2024.

Shi, W., Dustdar, S., & Nastic, S. 2016. The Promise of Edge Computing. Computer, 49(5), 78-81. Short-long term anomaly detection in wireless sensor networks based on machine learning. Accessed 22.04.2024.

Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. 2015. Security, privacy, and trust in Internet of Things: The road ahead. Computer Networks, 76, 146-164. doi:10.1016/j.comnet.2014.11.008 Accessed 25.01.2024.

Singh, R. 2017. Kali Linux 2: Windows Penetration Testing. Packt Publishing. Accessed 17.03.2024.

Sommer, R., & Paxson, V. 2010. Outside the Closed World: On Using Machine Learning for Network Intrusion Detection. Proceedings of the 2010 IEEE Symposium on Security and Privacy, 305-316. doi:10.1109/SP.2010.25 Accessed 19.03.2024.

Sommestad, T., Hallberg, J., & Ekstedt, M. 2015. Toward a Definition of the Internet of Things (IoT). IEEE Internet Computing, 19(4), 42-50. Accessed 26.04.2024.

Tully, J. 2019. The Internet of Things in the Circular Economy: A Comprehensive Review of the State of the Art. IEEE Access, 7, 124425-124443 Accessed 06.04.2024.

Weber, R. H. 2010. Internet of Things – New security and privacy challenges. Computer Law & Security Review, 26(1), 23-30. doi:10.1016/j.clsr.2009.11.008 Accessed 04.04.2024.

Wolfert, S., Ge, L. Verdouw, C., & Bogaardt, M.-J. 2017. Big Data in Smart Farming – A review. Agricultural Systems, 153, 69-80. doi:10.1016/j.agsy.2017.01.023 Accessed 18.04.2024.

Wright, D. & Raab, C. 2014. Privacy principles, risks, and harms. International Review of Law, Computers & Technology, 28(3), 277-298. doi:10.1080/13600869.2014.948035 Accessed 18.04.2024.

Zanella, A. Bui, N. Castellani, A. Vangelista, L. & Zorzi, M. 2014. Internet of Things for Smart Cities. IEEE Internet of Things Journal, 1(1), 22-32. doi:10.1109/JIOT.2014.2306328 Accessed 18.04.2024.

Zhang, X. Zhu, S. & Cheng S. 2017. Security and privacy in smart city applications: Challenges and solutions. IEEE Access, 5, 23021-23032. Accessed 20.04.2024.

Zhang, Y. Demchenko, Y. & De Laat, C. 2014. Cloud security for IoT: A survey. Future Generation Computer Systems, 56, 684-700. Accessed 20.04.2024.

Ziegeldorf, J. H. Morchon, O. G. & Wehrle, K. 2014. Privacy on the Internet of Things: Threats and challenges. Security and Communication Networks, 7(12), 2728-2742. doi:10.1002/sec.795 accessed 30.4.2024.