European Journal of
Technology
(EJT)

Analysis of Cyber Attacks within Critical IoT Infrastructures and Information Systems

Suh Charles Forbacha, Tambou Guemgne Eudoxie Juliana

European Journal of Technology
ISSN 2520-0712 (online)
Vol.8, Issue 6, pp1 28 - 61, 2025
www.ajpojournals.org

Analysis of Cyber Attacks within Critical IoT Infrastructures and Information Systems

Suh Charles Forbacha[1*], Tambou Guemgne Eudoxie Juliana[2]
[1]College of Technology, The University of Bamenda, Bambili, Cameroon
[2]National Higher Polytechnic Institute, The University of Bamenda, Bambili, Cameroon

Article history
Submitted 10.12.2024 Revised Version Received 06.01.2025 Accepted 03.02.2025

Abstract

Purpose: This research aims were to provide valuable insights into the potentials, risks, and best practices of deploying IoT in critical sectors, thus contributing to the knowledge base and fostering decision-making. The goal was to identify the possible types of cyber-attacks, take various precautions against these attacks, and to develop protection methods.

Materials and Methods: To attain this goal, we conducted a series of targeted questionnaires with a sample size of 100 and 89 responded to the questionnaire. The primary data collected from the respondents was analysed with a statistical package for social science (SPSS) and the results were summarised in pie charts and frequency tables.

Findings: The result showed that 80.9% of the respondents were familiar with the concept of connected devices, a fundamental principle of IoT, 54% of them believed that IoT infrastructures in their sector were secure to a high or very high extent while 46% perceived them as only somewhat secure or not secure at all. On the other hand, 83.1% of respondents believed that there was a high or very high need for stricter regulations regarding the cybersecurity of critical IoT infrastructures.

Implications to Theory, Policy and Practice: The researchers proposed a framework for enhancing the security posture of critical IoT infrastructures. This framework encompasses a combination of technological measures, and policy recommendations. In addition to this, they also recommended; Investing in the development of robust and reliable internet infrastructure to support the widespread deployment of IoT devices and enable seamless connectivity across the country. Providing training programs and workshops to enhance the technical skills of professionals in IoT technologies, cybersecurity, data analytics, and information systems management and implementing small-scale pilot projects in different sectors, such as healthcare, agriculture, transportation, or energy, to evaluate the feasibility and effectiveness of IoT infrastructures and information systems in the Cameroonian context. Conducting research to identify the specific needs and challenges in implementing IoT infrastructures and information systems in Cameroon, and developing tailored solutions to address them.

Keywords: *Internet of Things, security, critical infrastructure, information systems, cyber attacks*

INTRODUCTION

In an era marked by unprecedented technological advancements, the pervasive integration of the Internet of Things (IoT) into our daily lives has introduced a new frontier of connectivity and efficiency, from smart cities to industrial automation. However, this digital revolution is not without its challenges, particularly concerning the security and resilience of critical IoT infrastructures. This research embarks on a crucial exploration into the realm of Critical IoT Infrastructures and the information they managed. As these infrastructures permeate sectors such as energy, healthcare, transportation, and finance, their significance becomes undeniable, rendering their security a matter of paramount importance.

Background of the Study

The convergence of technologies over the years has resulted in the deployment of integrated systems to accomplish various activities. Internet of Things is one of such systems that has emerged from this convergence. IoT is therefore a system that connects everything in the modern world and is gaining traction in sectors such as electronic communications, energy, banking and finance, critical public services, transportation and water management, healthcare which are a few to be stated. IoT is one of the most popular new ideas in recent years. It locates, transmits, and analyses data using a network of connected components.

IoT has an impact on our daily social, commercial, and economic activities. IoT revenue is expected to increase from 892 billion USD in 2018 to more than 4 trillion USD by 2025 (Hassija et al., 2019). This expansion is directly related to the growth of the digital economy. The Internet of Things has enabled smart meters, remote monitoring, process automation, smart homes, smart cities, and smart businesses (Ślusarczyk, 2018). Current and future Internet of Things applications and services have the potential to significantly improve the ease, speed, and comfort of customers' lives (Sarker et al., 2020). In the context of critical infrastructures and information systems, the integration of IoT has the potential to revolutionize how essential services and operations are managed and monitored. For instance, in Industrial sector IoT devices such as tracking devices and temperature or pressure sensors are used for predictive maintenance and supply chain optimization, IoT devices are used in smart cities and transportation devices such as traffic control, smart lighting, and parking Sensors and in the healthcare sector, medical devices such as blood pressure monitors, infusion pumps, ECG units, and fitness.

Critical infrastructures, such as energy grids, transportation networks, and water supply systems play a fundamental role in modern societies and their proper functioning is crucial for public safety and economic stability. Additionally, information systems, which handle vast amounts of data and provide the backbone for communication and information exchange are also of utmost importance for governments, businesses and individuals.

In the African continent, precisely in Cameroon, there is a growing interest in harnessing the potential of IoT to address specific challenges and optimize critical services. The country faces unique infrastructural and socio-economic contexts, which require tailored solutions to ensure successful IoT implementations. The incorporation of IoT in critical infrastructures and information systems in Cameroon more precisely in the mfoundi and Mezam diviion would offer exciting opportunities for sustainable development, increased efficiency, and improved resource management.

When these infrastructures are connected through the internet, they may be subject to cyber-attack. As a result, it is crucial to analyse these infrastructure and proposed security approaches to mitigate or prevent IP-based cyber-attacks. A cyber-attack on the infrastructure of another

nation may even be a potential war justification (Das & Gündüz, 2019). Therefore, cyber-security is a crucial topic in defending organisational infrastructure as well as the nation.

Problem Statement

Despite the growing interest in critical IoT deployment, there is a lack of comprehensive study that specifically address its impact on infrastructures and information systems in Africa, particularly in Cameroon. Additionally, the complexities and security concerns related to deploying IoT in critical settings need to be addressed to ensure successful and safe implementations.

Cyber and physical attacks against key infrastructure such as power grids, water systems, telecommunications systems, and gas pipelines which are but few to be mentioned could be used to cause mass disruption or loss of life in a single location, shutting down the power of a hospital, alter the temperatures in nuclear cooling towers, and exploit features in smart cars while they are in motion are some destructive scenarios. Therefore, critical infrastructures are subjected to increased cases of hacking with the aim of cyber theft, espionage, intimidation, disruption, and cyberterrorism as noted by (Baykara & Daş 2015). These cyber threats and attacks, however, are significant impediments to IoT development. Analyzing critical IoT infrastructures and information systems in Africa, especially in Cameroon, presents several significant challenges that need to be addressed. These challenges include:

- Limited Infrastructure that can hinder the effective analysis of IoT systems. Inadequate network coverage, unreliable power supply, and limited connectivity options pose challenges for seamless data collection and analysis.
- IoT infrastructures generate vast amounts of data from numerous sensors and devices. Effectively managing this data is a significant challenge in Cameroon, including issues related to data storage, data quality assurance, and data governance frameworks.
- The regulatory landscape surrounding IoT infrastructures and information systems in Africa, especially in Cameroon, is still evolving. There may be gaps or inconsistencies in regulations regarding data privacy, security standards, and interoperability requirements.

Research Questions

In order to effectively conduct this research, we laid out our main research question which was:

How does the implementation of IoT impact critical infrastructures and information systems in Africa, with a specific focus on Cameroon?

The main research question was supported by the following specific questions:

1. What is the state of the current IoT infrastructure systems in Cameroon?
2. What are the various IoT security challenges in line with the critical infrastructure?
3. How can we develop a protection method against the challenges?

Objectives

Defining research objectives is a fundamental step that is necessary in providing an overall framework that derives the scope of the research. In this study, we outlined our general object which was:

To analyze the impact of IoT on critical infrastructure and information systems in Africa with a focus on Cameroon.

This was further supported with specific objectives that focused on:

1. Discussing the current state of IoT Infrastructure Systems in Cameroon.
2. Identifying IoT security challenges in line with its critical infrastructure.
3. Discussing the various IoT security challenges and how to overcome plus manage these challenges.

Internet of Things

We conducted a comprehensive analysis of existing studies and research related to the implementation of critical Internet of Things (IoT) in infrastructures and information systems, with a specific focus on Africa and Cameroon. This review examined the opportunities, challenges, and best practices associated with deploying IoT solutions in critical sectors within the region. It also basically concluded, summarized, and evaluated previous research or work that had been conducted on developing the proposed system. This, therefore took into consideration the critical points of current knowledge including substantive findings as well as theoretical and methodological contributions our specific topic. The main goals are to situate the current study within the body of knowledge and to provide context for the particular reader as noted by Paré & Kitsiou (2017). IoT was first introduced in 1999, when Kevin Ashton, a researcher at Procter & Gamble, coined the term. However, the concept only gained popularity after 2010, when several large technology companies began investing in IoT.

Internet of Things (IoT) is the networking of devices. It's comparable to a social network or email provider, but IoT links devices rather than people. According to (Ericsson, 2020), 22 billion devices will be on the Internet of Things by the end of 2022. Business Insider's experts expect the figure to grow to 30.9 billion by 2025 (Research and Markets, 2020). As IoT devices increase in number so is the attack surface of the cybersecurity vulnerabilities they present. IoT devices are particularly vulnerable to network attacks such as data thefts, phishing attacks, spoofing, and denial of service attacks (DoS attacks). These can lead to other cyber security threats like ransomware attacks and serious data breaches that can take businesses a lot of money and effort to recover from. These devices can operate independently of human interaction in some capacity and have autonomous functions and features (Weber, 2016).

Operation of IoT

As earlier mentioned, IoT is a giant network consisting of interconnected devices. (Team, 2021)

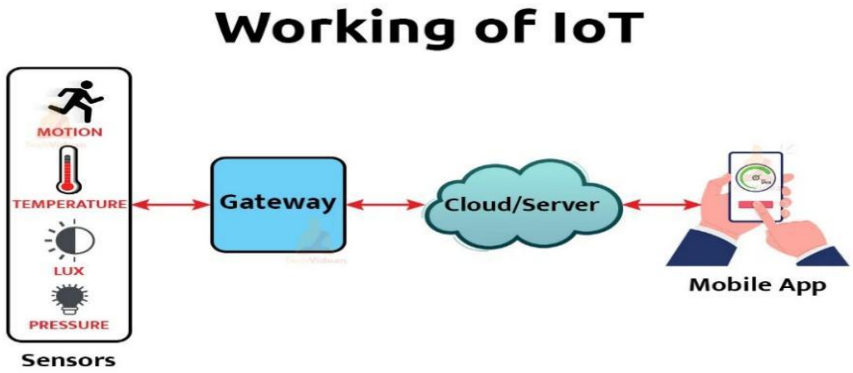

Figure 1: Working of IoT (TechVidvan Team)

IoT devices have sensors embedded into them. These sensors are capable of sensing their surroundings. Devices store the information in some form of data. These devices include

appliances such as mobile phones, coffee machines, microwaves, geysers, fire alarms, Air conditioners, cars, and so on.

The sensors embedded in these devices constantly emit data about the surroundings and on the working information of these devices. IoT serves as a platform to dump all the data collected by these devices. IoT platforms includes cloud servers and large databases. The IoT platform acts on the data. It integrates and processes the information. Further, the platform analyses the data thoroughly to gather important details. The platform then sends back instructions based on the data provided.

Finally, the data aggregation is shared with other devices for better performance in the future. It is also done for improved user experience. This data may be used to identify trends, provide suggestions, and detect potential issues before they arise.

Impact of IoT on Critical Sectors

Conventionally, home computers were independently operated and were controlled physically. However, now that society has reached the age of IoT each connected device could be a potential doorway into the IoT infrastructure or personal data (Ugur & Barutcu, 2018). This implies that today's world devices can be remotely controlled using other devices, either through an app, a programmed schedule, a mobile phone, or even another IoT device, taking much less, but not a complete absence of human interaction to operate. This leads to the main purpose of the IoT's existence and that is to improve the quality of life for the user by making manual tasks more automated.

In the healthcare sector, IoT has also taken advantage, devices, such as smartwatches, smartphones, and ingestible monitors can keep track of a patient's data regarding blood pressure, heart rate, and other concerns in real-time (Affia et al., 2023), also by offering essential advantages, including remote patient monitoring and data-driven decision-making, Wearables, remote monitoring systems, and telemedicine platforms, on the other hand, have transformed healthcare delivery. The potential for IoT in healthcare is exciting, despite issues like data overload and security worries. Collaborative efforts are essential to solve problems, fully take advantage of IoT's advantages, and build a patient-centered, effective, and data-driven healthcare system. IoT will change patient care and healthcare services with continual innovation, leading to better results and an improved health industry.

In Cameroon, IoT is also transforming sustainable agriculture. Agriculture is an important industry in the country, employing a large section of the workforce. Unpredictable weather patterns caused by climate change, limited access to resources, and antiquated farming practices, on the other hand, have resulted in lower agricultural productivity. IoT connected drones are another tool that the agricultural sector are using to monitor crops, livestock, weather and light conditions. Drones are also being utilized for pollinating, fertilizing, and spraying crops with pesticides. This automated process reduces the need for on-hand farming and saves time and resources. IoT sensors provide farmers with real-time data on soil moisture, temperature, and nutrient levels, allowing them to optimize resource consumption and boost crop yields. The adoption of precision agriculture practices enabled by IoT benefits not only local farmers but also adds to regional food security.

In telecommunications, IoT assists in tracking and tracing all information and data rendered to consumers. Such information is usually about services and products offered to the consumers. The installation of IoT-powered cameras and beacons for security deployment also helps the telecommunication industries combat the challenge of security maintenance. IoT also assists telecom companies in conducting the performance evaluation of their products. Accomplish

the data collection through pre-integrated sensors after deploying products. As a result, it helps in checking and measuring the performance of telecommunication.

Another industry benefiting from the convergence of IoT in Cameroon is Education. The country has a high percentage of illiteracy and inadequate access to high-quality education, especially in rural areas. However, the digitization of education has bridged the gap through efforts such as online learning platforms and smart classrooms. Furthermore, IoT devices improve connectivity, allowing students to access instructional resources even in remote locations. Cameroon is fostering a new generation of technologically literate citizens who will contribute to the country's long-term prosperity and share their knowledge beyond its borders by democratizing education (Alaine, 2 August 2023).

In the transportation sector, IoT in transportation is revolutionizing traffic management, easing congestion, and promoting safety. It is powered by Smart Traffic Management Systems (STMS) - a blend of IoT devices and technology. Using IoT technology, transportation companies in urban cities ensure smooth traffic flow, incorporating IoT sensors at thousands of intersections. Such systems help reduce traffic congestion and pollution by minimizing idle time for vehicles (Mansha Kapoor, 2023). IoT also has a transformative impact on the energy industry, providing companies with new tools and technologies through the use of connected devices and sensors. These devices can be used to monitor the performance of power plants, wind turbines, and other energy infrastructure, providing real-time data on energy production and consumption. This data can then be analyzed to identify inefficiencies and areas for improvement in the Energy sector.

IoT-generated data provides fintech companies with a wealth of information about customer behavior, preferences, and needs. By analyzing this data, fintech firms can tailor their marketing strategies, engage with customers more effectively, and develop financial products that better suit individual requirements.

IoT is a boon for Infrastructures operating with employees in critical sectors, and employees are the first to reap the benefits. Some benefits are:

1. Real-time business insights
2. Cost-savings
3. Increased revenues
4. Improved user satisfaction
5. Differentiated brand and improved competitiveness
6. Improved long-term planning and strategy

Businesses should safeguard data flowing to and from IoT devices for optimal security and to avoid halts in service. As such, organizations that are aspiring to grow will see a significant amount of changes in their operations and profitability resulting from the implementation of this technology. Businesses are willing to improve their profitability over time, and these smart technologies are helping them to accomplish their objectives. IoT continues to reshape all sectors profoundly in amazing ways.

Critical Infrastructures

Infrastructures are large-scale, man-made systems that function interdependently to produce and distribute essential goods (such as energy, water, and data) and services (such as transportation, banking, and health care). An infrastructure is termed critical if its incapacity or destruction has a significant impact on health, safety, security, economics, and social well-

being (Council Directive 2008/114/EC). A failure in such an infrastructure, or the unavailability of its service, can be damaging to a single society and its economy, while it could also cascade across boundaries causing failures in multiple infrastructures with potential catastrophic consequences (Kroger and Zio 2011). Major critical infrastructure sectors are shown in Figure 2.

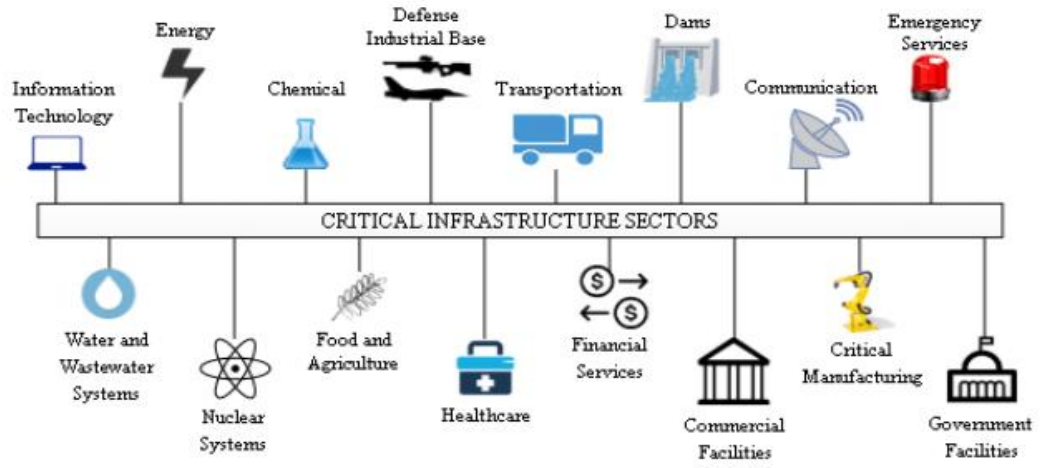

Figure 1: Major Critical IOT Infrastructures (Das & Gündüz, 2019)

The growing trend for convergence and multi-system interconnectedness in CIs is introducing several security issues that threaten normal economic and social functions. As new technologies such as the Internet of Things (IoT) get integrated into CNI, new security risks (threats, vulnerabilities, and attacks) emerge that require specific security solutions (Alcaraz & Zeadally, 2015). The risks are particularly difficult to identify, and handle given that the IoT has emerged from a range of disparate fields of study (Maple, 2017). The benefits of CIs can be realized if they function properly and are not impaired. This requires CIs to be kept safe from harm, and secure from any disruptive or destructive compromise. Thus, it is crucial to protect CIs, especially in the light of the growing and evolving malignity. It is important to understand potential security risks and how to effectively manage them using effective protection tools and techniques.

In the context of this study, we focused on the most prevalent IoT-based cyber-attacks that are highlighted below. In order to understand the severity of the situation, it is important to evaluate the effects and consequences of the mentioned cases. In this context, the whole cases emphasize the vulnerabilities in critical infrastructure systems. These vulnerabilities often depend on insecure setups in the IoT-based control systems, outdated firmware, weak authentication protocols and/or inadequate encryption as well as weak access protection techniques. For instance, Mirai bonet created in 2016 has had a widespread and significant impact on several IoT devices (Zhang et al., 2020).

Common Types of Cyber-Attacks

A cyber-kinetic attack targets IoT-based applications and Information Systems (ICS). This type of attack threatens human life, physical well-being, or the environment. Cyber-kinetic attacks on IoT-based critical infrastructures are often complex (Shim, 2019). They are performed using multiple different methods and techniques. The most common methods used in these cyber-attacks are presented in this section:

Malware injection is the settlement of malicious software into a cyber-space to cause damage or to disable the system (Wells et al., 2014). Adware, keyloggers, worms, spyware, rootkits, ransomware, trojans, or viruses are prominent malware. WannaCry ransomware is a famous malware example. It is used to deny people access to their files and essential services unless a ransom is paid.

Phishing is a data request attack from an untrusted source. The untrusted resource tries to convince users that it is a trusted source. If the victim is convinced that the attacker is a trusted source, he performs certain actions that the attacker has identified before, such as clicking the malicious link and entering sensitive data. In this case, the victim gives his sensitive data to the attacker with his own hand. If the victim is an employee in a critical infrastructure system, the situation can turn into a disaster (Tracey, 2024).

Spear phishing is the most common phishing attack, especially in critical infrastructures. Email attachments are used to make the user click on a link to trigger malicious software (Li et al., 2016). Although spear phishing is considered as one of the least complex methods of cyber-attacks, it has recently led to catastrophic effects on critical infrastructures. Therefore, the low level of cyber-security awareness is potentially the highest risk of cyber-attack in IoT-based critical infrastructures.

Hacking is the process of gaining access to the system. The most important operation of this process is to obtain the password of the system. Hacking is usually done by using various methods such as brute force, man-in-the-middle (MITM), and social engineering (Da¸ Karabade, & Tuna, 2015).

Denial of Service attacks aim to congest the infrastructure of a system network with excessive traffic and spam data. The system communication infrastructure is overloaded by too many unnecessary connection requests. This makes the system slow or inoperable. DDoS attacks potentially can be performed on all devices connected to the Internet, especially on backbone components (Da¸Karabade, & Tuna, 2015).

SQL injection attacks aim to steal, alter, or delete database content. It is used to attack the data-driven systems. Attackers execute SQL query statements to access the database server of the system. Almost all of the IoT-based critical infrastructures have databases (DemiRol et al., 2013).

A Review of Recent Cyber Attacks

IoT-based solutions are the most prominent technologies to improve critical infrastructures. If a device has an IP address, it means that it can connect to the Internet. It is possible to say that devices connected to the Internet are in the scope of the IoT concept, thanks to the current Internet infrastructure. So, IoT devices may be exposed to nearly all cyber-attacks that may occur in IP-based environments. The security vulnerabilities of the Internet also disrupt IoT applications. Thus, this new technology comes with some cyber-security vulnerabilities.

In this section, the most considerable examples of IoT-based cyber-attacks in the world and their dangers for critical infrastructures have been highlighted.

- Power Company Hacking*:* In the year 2009, an employee, fired from his company, hacked the system network to shut down the company's power forecasting systems. To do this, the attacker used his login information that was not disabled by system administrators (Wells et al., 2014).

- Tram Hacking*:* A teenager hacked the tram system of Lodz city in 2008 with a homemade transmitter that redirected trains. This was the first cybernetic attack that injured some people (Kimani et al., 2019a).
- Water Distribution System Hacking*:* The water distribution system at the water and sewer department was hacked. Then, the attackers presented some diagram screenshots of the system plans of water and waste-water treatment facilities. Also, a three-character password was used to protect the system, and this showed that a remote attack could easily be accomplished by capturing the password. This attack was carried out in 2011 (Miller & Rowe, 2012).
- Dam Cyber-attack*:* In 2013, the attackers obtained unauthorized access to the SCADA system of Bowman Avenue Dam and they were able to gather data on operations including water levels, temperatures, and the status of devices. It showed that the attackers can easily change the settings of water flow, and the amount of chemicals used in water treatment and open the floodgates during a rainstorm. Also, the event exemplifies the immense destruction that can be caused by such a cyber-attack against IoT-based critical infrastructures (Segovia et al., 2019).
- Power Grid Hacking*:* Attackers were able to seize control of Ukraine's power grid control system by hacking the SCADA system in 2015. This caused a power outage that left about 700,000 people without power for a few hours. Attackers are thought to be testing the most complex sabotage software with this IoT-based cyberattack (Whitehead et al., 2017).
- Dyn DDoS Attack*:* The DDoS attack used a system known as the Mirai botnet. Mirai botnet targets IoT devices and also scans the web to poorly secured IoT devices that still have default usernames and passwords. Moreover, it is responsible for large-scale DDoS attacks on Dyn servers which is an Internet Service Provider (ISP). This attack was largely successful and it occurred in the year 2016, as many people did not change the default logins of their devices. Numerous websites such as Twitter, Netflix, Spotify, and Reddit could not be available for a day (Liu et al., 2019).
- Light Rail System Attack*:* In 2016, the light rail system of San Francisco in the USA was subjected to a ransomware attack. In the attack, no firewalls were breached but an employee invited the hackers into the system by clicking a phishing mail (Tariq et al., 2021).
- Water Company Hacking*:* The attackers infiltrated the water utility's SCADA system and they managed to manipulate the system to change the amount of chemicals used. Thus, they intervened in water treatment and production (Sánchez et al., 2019).All these happened in the year 2016.
- Smart Building Attack*:* Smart homes and buildings are the general applications of IoT. The applications are developed via IoT devices and stay connected to the Internet continuously. The DDoS attack shut down heat and hot water systems at two buildings in winter. The DoS attack flooded the building control system with bogus Internet traffic. So, this caused to restart the system every few minutes and denied administrators remote access to the device (Luiijf, Žutautaite & Hämmerli, 2018).
- Electric Grid Cyber-attack*:* In 2017 on the day of general election in the UK, an electricity supplies the network was attacked. The aim of the cyberattack was to infiltrate into the SCADA system plans of water and waste-water treatment facilities. Also, a three-character password was used to protect the system, and this showed that a remote attack can easily be accomplished by capturing the password (Segovia et al., 2019).

- Petrochemical Plant Cyber-attack*:* A failed cyber-attack against a petrochemical plant was carried out. The aim of the cyber-attack was to sabotage the operations of the facility and to cause an explosion that could kill people. Fortunately, an error in the source code of the attackers did not enable the explosion occurs. In other words, the only reason it did not happened, there was a mistake in the attackers' source code. Also, the source code was not seen in an earlier cyber-attack. All of the IoT-based hacking tools were custom-built (Wilkins, 2019)
- Transport Network Cyber-attack*:* During the year 2017 a cyberattack hit the transportation network causing train delays and disrupting travel services. Customers were unable to make reservations or receive updates about the delays.
- Healthcare Company Cyber-attack*:* In 2018 A sophisticated attack was carried out on a healthcare company. Firstly, the attackers seized login information from a vendor who provides IT devices to the hospital. Secondly, they targeted a server by using remote execution techniques for Samsam ransomware. Finally, they encrypted the hospital's critical data files (Coventry & Branley, 2018).
- Telecommunication and Finance Sectors Cyberattack*:* An organized attack was carried out in 2019 against the prominent institutions that provide communication infrastructure and financial services. The attack was aimed denial of services on critical infrastructures. The institutions that were attacked could not serve for a time(Daily Sabah, 2019).

Nature and physical attacks are not the only threats to infrastructure any longer. As critical sectors increasingly rely on wireless and interconnected solutions, the threats they face have evolved accordingly. Network resilience and security are paramount to ensuring that connectivity remains uninterrupted. Constant vigilance and checks can go a long way towards securing infrastructure, but these steps are not always sufficient. The most successful and straightforward way to protect your networks and infrastructure starts at the roots with a network-based security solution like First point.

Some Effective Techniques Used to Secure them

Using one of these security solutions will ensure your facilities, networks, and devices are secure from the ground up. Mitigating the effects of cyber-attacks includes both intrusion detection methods and intrusion prevention methods, (Baykara & Daş 2015). Some of the leading methods to mitigate the effects of cyberattacks in IoT-based critical infrastructures have been listed below:

i. Encryption*:* Attackers want to capture data from the system or IP packets. However, providing encryption with strong encryption methods reduces this (Yang et al., 2011) . Therefore, when IoT applications are used in critical infrastructures, the traffic of IoT devices to and from the control system must be effectively encrypted. So, encryption is very crucial to protect data integrity and confidentiality in communication networks.

ii. Access Control*:* It is vital to determine which resources, data files, and components can be accessed by users and devices. Also, the areas that the users or devices cannot access must be defined too (Yang et al., 2011) . Using predefined access rules reduces the possibility of malicious access to the network. In remotely monitored and configured cyber-physical systems, such as IoT-based smart grids, access controls are very important to restrict the access of users and devices in the network.

iii. Authentication*:* Device authentication is the primary step in the secure data transmission session. It is responsible for identifying devices and authorizing the tasks that devices must do in the network. Time-sensitive is very crucial for IoT-based CPS

communications. Authentication ensures that smart devices do not accept unauthorized commands(Yang et al., 2011) .

iv. Blockchain technology**:** The blockchain is used to record IoT data in a distributed ledger that cannot be changed or manipulated by unauthorized users. This feature ensures the traceability and integrity of the data. Blockchain verifies data and ensures it comes from a reliable source, which improves secure transmission and improves privacy agreements. Multiple layers of security are needed to block unassigned access and blockchain helps in achieving this by providing safe data and restricting access to authorized users. (Al Sadawi, Hassan, & Ndiaye, 2024)

v. Regular and remote security updates*:* IoT devices need to be easily updated in a manageable way. So, security updates of devices can be done simply too. If an IoT device is not configured to receive the updates, ensuring security updates may be a hardship. Unfortunately, most developers are currently developing IoT devices without considering firmware and security updates. However, due to the fast improvements in technology, it is important to provide updates effectively to address issues that operating systems and source codes may face due to security vulnerabilities(Kimani et al., 2019b). Also, for an IoT-based smart grid, regular updates of the firmware is a logical solution as compared to large-scale replacement of the out-of-date devices. Moreover, updating of firmware remotely and easily is an important security requirement to mitigate potential threats in IoT-based systems.

vi. Physical security*:* It is very important to ensure the physical security of the devices in the system. Accessing devices physically by unauthorized people may compromise the stored data in the devices. Moreover, it should be remembered that the physical security of the control rooms and the servers is more important. As a result, the physical security vulnerability of any device poses a risk to the entire network (Bou-Harb et al., 2013). So, precautions should be taken at the infrastructure installation stage.

vii. Backdoors and login process*:* IoT solutions for critical infrastructures should ensure the data privacy and confidentiality of end-users. Therefore, manufacturers should ensure that backdoor and malicious codes are not embedded in the devices during production. There are discussions about adding a backdoor used for legal surveillance on some IoT devices (Kimani et al., 2019c). However, it is important to note that this back door is the same one used by attackers who attempt to gain illegal access to devices. Also, in mass-produced devices, unique logins should be created for each device, instead of the common default login password. Therefore, it would be hard for intruders to compromise devices and to participate in a botnet for DDoS attacks.

viii. Zero-trust architecture**:** Zero-trust in IoT aims to protect sensitive data and systems by implementing strict access controls, authentication mechanisms, and monitoring techniques, regardless of the location or network where the devices are connected.
Zero-trust is necessary because IoT devices are often connected to networks that have access to sensitive data and limited security features, making them vulnerable to cyberattacks and compromises. Zero-trust security ensures that every device is treated as potentially untrusted and requires continuous authentication and authorization, regardless of location or network. By implementing zero-trust, organizations can better protect their IoT devices and collected data, reducing the risk of unauthorized access and potential breaches (Moffa, 2024).

Related Works

Empirical frameworks provide a systematic approach to conducting empirical research and analysis. They involve the development of theories or models, data collection, analysis, and

drawing conclusions based on empirical evidence. Empirical frameworks are commonly used in various fields, including social sciences, economics, and engineering, to study real-world phenomena and validate hypotheses. The adoption of IoT technologies in infrastructure management and information systems has garnered significant attention globally. Several studies have demonstrated the potential benefits of integrating IoT in critical sectors, such as energy, transportation, healthcare which are but a few to be stated

Liu et al. (2019) worked on secure Internet of Things (IoT) based smart world critical Infrastructures. They carry out a holistic survey on a detailed assessment of vulnerabilities in IoT-based critical infrastructures from the perspectives of applications, networking, operating systems, software, firmware, and hardware. In addition, they highlighted the three key critical infrastructure IoT-based cyber-physical systems, namely smart transportation, smart manufacturing, and smart grid. They introduced a case study, in which they assessed the impacts of potential attacks on critical IoT-based systems, using smart transportation systems as an example.

Mercan et al. (2020) stressed on the importance of developing comprehensive policies to address privacy, data protection, and ethical considerations of IoT implementations in the hospitality business. In this paper, they introduced various sectors in hospitality that adopted IoT with the implementation of specific applications. Then, investigated the security, privacy, and ethical concerns of IoT utilization by focusing on the hospitality domain. The hospitality environment poses some specific challenges in terms of secure and privacy-preserving implementation. Their aim was to increase awareness of potential risks as IoT is being adopted at a great pace. In their paper, they gave a typical example the case of Romantik Seehotel in Austria whose locking system was frozen by ransomware [6]. The hotel had to pay $1800 (two bitcoins) to end this Distributed Denial of Service (DDoS) attack. If the IoT devices are integrated with other information systems, perpetrators may access sensitive information such as credit card numbers or financial records (wang wei, 2018). They explore some exemplary uses, cases, potential problems, and solutions in order to contribute to better understanding and guiding the business operators in this sector. Finally, they gave some general guidelines to be adapted in the implementation and execution phases.

Acharya et al. (2022) conducted a study on IoT applications in agriculture, illustrating how IoT sensors and data analytics can revolutionize farming practices, leading to increased agricultural productivity and food security. Internet of Things (IoT) and data analytics (DA) are used to upgrade the operational effectiveness and profitability in horticulture. It not only gives importance to increased productivity, but it also emphasizes environmental sustainability along with features of data analytics, where the task is to find requirements and predict the suitability of a crop (Acharya et al., 2022).

Gubbi et al. (2013), the authors presented the Internet of Things (IoT): A vision, architectural elements, and future directions. This paper presents a Cloud-centric vision for the worldwide implementation of the Internet of Things. The key enabling technologies and application domains that are likely to drive IoT research shortly were discussed. This paper presented the current trends in IoT research propelled by applications and the need for convergence in several interdisciplinary technologies. Specifically, section 2, presented the overall IoT vision and the technologies that will achieve it. They discussed several application domains in IoT with a new approach in defining them in section 4 and section 5 providing Cloud-centric IoT vision. And finally, a case study of data analytics on the Aneka/Azure cloud platform was given and they concluded with discussions on open challenges and future trends in the last section.

In the African context, a report written by (Heath Muchena, 2019) Africacom highlighted how the Internet of Things was being deployed for regional challenges in energy, utilities, and transportation in Africa. During a conference in Cape Town Africacom highlighted how in Africa, IOT is focused on critical, often life-saving, utility, agricultural, transportation, and infrastructure applications.

South African-based mobile group Vodacom, for example, is investing heavily in IoT and has acquired a majority stake in IoT.nxt to develop applications for the automotive, mining, agriculture, finance, and consumer markets. Transnet – South Africa's state-owned rail, port, and pipeline company is one of the largest African entities implementing IoT technologies.

The company is using IoT technology for container and marine craft monitoring, smart energy management, and asset tracking, said Transnet CIO 'Rebatho Madiba'. Though the conference spotlighted several successfully implemented IoT applications, some speakers injected a note of caution. Vast IoT networks, transmitting data back to enterprise systems for analysis, have multiple points of weakness. When essential infrastructure such as hospitals and emergency alert systems are hacked, IoT-based "smart cities" could end up in nightmare scenarios.

Tahiru (2018) in his paper discussed cybersecurity in Africa: the threats and challenges. Also discussed on the commanding threats cyber insecurity poses to Africa as a continent. Relevant analysis was made in other to bring forth the consequences, the lack of cyber security mechanism subjected to a continent like Africa, and further plausibly explained the need to protect and guide desirously the internet space of Africa since it is exposed to hazards of many kinds. This paper qualitatively assesses relevant documents and frameworks about this field and other important literature, to develop an appreciable understanding of both the concepts of cybersecurity and accompanying challenges and threats, and to provide a more focused analysis and a basis for this piece of work. This paper discusses the digitalization of Africa's infrastructure systems vis-a-vee the challenges and threats the continent faces as far as the growing base of internet access is concerned. It explores to provide information and depict the clearest picture as to where the African continent stands about cyber security. The intent and purpose of this paper are to unearth and bring to bear the state of cyber security and cybercrime in Africa. The challenges and threads that are facing the continent have caused a whooping number of resources to go down the drain due to a lack of or loose measures in place as far as the protection and preserving the sanctity of the cyber community is concerned.

Das & Gündüz (2019) examined attacks on critical infrastructures, especially in recent years, and presented the most common attacks. Furthermore, security approaches to mitigate or prevent IP-based cyber-attacks are mentioned. With the increase in IoT-based solutions, network and Internet connections are established in these critical infrastructures. Therefore, these critical systems included in information networks are also subject to digital attacks. It is of great importance to identify the possible types of cyber-attacks, to take various precautions against these attacks, and to develop protection methods.

It is worth noting that in these related works, none of them carried out any detailed analysis on the existent IoT critical infrastructures nor provided the solution to overcome cyber-attacks in Africa, precisely Cameroon. So, in this study, we aim to provide a substantiated understanding of the concept of the Internet of Things and propose a robust security method on how to mitigate cyber-attacks on critical infrastructure in Cameroon. However, there is equally room for future studies in other sectors such as health, defence, space exploration, aviation industry, financial sector and environmental monitoring which are but few to be stated.

MATERIALS AND METHODS

Research Approach

Quantitative research approach was chosen for this study, which is characterized by the collection of numerical data and the use of statistical analysis. This approach was chosen because it was very appropriate for a precise measurement of responses, making it possible to draw objective inferences from the data.

The quantitative approach is particularly suitable for this study as it aims to analyze the impact of critical IoT on infrastructure and information systems in institutions in Cameroon. The use of a Likert scale questionnaire for data collection aligns with the quantitative approach, as it enabled the quantification of responses, thereby facilitating statistical analysis. The responses to the questionnaire provided valuable data on the current state of IoT infrastructure systems in these institutions, the IoT security challenges they faced, and the strategies they employed to overcome and manage these challenges.

Study Design

The research design for this study was a cross-sectional survey, which involved collecting data at a single point in time. This design is particularly suitable for this study as it allows for a snapshot of the current state of IoT infrastructure and information systems in institutions in Cameroon, aligning with the study's objectives.

This design enabled the collection of data from several respondents at one point in time, providing a comprehensive overview of the situation at that particular moment (Scriber, 2023). The cross-sectional design also aligned with the quantitative research approach of this study, as it allowed for the collection of numerical data and the use of statistical analysis. This made it possible to understand the situation regarding critical IoT infrastructure and information systems in Cameroon's institutions, which is the primary aim of this study.

Population

The population for this study included institutions in Cameroon that use IoT infrastructure and information systems. According to Simplilearn (2022), the population in research refers to the total set of observations that can be made. It is the entire group that a researcher is interested in, which he/she wishes to describe or draw conclusions about.

In the context of this study, the population was not individuals, but institutions that were implementing or have implemented IoT infrastructure and information systems. Selecting a population for a study is a critical step in the research process. In this case, the population was defined based on the focus of the study, which is IoT infrastructure and information systems in institutions in Cameroon. It is important to note that while the population included institutions in Cameroon that deployed IoT infrastructure and information systems, not all of these institutions were included in the study. A sample was selected from this population for the study. A sample represents a group of the interest of the population which was used to represent the data. The sample is an unbiased subset of the population which we used to represent the whole data. (GeeksforGeeks, 2022).

Sample Size

The sample size of one hundred (100) questionnaires for this study was set for about 10-15 institutions. This number represents the subset of the population that was surveyed in the research. The sample size is an important feature of any empirical study in which the goal is to make inferences about a population from a sample. The choice of a sample size is a critical

step in the research process as it can significantly impact the reliability and validity of the study's findings (Israel, 1992).

In this study, a sample size of 100 was chosen from the population of institutions in Cameroon that used or implemented IoT infrastructure and information systems. This sample size was manageable and allowed for a detailed analysis of each institution within the scope of the study.

Data Collection Method

Kothari (2004) explained that there are several methods for collecting primary data, especially in surveys and descriptive research. Data collection is a fundamental aspect of any research study. In this study, data was collected through a self-administered questionnaire. The questionnaire was divided into three sections, each addressing each of the research objectives. Each section contained questions, and respondents indicated their level of agreement with each statement on a five-point Likert scale. The use of a Likert scale allows for the quantification of responses, which facilitated statistical analysis. The data collected from the questionnaire were compiled and organized for analysis.

Validity and Reliability of Research Instrument

In this study, the research instrument was a self-administered questionnaire. The validity and reliability of this instrument are crucial to ensure the quality of the data collected. Validity refers to the extent to which the instrument measures what it is intended to measure. In other words, a valid instrument accurately reflects the concept it is designed to measure. For this study, the questionnaire was designed to gather data on the current state of IoT infrastructure systems in institutions, the IoT security challenges they faced, and the strategies they employed to overcome and manage these challenges. Therefore, the validity of the questionnaire determined how well it measured these aspects. Reliability, on the other hand, refers to the consistency and stability of the measurements obtained from the research instrument.

A reliable instrument produces consistent results when the measurement is repeated under the same conditions (Scribbr, 2022). In the context of this study, the reliability of the questionnaire was assessed by the consistency of the responses. To ensure the validity and reliability of the questionnaire, it was pre-tested with a small group of respondents. Their feedback was used to refine the questionnaire before it was administered to the full sample. This process helped to identify and correct any issues with the questionnaire that could affect its validity and reliability (Miami University, 2016).

Data Analysis

The questionnaire designed for the study was cross-examined to determine its accuracy, comprehensiveness, and reliability. The raw data that was collected through the questionnaire was coded in readiness for analysis to provide a means to introduce the interpretations into quantitative methods. The researcher read the data and established segments within it. Each segment was labeled with a "code" a word or short phrase that suggested how the associated data segments inform the research objectives. Descriptive statistics such as mode means and standard deviations aided by Statistical Package for Social Scientists (SPSS) 25.0 software, were used to analyze the data. The researcher used frequency Tables, charts, percentages, frequencies, and crosstabulation to establish the relationship between different variables. The results from the data analysis were interpreted and presented using the frequency distribution Tables, bar charts, and pie charts which were stored in both soft and hard copy.

Ethical Considerations

In the study, ethical considerations were of paramount importance and were carefully adhered to throughout the research process. These considerations were designed to protect the rights, safety, and well-being of research participants, as well as the integrity and credibility of the research itself (Scribbr, 2022). One of the key ethical considerations was a consent form which was administered to the selected institutions before data collection. The researchers ensured that participants' privacy and confidentiality were protected.

The aim of the study was to contribute to the understanding of IoT infrastructure and information systems in institutions in Cameroon and to provide insights that could help these institutions overcome and manage IoT security challenges. The potential benefits of the study were considered to outweigh any potential risks (Scribbr, 2022).

Study Area

The study area for this research was mainly the Mfoundi Division of the Center Region and the Mezam division in the Northwest of Cameroon. These regions are part of Cameroon often referred to as "Africa in miniature" due to its diverse climates and vegetation, which include mountains, rain forest, savanna grassland, and ocean coastland. The total population of Cameroon is approximately 26.55 million. Economically, Cameroon is the largest economy in the Economic and Monetary Community of Central Africa (CEMAC), contributing to over 40 percent of the region's GDP and over 60 percent of regional foreign exchange reserves. The country is also part of the Congo Basin, one of the world's three largest forests and the largest carbon sink. This study will focus on institutions within the Mfoundi and Mezam Divisions that are utilizing IoT infrastructure and information systems. The data collected from these institutions would provide valuable insights into the current state of IoT infrastructure systems, the IoT security challenges they face, and the strategies they employ to overcome and manage these challenges.

Mfoundi is characterized by its significant population and urban development. As of the 2005 census, the population was approximately 1,881,876 individuals, residing within an area of about 297.0 km² (Brinkhoff, 2017). This results in a high population density of 6,336 individuals per km², indicating a high level of urbanization. Between 1987 and 2005, Mfoundi experienced an annual population change of 5.4%, reflecting the region's dynamic demographic trends (Yang et al., 2011). These factors combined present both challenges and opportunities for urban planning, infrastructure development, and resource allocation in Mfoundi. Mezam is a division of the North West Region of Cameroon. The department covers an area of 1745 km2 and as of 2005 had a total population of 524,127(*Mezam*, 2024). The capital of the department lies at Bamenda. Subdivisions The department is divided administratively into 5 communes namely: Santa, Tubah, Bali, Bafut, and Abakwa Central. The Abakwa Central district is further divided into 3 sub-districts, namely Bamenda I, Bamenda II, and Bamenda II

Materials Used

Software Tools Used

Windows 10 Pro

Windows 10 was chosen as operating system and all applications were implemented with Windows 10 Professional version environment. There are many versions but this one is better due to its stability and ergonomics. It is also so familiar, easy to use, and has more built-in security. (*Microsoft Windows 10 Pro*, 2023.)

Statistical Package for Social Scientists (SPSS) 25.0

SPSS Statistics is a statistical software suite developed by IBM for data management, advanced analytics, multivariate analysis, business intelligence, and criminal investigation. Long produced by SPSS Inc., it was acquired by IBM in 2009. Versions of the software released since 2015 have the brand name IBM SPSS Statistics.

The software name originally stood for Statistical Package for the Social Sciences (SPSS), reflecting the original market, then later changed to Statistical Product and Service Solutions. ('SPSS', 2023)

Kobo Toolbox

Kobo Toolbox is an intuitive, powerful, and reliable software used to collect, analyze, and manage data for surveys, monitoring, evaluation, and research. It is extremely user-friendly and accessible, making it easy to get started quickly. It works offline, on any device. Most importantly, all its core functionalities are free to use for nonprofit organizations.

Google Forms

Google Forms is a survey administration software included as part of the free, web-based Google Docs Editors suite offered by Google. Users can analyze responses to their form using either the built-in analysis tools, or export them to a new or existing Google Sheets spreadsheet that updates as new responses are received. Google Forms is only available as a web application. The app allows users to create and edit surveys online while collaborating with other users in real time. The collected information can be automatically entered into a spreadsheet. ('Google Forms', 2023)

Hardware Tools Used

For the analysis part of our work, we used a computer having the following characteristics:

- Intel Core i5 processor with a clock speed of 2.7 GHz.
- 6 GB of RAM.
- 500 G0 hard disk capacity.
- Screen: 15 inches
- Operating System: Windows 10 Professional 64-bits

FINDINGS

Here, the researchers provided an analysis of the research findings and data collected in the field. As reviewed in the the previous sections above, the main objective of this study was to analyze the impact of critical IoT on infrastructure and information systems in Africa with a focus on Cameroon. As such, this section is structured in three sections. The first section contains information on the demographic of the respondent. The second gives a descriptive analysis of the responses of the participants concerning the research objectives and the third discusses the findings about the study research objective.

Response Rate

Out of the 100 participants who were sampled for the study, 89 responded to the questionnaire. In this regard, it can be concluded that the response rate for the research was 89%.

Demographic Data Analysis

The study was interested in the demographic information of the respondents to assess the target population under study. The entailed information on respondents included a sector of critical infrastructure, gender, age, and qualification.

Distribution of Respondents by Sector of Critical Infrastructure.

The figure below captures the impact of the Internet of Things (IoT) across various sectors of critical infrastructure in Cameroon. The data, accurately collected and analyzed, provided a snapshot of how IoT is reshaping these sectors. From Information Technology to Banking and Finance, each sector's representation is quantified by its frequency and percentage, offering a clear picture of the extent of IoT integration. Figure 3 below detailed sector-wise analysis.

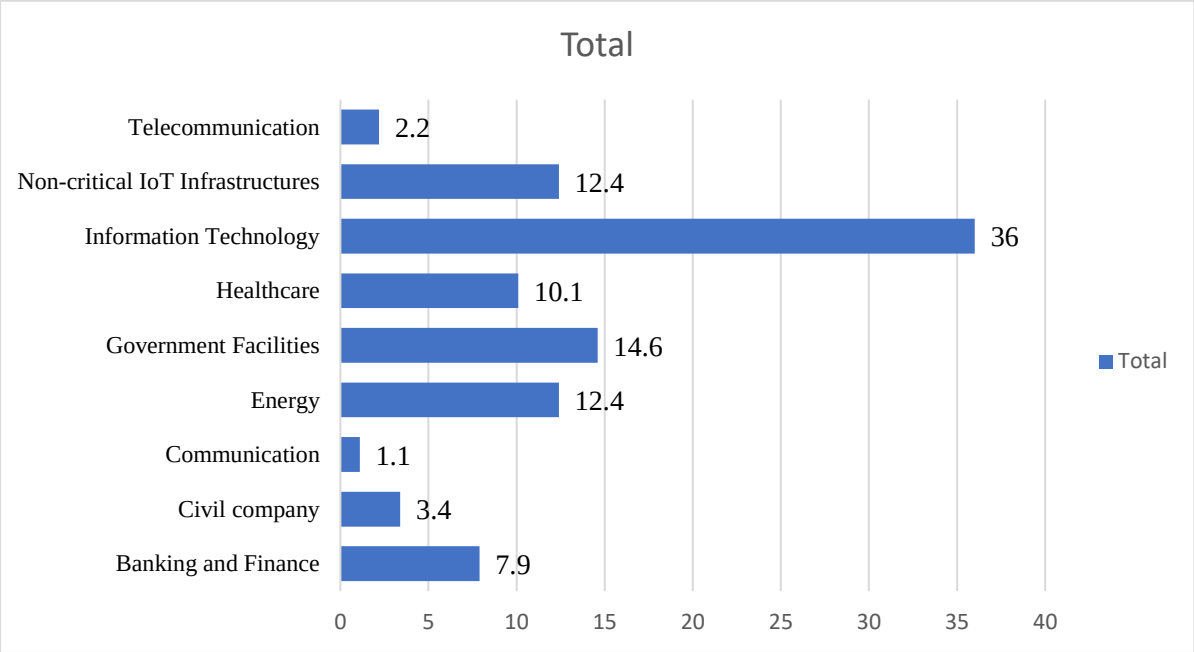

Figure 3: Distribution of Respondents by Sector of Critical Infrastructure

Figure 3 offers an insightful analysis of the distribution of various critical infrastructure sectors in Cameroon, each impacted by the Internet of Things (IoT) to varying degrees. The Information Technology sector emerged as the most prominent, accounting for a substantial 36.0% of the total responses. This underscored the significant interplay between IoT and IT. The Energy and Non-critical IoT Infrastructures sectors followed closely, each contributing 12.4% to the total. The Healthcare sector, with a 10.1% share, underscores the increasing penetration of IoT in healthcare systems. Government Facilities, representing 14.6% of the total, indicated a growing trend of IoT utilization in public services. Conversely, the Banking and Finance sector, making up 7.9% of the total, suggests a more measured integration of IoT. The least represented sectors - Civil Company and Telecommunication - contributed 3.4% and 2.2% respectively, indicating potential areas for further IoT exploration. Lastly, the Communication sector, with a single representation accounting for 1.1%, points towards an emerging area for future IoT integration.

Distribution of Respondents by Gender

It was necessary to get the gender of the respondents to establish the percentage of each gender and henceforth be able to classify if the data of respondents at various sectors of infrastructure was balanced. This is because both genders have a great role to play as far as the policies guiding employment in Cameroon are concerned.

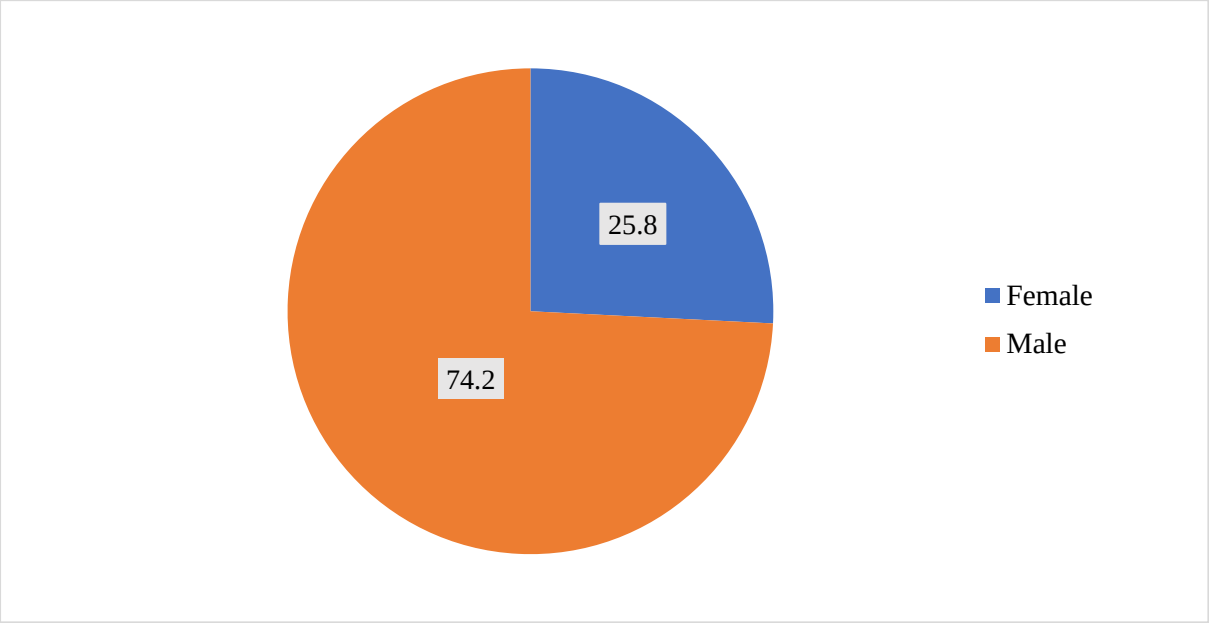

Figure 4: Distribution of Respondent by Gender

Figure 4 above presents a gender-based analysis of the participants. Out of the total 89 respondents, a significant majority, precisely 66 or 74.2%, were male. This leaves a smaller but yet a substantial portion of the sample, 23 or 25.8%, as female. This data suggests a male-dominated participant pool in this study.

Distribution of Respondents by Age

On the distribution of Respondents by Age, the participants were grouped into various age sets of class intervals of 9 years. The age of the respondents distributed ranged from 20 years to 60 years and above. This is revealed in Figure 5 below

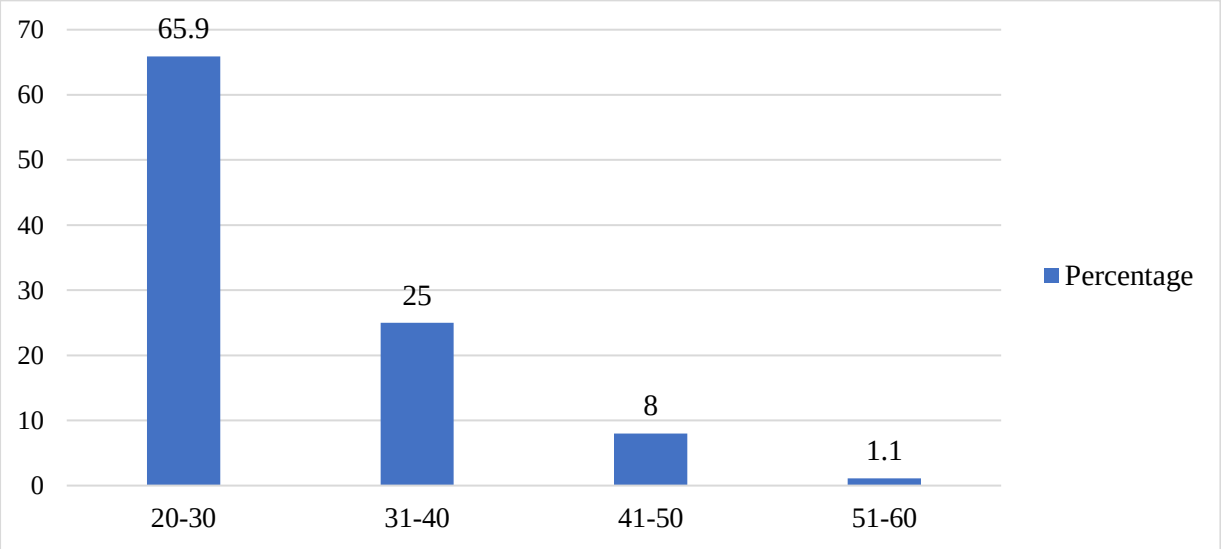

Figure 5: Distribution of Respondents by Age

Figure 5 above provides a compelling demographic breakdown of the respondents by age. A substantial majority, precisely 65.9%, fell within the 20-30 age bracket, indicating a youthful participant. The next significant age group, 31-40, represents a quarter of the respondents, accounting for 25%. The remaining respondents are distributed across the 41-50 and 51-60 age

groups, contributing 8% and a minimal 1.1% respectively. This data offers valuable insights into the age dynamics of the study's participants.

Distribution of Respondents by Level of Education

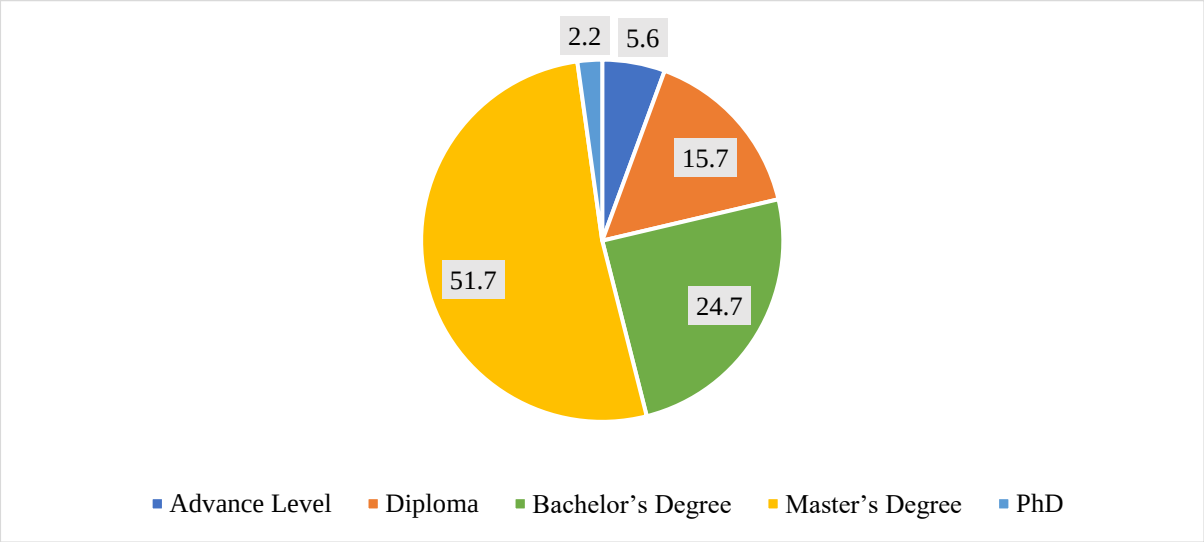

Figure 6: Distribution of Respondents by Academic Qualification

Figure 6 above illuminates the diverse educational backgrounds of the study's respondents. A significant proportion of the respondents, 51.7% to be precise, hold a Master's Degree, while 24.7% have earned a Bachelor's Degree. This indicates a high level of academic achievement among the infrastructure sector workers assessed in this study. Furthermore, a noteworthy 15.7% of respondents possess a Diploma, and 5.6% have an Advanced Level Certificate, contributing to the diversity of educational qualifications. Interestingly, a select group of respondents, accounting for 2.2% of the total participants, held a Ph.D., representing the peak of academic accomplishment in this study.

Presentation of Result Findings

This research embarked on an in-depth exploration of the impact of critical IoT on infrastructure and information systems, with a specific focus on Africa, and more precisely, Cameroon. Like other empirical studies, this research was steered by three distinct objectives, each contributing to a comprehensive understanding of the subject matter. The first objective aimed to delve into the current landscape of IoT Infrastructure Systems in Cameroon. This involved a thorough examination of respondents' existing IoT systems, their implementation, and their integration within various sectors. The goal was to provide a clear picture of how IoT was currently being utilized in Cameroon and how it was influencing infrastructure and information systems. The second objective sought to unearth the security challenges posed by IoT about its critical infrastructure. This involved identifying potential vulnerabilities, risks, and threats associated with IoT implementation. The aim was to highlight areas that require attention and improvement to ensure the secure and effective use of IoT in critical infrastructure. The third objective revolved around discussing these identified IoT security challenges and proposing strategies to surmount and manage these hurdles effectively. This included suggesting potential solutions, preventive measures, and management strategies that could be employed to tackle the identified challenges. These objectives served as the basis for the presentation and analysis of results. They guided the research process, shaping the direction of the study and ensuring a focused approach toward understanding the impact of critical IoT on infrastructure and information systems in Cameroon.

Objective One: Discuss the Current State of IoT Infrastructure Systems in Cameroon

The first objective of this research was to delve into the current state of IoT (Internet of Things) Infrastructure Systems in Cameroon. This objective is essential as it sets the stage for understanding the extent of IoT integration and its impact on various sectors within the country. The focus here is twofold. Firstly, we aimed to assess the knowledge and awareness of IoT among the participants. This involves understanding their familiarity with IoT, its applications, and its potential benefits and challenges. Secondly, the study aims to discuss the current state of IoT Infrastructure Systems in Cameroon. This involves examining the existing IoT systems, their implementation, and their integration within various sectors. In essence, this objective serves as a foundation for the study, providing a comprehensive understanding of the IoT landscape in Cameroon.

The forthcoming Table offers a detailed insight into the respondents' knowledge and understanding of the Internet of Things (IoT). It captures the respondents' familiarity with various aspects of IoT, from the concept of connected devices to the integration of physical objects with digital technology. The table also sheds light on the respondents' awareness of practical IoT applications, such as the use of sensors in various infrastructures and remote monitoring and control of devices. Findings are presented in Table 4.1 below.

Table 1: Respondent's Knowledge of the Internet of Things (IoT)

Variables	Very High Extent	High Extent	Low Extent	No Extent
Concept of Connected Devices	32.6%	48.3%	19.1%	00%
Integration of Physical Objects with Digital Technology	33.7%	39.3%	22.5%	4.5%
Use of Sensors in Various Infrastructures	37.1%	40.4%	18%	4.5%
Remote Monitoring and Control of Devices	38.2%	32.6%	16.9%	12.4%

The data presented in Table 1 above provides a comprehensive understanding of the respondents' knowledge and awareness of the Internet of Things (IoT). A significant majority of respondents, 80.9%, are familiar with the concept of connected devices, a fundamental principle of IoT. Furthermore, 73% of respondents had a high or very high extent of knowledge about the integration of physical objects with digital technology, a key aspect of IoT. However, it is worth noting that 4.5% reported no knowledge in this area. In terms of practical applications, 77.5% of respondents understood the use of sensors in various infrastructures such as agriculture, healthcare, telecommunication systems, and energy systems. This suggests a good understanding of how IoT is applied in different sectors. Additionally, 70.8% of respondents are familiar with the concept of remote monitoring and control of devices through the internet, one of the key benefits of IoT. However, 12.4% reported no familiarity with this concept. Overall, the data suggests a substantial level of understanding and awareness about IoT among the respondents.

The Table 2 below provides a detailed examination of the current state of IoT Infrastructure Systems in Cameroon, particularly focusing on the aspect of security. The table captures respondents' perceptions on various facets such as the perceived security of IoT infrastructures in their sector, witnessed security breaches, the need for stricter regulations, confidence in

current security levels, the importance of collaboration among stakeholders, and recommendations for specific technologies or solutions to enhance security.

Table 2: The Current State of IoT Infrastructure Systems in Institutions

Variables	Very High Extent	High Extent	Low Extent	No Extent
Perceived Security of IoT Infrastructures	13.5%	40.5%	37.1%	09%
Witnessed Security Breaches	3.4%	14.6%	49.4%	32.6%
Need for Stricter Regulations	64%	19.1%	14.6%	2.2%
Confidence in Current Security Levels	7.9%	36%	38.2%	18%
Importance of Collaboration	48.3%	27%	20.2%	4.5%
Recommendation of Specific Technologies/Solutions to enhance the security of CIS	44.9%	44.9%	7.9%	2.2%

The data presented in Table 2 above provides a comprehensive understanding of the current state of IoT Infrastructure Systems in Cameroon, particularly from a security perspective. A combined 54% of respondents believe that IoT infrastructures in their sector are secure to a high or very high extent, while 46% perceive them as only somewhat secure or not secure at all. When it comes to witnessing security breaches or incidents, a majority (82%) have witnessed them to a low extent or not at all, suggesting that while breaches may occur, they are not highly prevalent or noticeable. On the other hand, a significant 83.1% of respondents believe there is a high or very high need for stricter regulations regarding the security of critical IoT infrastructures. This indicates a strong demand for more robust security measures. However, only 44% of respondents are confident to a high or very high extent in the current level of security implemented in critical IoT infrastructures. Nearly 75.3% of respondents believe to a high or very high extent that collaboration among different stakeholders is crucial for securing critical infrastructures. Furthermore, a combined 89.8% would recommend specific technologies or solutions to enhance the security of Critical Infrastructure Systems (CIS) to a high or very high extent.

The respondents were also enquiring about their observations concerning the current state of IoT Infrastructure Systems in Cameroon. Findings revealed a multifaceted perspective. A strong belief in the robustness of IoT infrastructure security, particularly due to the implementation of blockchain technology, is evident. However, there is also a call for the government to sensitize youth about the security of critical infrastructures. The presence of IoT, such as video surveillance in school premises, is noted and there's a suggestion for broader implementation of IoT in schools. On the other hand, while IoT is recognized as a beneficial concept, concerns are raised about the potential for misuse, particularly in the African environment. This highlights the need for more education on IoT, as it's a new technology that most companies in Cameroon are not yet accustomed to. Observations indicate that there's little digitalization and no major digitalized system currently in place. There's also a noted lack of willingness to change to IoT. The low level of awareness and adoption of IoT solutions among educators and learners is seen as limiting the potential benefits of IoT in enhancing teaching and learning outcomes.

Objective Two: To Identify IoT Security Challenges in Line with its Critical Infrastructure

The second objective of this research was to identify the security challenges associated with IoT in the context of critical infrastructure. This objective is crucial as it helped us to understand the vulnerabilities and risks associated with the implementation of IoT in these sectors. The focus here is on evaluating the significance of these security challenges across various critical infrastructure sectors. This involved assessing how these challenges impact the functionality, reliability, and integrity of IoT systems within these sectors. By doing so, we can gain an understanding of the areas that need improvement or reinforcement to ensure the secure and effective use of IoT in critical infrastructure. This objective serves as a stepping stone towards enhancing the security posture of IoT Infrastructure Systems in Cameroon.

The table below provides a comprehensive study of the significance of various security challenges associated with IoT within critical infrastructure sectors in Cameroon. The table captures respondents' perceptions on a range of issues, from encryption and authentication to unauthorized access, data breaches, physical tampering, and insider threats. It also sheds light on the need for standardized security protocols.

Table 3: Security challenges associated with IoT within critical infrastructure sectors

Variables	Insignificant	Minor	Moderate	Major
Lack of Encryption and Authentication	7.9%	10.1%	39.3%	42.7%
Unauthorized Access and Data Breaches	3.4%	6.7%	32.6%	57.3%
Physical Tampering and Sabotage	2.2%	15.7%	44.9%	37.1%
Insider Threats	2.2%	12.4%	48.3%	37.1%
Lack of Standardized Security Protocols	6.7%	7.9%	58.4%	27%
Supply Chain Vulnerabilities.	3.4%	22.5%	51.7%	22.5%
Complexity and Scale of Interconnected Systems	5.6%	10.1%	51.7%	32.6%

The data in Table 3 provided a wide-ranging understanding of the significance of various security challenges in IoT for critical infrastructure sectors in Cameroon. A significant 82% of respondents viewed the lack of encryption and authentication as a moderate or major concern, with 42.7% viewing it as a major concern and 39.3% as a moderate concern. This highlights the importance of encryption and authentication in IoT security. Unauthorized access and data breaches were viewed as a moderate or major challenge by a substantial 90% of respondents, with 57.3% viewing it as a major challenge and 32.6% as a moderate challenge.

This underscores the criticality of preventing unauthorized access and data breaches in ensuring IoT security. Physical tampering and sabotage are viewed as a moderate or major risk by 82% of respondents, with 37.1% viewing it as a major risk and 44.9% as a moderate risk. Insider threats are viewed as a moderate or major concern by 85.4% of respondents, with 37.1% viewing it as a major concern and 48.3% as a moderate concern. The lack of standardized security protocols is viewed as a moderate or major challenge by 85.4% of respondents, with 27% viewing it as a major challenge and 58.4% as a moderate challenge. While there are various challenges in ensuring IoT security for critical infrastructure, they are recognized and considered significant by a majority of respondents.

Respondents were also enquired if there are any other CIS security challenges that they have encountered in your institution. Figure 7 below depicts their responses.

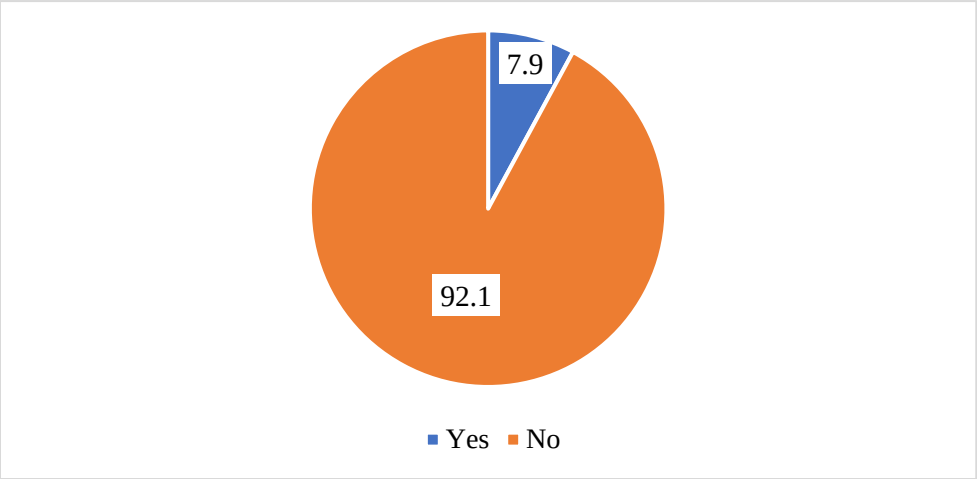

Figure 7: Additional CIS Security Challenges that Institutions Encountered

Figure 7 provides insights into additional Critical Infrastructure Systems (CIS) security challenges encountered by respondents in their institutions. Out of the total 89 respondents, only 7 (7.9%) reported encountering other CIS security challenges in their institutions. The majority, 82 respondents (92.1%), did not report any additional challenges. For those who reported additional challenges, they mentioned: building from-scratch issues, Cyber theft, challenges in achieving high security as per models, insiders publishing fake news about the company, lack of authentication on government user portals, and issues with sensor monitoring in case of service disruption as additions challenges encountered within their institutions. These additional challenges highlight the complexity and multifaceted nature of securing IoT in critical infrastructure sectors. They underscore the need for comprehensive security strategies that address not only common threats but also institution-specific challenges.

Objective Three: To Discuss the Various Iot Security Challenges and how to Overcome Plus Manage these Challenges

Objective Three of our study focuses on evaluating how to develop effective protection methods against security challenges in the realm of the Internet of Things (IoT). This objective is of paramount importance as the proliferation of IoT devices has exponentially increased the potential attack surface for cyber threats. The evaluation process involves a comprehensive analysis of various protective measures such as conducting regular security audits, implementing strong access control measures, encryption, and authentication mechanisms, and regularly updating and patching software and firmware. The objective also emphasizes the role of Critical Infrastructure Sectors (CIS) in encouraging and promoting the deployment of these effective protection methods. By focusing on these areas, the study aims to develop a robust framework that can significantly enhance the security posture of IoT systems in institutions in Cameroon.

Table 4: Protection Method Against IoT Security Challenges

Variables	Strongly Disagree	Disagree	Agree	Strongly Disagree
Conducting regular security audits and assessments	13.5%	4.5%	33.7%	48.3%
Implementing strong access control measures	09%	5.6%	39.3%	46.1%
Implementing encryption and authentication mechanisms	09%	09%	36%	46%
Regularly updating and patching software and firmware	10.1%	13.5%	41.6%	34.8%
Encouraging and promoting the deployment of effective protection methods in Critical Infrastructure Sectors (CIS)	6.7%	7.9%	38.2%	47.2%

Table 4 indicates a strong consensus among respondents on the importance of various methods for developing protection against security challenges. A significant majority, 82%, agree or strongly agree that conducting regular security audits and assessments is an effective method. Similarly, implementing strong access control measures is seen as beneficial by 85.4% of respondents. Implementing encryption and authentication mechanisms also received strong support with 82% agreement. In terms of software maintenance, 76.4% of respondents agree or strongly agree that regularly updating and patching software and firmware is an important aspect of developing protection against security challenges. Furthermore, there is a strong belief (85.4% agree or strongly agree) that Critical Infrastructure Sectors (CIS) should encourage and promote the deployment of effective protection methods for Internet of Things systems. This data underscores the perceived importance of these measures in addressing IoT security challenges.

Figure 8 below delves into whether institutions are employing any additional protection methods. While a majority are not, a small percentage have implemented further measures such as authentication measures, regular security audits, intrusion detection, and traffic and systems isolation.

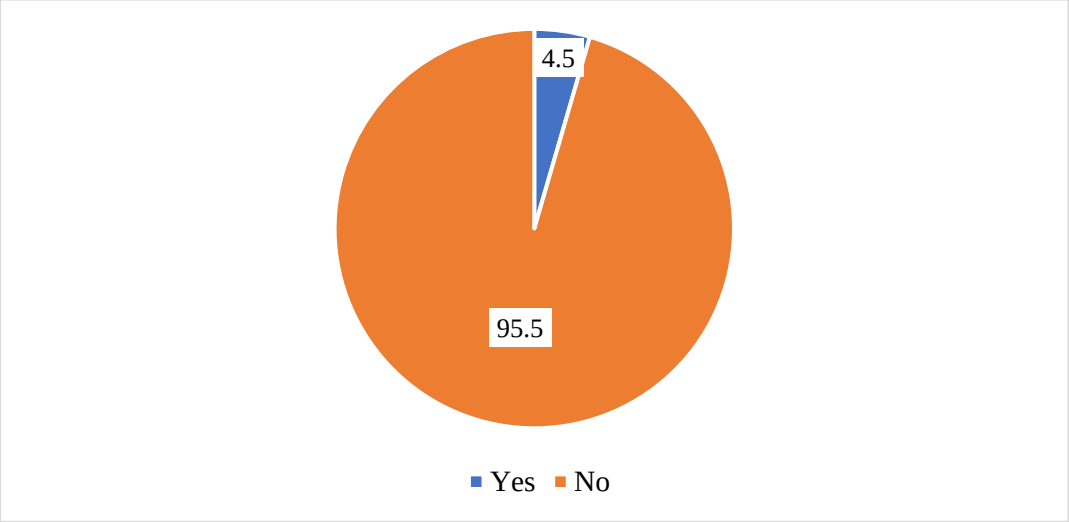

Figure 8: Protection Method against IoT Security Challenges

Figure 8 above indicated that a majority of institutions, 95.5%, are not using any protection methods other than those previously mentioned. However, a small percentage (4.5%) of institutions have implemented additional measures. These include authentication measures, regular security audits, intrusion detection, and traffic and systems isolation. These additional measures highlight the multifaceted approach institutions are taking to tackle IoT security challenges. Authentication measures and regular security audits help ensure that only authorized individuals have access to IoT systems and that any potential vulnerabilities are identified and addressed promptly. Intrusion detection systems provide an additional layer of security by identifying and alerting to any unauthorized access or suspicious activity. Traffic and systems isolation can help contain any potential security breaches, preventing them from spreading across the network.

Discussion of Findings

Objective One: Discuss the Current State of IoT Infrastructure Systems in Cameroon.

The findings from our study revealed a substantial understanding and awareness of the Internet of Things (IoT) among the respondents. A significant majority are familiar with the concept of connected devices and the integration of physical objects with digital technology**.** In terms of practical applications, many respondents understand the use of sensors in various infrastructures such as agriculture, healthcare, telecommunication systems, and energy systems. This indicates a good understanding of how IoT is applied in different sectors. Additionally, many respondents are familiar with the concept of remote monitoring and control of devices through the Internet. However, a small percentage reported no knowledge or familiarity in these areas. This suggests that while there is a substantial level of understanding and awareness about IoT, there is still room for improvement in terms of education and awareness campaigns.

Furthermore, the results revealed that while a majority of respondents believed that IoT infrastructures in their sector were secured, a significant portion perceived them as only somewhat secure or not secure at all. This dichotomy underscores the complexity and variability of security perceptions within the IoT landscape, aligning with the findings of (Roman et al., 2013). In terms of security incidents, most respondents have witnessed them to a low extent or not at all. This could suggest that while breaches may occur, they were either not highly prevalent, not noticeable, or perhaps not reported. This finding aligns with the work of (Stouffer, 2023), who highlighted the often-invisible nature of cyber threats until they manifest in a breach. Also, the findings showed that there was a strong demand for stricter regulations regarding the security of critical IoT infrastructures. This finding was particularly relevant in light of ongoing debates in cybersecurity literature about the role and effectiveness of regulation in enhancing security (Weber, 2010). The confidence level in the current security measures implemented in critical IoT infrastructures is less than half. This suggests a potential gap between the perceived importance of IoT security and the confidence in existing measures. It aligns with broader discussions about the challenges of securing increasingly complex and ubiquitous IoT systems (Alaba et al., 2017). The belief that collaboration among different stakeholders is crucial for securing critical infrastructures was widely held among respondents. This finding resonated with the current discourse on the importance of multi-stakeholder approaches to cybersecurity (Cherdantseva et al., 2016). Finally, most respondents would recommend specific technologies or solutions to enhance the security of Critical Infrastructure Systems (CIS). This suggests an openness to innovation and new approaches in addressing IoT security challenges. These findings contribute significantly to our understanding of the current state of IoT Infrastructure Systems in Cameroon. They highlighted areas for further research

and potential intervention, including regulation, multi-stakeholder collaboration, and innovative security solutions.

Objective Two: To Identify IoT Security Challenges in Line with its Critical Infrastructure

The findings revealed that a significant number of respondents viewed the lack of encryption and authentication as a concern. This emphasizes the importance of encryption and authentication in IoT security as pointed out by Thales (2022.) in his work. Unauthorized access and data breaches were viewed as a challenge by a substantial number of respondents, underscoring the criticality of preventing unauthorized access and data breaches in ensuring IoT security (ISACA, 2019). Physical tampering and sabotage are viewed as a risk by many respondents. Insider threats are viewed as a concern by a majority of respondents. The lack of standardized security protocols was viewed as a challenge by many respondents. These findings highlighted the complexity and multifaceted nature of securing IoT in critical infrastructure sectors, underscoring the need for comprehensive security strategies that address not only common threats but also institution-specific challenges. A small number of respondents reported encountering other Critical Infrastructure Systems (CIS) security challenges in their institutions, such as building from scratch issues, cyber theft, challenges in achieving high security as per models, insiders publishing fake news about the company, lack of authentication on government user portals, and issues with sensor monitoring in case of service disruption (MDPI, 2020). These findings contributed to our understanding of the current state of IoT Infrastructure Systems in Cameroon. They highlighted the importance of addressing these challenges to ensure the security and integrity of critical infrastructure sectors.

Also, the findings further revealed that a small number of respondents reported encountering other Critical Infrastructure Systems (CIS) security challenges in their institutions. These included building-from-scratch issues, cyber theft, challenges in achieving high security as per models, insiders publishing fake news about the company, lack of authentication on government user portals, and issues with sensor monitoring in case of service disruption. These additional challenges highlighted` the complexity and multifaceted nature of securing IoT in critical infrastructure sectors as reviewed by Smith (2023) in his work “Analysis of Critical IoT Infrastructures and Information. Journal of IoT Research.”

Objective Three: To Discuss the Various IoT Security Challenges and how to Overcome Plus Manage these Challenges.

The findings from Table 5 revealed a strong consensus among respondents on the importance of various methods for developing protection against security challenges. A significant majority concur that conducting regular security audits and assessments is an effective method. This is related to a review by JAC-ECC. (2020) on IoT Security Challenges and Solutions. 8th International Japan-Africa Conference on Electronics, Communications, and Computations. Similarly, implementing strong access control measures is seen as beneficial by a large number of respondents (Abiodun et al., 2021). Implementing encryption and authentication mechanisms also received strong support. In terms of software maintenance, a considerable number of respondents agree that regularly updating and patching software and firmware is an important aspect of developing protection against security challenges (Wireless Mobile Ad-hoc Network, 2020). Furthermore, there is a strong belief that Critical Infrastructure Sectors (CIS) should encourage and promote the deployment of effective protection methods for Internet of Things systems (Zhang et al., 2020). These findings provide a valued understanding of how to overcome and manage IoT security challenges. The findings emphasize the need for

regular audits, strong access control measures, encryption, authentication mechanisms, and software maintenance.

Furthermore, the findings revealed that most institutions are not using any protection methods other than those previously mentioned. However, a small number of institutions have implemented additional measures. These included authentication measures, regular security audits, intrusion detection, and traffic and systems isolation. These additional measures highlight the multifaceted approach institutions are taking to tackle IoT security challenges. Authentication measures and regular security audits help ensure that only authorized individuals have access to IoT systems and that any potential vulnerabilities are identified and addressed promptly as discussed by Smith (2021). Intrusion detection systems provide an additional layer of security by identifying and alerting to any unauthorized access or suspicious activity as discussed by Johnson & Williams (2022). Traffic and systems isolation can help contain any potential security breaches, preventing them from spreading across the network as revealed by Brown et al. (2023). These findings emphasized the importance of a comprehensive approach to IoT security. They highlighted the need for a combination of preventive measures such as authentication and regular audits, as well as reactive measures like intrusion detection and traffic isolation.

Summary of the Findings

The general objective of this study was to analyze the impact of IoT on critical infrastructure and information systems in Africa with a focus on Cameroon. This research examined three measures objectives firstly to delve into the current landscape of IoT Infrastructure Systems in Cameroon, secondly to unearth the security challenges posed by IoT in relation to its critical infrastructure and finally to discuss these identified IoT security challenges and propose strategies to surmount and manage these hurdles effectively. To assess these three measures, the researcher adopted descriptive statistics where questionnaires and interviews were carried out by the research student. A survey questionnaire was randomly distributed to 100 respondents in some parts of Cameroon, and only 89 validated questionnaires were obtained. The primary data collected from the respondents were analysed with a statistical package for social science (SPSS) and the results were summarised in pie charts and frequency tables.

Generally, findings based on demographic characteristics revealed that Out of the 100 participants who were sampled for the study, 89 responded to the questionnaire, and the number of males exceeded the number of female employees. Female respondents constituted 25.8% of the entire sample size, while the remaining 74.2% were male patients. This result does not necessarily imply that males are more employed than females in this country. Also, findings on respondents' knowledge and understanding of the technology Internet of Things (IoT) demonstrated that a significant majority of respondents, 80.9%, are familiar with the concept of connected devices, a fundamental principle of IoT. On the other hand, while examining the respondents on a comprehensive understanding of the current state of IoT Infrastructure Systems in Cameroon, particularly from a security perspective, 54% of respondents believe that IoT infrastructures in their sector were secure to a high or very high extent, while 46% perceive them as only somewhat secure or not secure at all.

Again, questions to identify the security challenges associated with IoT in the context of critical infrastructure. The focus here was evaluating the significance of these security challenges across various critical infrastructure sectors it came out that some security challenges such as unauthorized access and data breaches are viewed as a moderate or major challenge by a substantial 90% of respondents, with 57.3% viewing it as a major challenge and 32.6% as a

moderate challenge. While there are various challenges in ensuring IoT security for critical infrastructure, they are recognized and considered significant by a majority of respondents.

The results from evaluating how to develop effective protection methods against security challenges in the realm of the Internet of Things (IoT) showed that a significant majority concurred that conducting regular security audits and assessments is an effective method, implementing encryption and authentication mechanisms also received strong support, respondents agree that regularly updating and patching software and firmware is an important aspect of developing protection against security challenges.

The findings of the study have broadened and deepened the understanding the impact of IoT on critical infrastructures and information systems in Cameroon. As per analysis and discussion from chapter four, some of the deficiencies were revealed:

- The existing IoT infrastructure in Cameroon is limited and lacks comprehensive coverage.
- Information systems in critical sectors such as healthcare, transportation, and energy face significant vulnerabilities. For instance, we can notice the presence of outdated software, lack of cybersecurity awareness and data manipulation/misused in the above sectors.
- Cybersecurity measures in place were inadequate, leaving these systems susceptible to cyber threats.
- There is a need for investment in robust and secure IoT infrastructure to enhance the efficiency and security of critical services.
- Collaboration between government, industry stakeholders, and cybersecurity experts is crucial to address the identified challenges and ensure the resilience of IoT infrastructures in Cameroon.

CONCLUSION AND RECOMMENDATIONS

Recommendations

A lot of issues have been identified and learned throughout the development of the research project. To this effect, we put forth the following recommendations to both Cameroonian government and stakeholders:

- Conducting research to identify the specific needs and challenges in implementing IoT infrastructures and information systems in Cameroon, and developing tailored solutions to address them.
- Infrastructure Development: Investing in the development of robust and reliable internet infrastructure to support the widespread deployment of IoT devices and enable seamless connectivity across the country.
- Pilot Projects: Providing training programs and workshops to enhance the technical skills of professionals in IoT technologies, cybersecurity, data analytics, and information systems management and implementing small-scale pilot projects in different sectors, such as healthcare, agriculture, transportation, or energy, to evaluate the feasibility and effectiveness of IoT infrastructures and information systems in the Cameroonian context.
- Encouraging collaboration between government agencies, academic institutions, private sector organizations, and international partners to share knowledge, resources, and best practices in the field of IoT infrastructures and information systems.

- Public Awareness and Engagement: Conduct awareness campaigns to educate the public about the benefits, risks, and responsible use of IoT technologies, fostering a culture of digital literacy and cybersecurity awareness.

The researcher believes that this study is of great importance to other researchers in Cameroon and thus recommends that the government should see how to embrace this innovative technology to increase the efficiency of critical infrastructures.

Conclusion

In conclusion, the analysis of Critical IoT Infrastructure and Information has illuminated the intricate and dynamic landscape in which these interconnected systems operate. The examination of vulnerabilities, risks, and the impact of potential breaches underscores the urgency and importance of securing critical infrastructures such as electronic communication, energy, banking and finance, critical public services, transportation, and water management. Cyber-attacks against these crucial infrastructures are increasingly growing day by day so if very important and critical steps are not taken to solve security problems, damages resulting from cyber-attacks on critical infrastructures will lead to a nightmare for nations and organizations with devastating consequences. IoT applications are the most important structures in terms of enhancing performance and communication in critical infrastructures. However, all attacks that can happen on the Internet can be performed in IoT environments too. Therefore, using IoT applications in critical infrastructures can lead to cyber-attacks that can be performed on the Internet. In conclusion, safeguarding critical IoT infrastructures is not merely a technical challenge but a multidimensional task that requires strategic, ethical, and collaborative considerations. Through ongoing research, development, and a commitment to best practices, we can work towards a future where these interconnected systems contribute to societal advancement without compromising security and privacy.

REFERENCE

Abiodun, O., Omolara, O., Alawida, M., Alkhawaldeh, R., & Arshad, H. (2021). A Review on the Security of the Internet of Things: Challenges and Solutions. *Wireless Personal Communications*, *119*, 1–35. https://doi.org/10.1007/s11277-021-08348-9

Acharya, B., Garikapati, K., Yarlagadda, A., & Dash, S. (2022). *Internet of things (IoT) and data analytics in smart agriculture: Benefits and challenges* (pp. 3–16). https://doi.org/10.1016/B978-0-12-823694-9.00013-X

Affia, A. O., Finch, H., Jung, W., Samori, I. A., Potter, L., & Palmer, X.-L. (2023). IoT Health Devices: Exploring Sec:urity Risks in the Connected Landscape. *IoT*, *4*(2), Article 2. https://doi.org/10.3390/iot4020009

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. https://doi.org/10.1016/j.jnca.2017.04.002

Alaine, B. T. (2 August 2023). How AI and IoT are driving SDGs in Cameroon and Beyond. Retrieved 27 January 2025, sur https://www.linkedin.com/pulse/how-ai-iot-driving-sdgs-cameroon-beyond-bate-tabenyang-alaine

Alcaraz, C., & Zeadally, S. (2015). Critical infrastructure protection: Requirements and challenges for the 21st century. *International Journal of Critical Infrastructure Protection*, *8*, 53–66. https://doi.org/10.1016/j.ijcip.2014.12.002

Al Sadawi, A., Hassan, M., & Ndiaye, M. (2024). Blockchain Technology for IoT Security and Trust: A Comprehensive SLR.

Baykara, M., & Daş, R. (2015). A Survey on Potential Applications of Honeypot Technology in Intrusion Detection Systems. *International Journal of Computer Networks and Applications*, *2*(5).

Bou-Harb, E., Fachkha, C., Pourzandi, M., Debbabi, M., & Assi, C. (2013). Communication security for smart grid distribution networks. *IEEE Communications Magazine*, *51*(1), 42–49. https://doi.org/10.1109/MCOM.2013.6400437

Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., & Stoddart, K. (2016). A review of cyber security risk assessment methods for SCADA systems. *Computers & Security*, *56*, 1–27. https://doi.org/10.1016/j.cose.2015.09.009

Coventry, L., & Branley, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. *Maturitas*, *113*, 48–52. https://doi.org/10.1016/j.maturitas.2018.04.008

D. E. Whitehead, K. Owens, D. Gammel, and J. Smith. (2017). *Ukraine cyber-induced power outage: Analysis and practical mitigation strategies | IEEE Conference Publication | IEEE Xplore*. https://ieeexplore.ieee.org/document/8090056

DAILY SABAH. (2019). *Cyberattacks blamed for Sunday's internet disruption across Turkey | Daily Sabah*. https://www.dailysabah.com/turkey/2019/10/28/cyberattacks-blamed-for-sundays-internet-disruption-across-turkey

Das, R., & Gündüz, M. Z. (2019). *Analysis of Cyber-Attacks in IoT-based Critical Infrastructures*.

DemiRol, D., Daş, R., & Baykara, M. (2013). *SQL Enjeksiyon Saldırı Uygulaması ve Güvenlik Önerileri*.

E. Luiijf, I. Žutautaite, and B. M. Hämmerli. (2018). *Critical Information Infrastructures Security: 13th International Conference, CRITIS 2018, Kaunas, Lithuania, September 24-26, 2018, Revised Selected Papers [1st ed.] 978-3-030-05848-7, 978-3-030-05849-4*. Dokumen.Pub. https://dokumen.pub/critical-information-infrastructures-security-13th-international-conference-critis-2018-kaunas-lithuania-september-24-26-2018-revised-selected-papers-1st-ed-978-3-030-05848-7-978-3-030-05849-4.html

Ericsson, 2020. (n.d.). *The Internet of Things (IoT) technology*. Retrieved 4 October 2023, from https://www.ericsson.com/en/internet-of-things

Google Forms. (2023). In *Wikipedia*. https://en.wikipedia.org/w/index.php?title=Google_Forms&oldid=1178230779

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. https://doi.org/10.1016/j.future.2013.01.010

Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., & Sikdar, B. (2019). *A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures* [Review]. Scopus OA2019; Institute of Electrical and Electronics Engineers Inc. https://scholarbank.nus.edu.sg/handle/10635/210052

Heath Muchena. (2019, November 13). *African CIOs look to IoT for critical infrastructure applications*. CIO. https://www.cio.com/article/215734/african-cios-look-to-iot-for-critical-infrastructure-applications.html

ISACA. (2019). *Security Issues in IoT: Challenges and Countermeasures*. ISACA. https://www.isaca.org/resources/isaca-journal/issues/2019/volume-1/security-issues-in-iot-challenges-and-countermeasures

J. P. Shim. (2019). *Kinetic Threats and IoT Cybersecurity Cyber-physical Systems and Industrial IoT Cybersecurity: Issues and Solutions Emergent Research Forum (ERF) Paper*. ResearchGate. https://www.researchgate.net/publication/344889050_Kinetic_Threats_and_IoT_Cybersecurity_Cyber-physical_Systems_and_Industrial_IoT_Cybersecurity_Issues_and_Solutions_Emergent_Research_Forum_ERF_Paper

J. Wilkins. (2019). *Key Steps to Safeguard Industrial Environments from Cyber Threats*. https://trout.software/blog/10-steps-to-protect-industrial-environments-from-cyber-threats

Kimani, K., Oduol, V., & Langat, K. (2019a). Cyber security challenges for IoT-based smart grid networks. *International Journal of Critical Infrastructure Protection*, *25*, 36–49. https://doi.org/10.1016/j.ijcip.2019.01.001

Kimani, K., Oduol, V., & Langat, K. (2019b). Cyber security challenges for IoT-based smart grid networks. *International Journal of Critical Infrastructure Protection*, *25*, 36–49. https://doi.org/10.1016/j.ijcip.2019.01.001

Kimani, K., Oduol, V., & Langat, K. (2019c). Cyber security challenges for IoT-based smart grid networks. *International Journal of Critical Infrastructure Protection*, *25*(C), 36–49.

Liu, X., Qian, C., Hatcher, W. G., Xu, H., Liao, W., & Yu, W. (2019). Secure Internet of Things (IoT)-Based Smart-World Critical Infrastructures: Survey, Case Study and Research Opportunities. *IEEE Access*, *7*, 79523–79544. https://doi.org/10.1109/ACCESS.2019.2920763

M. Li, W. Huang, Y. Wang, W. Fan, and J. Li. (2016). *The study of APT attack stage model*. ResearchGate. https://www.researchgate.net/publication/306925657_The_study_of_APT_attack_stage_model

Mansha Kapoor. (2023, August 11). *IoT in Transportation: The Role of IoT Solutions in Transforming Mobility | CognitiveClouds Blog*. https://www.cognitiveclouds.com/insights/iot-in-transportation

Maple, C. (2017). Security and privacy in the internet of things. *Journal of Cyber Policy*, *2*(2), 155–184. https://doi.org/10.1080/23738871.2017.1366536

Mercan, S., Akkaya, K., Cain, L., & Thomas, J. (2020). *Security, Privacy and Ethical Concerns of IoT Implementations in Hospitality Domain* (No. arXiv:2009.10187). arXiv. http://arxiv.org/abs/2009.10187

Mezam. (2024). Mapcarta. https://mapcarta.com/16799338

Microsoft Windows 10 Pro. (n.d.). StackSocial. Retrieved 4 October 2023, from https://www.stacksocial.com/sales/stacksocial.com/sales/microsoft-windows-10-pro

Miller, B., & Rowe, D. (2012). A survey SCADA of and critical infrastructure incidents. *Proceedings of the 1st Annual Conference on Research in Information Technology*, 51–56. https://doi.org/10.1145/2380790.2380805

Moffa, A. (2024). *Implementing Zero-trust to IoT Solutions.* Retrieved on https://www.ptc.com/en/

Paré, G., & Kitsiou, S. (2017). Chapter 9 Methods for Literature Reviews. In *Handbook of eHealth Evaluation: An Evidence-based Approach [Internet]*. University of Victoria. https://www.ncbi.nlm.nih.gov/books/NBK481583/

R. Da¸s, A. Karabade, and G. Tuna. (2015). *Common network attack types and defense mechanisms,*. https://www.researchgate.net/publication/350374715_Analysis_of_cyber-attacks_in_IoT-based_critical_infrastructures

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. https://doi.org/10.1016/j.comnet.2012.12.018

Sánchez, H. S., Rotondo, D., Escobet, T., Puig, V., & Quevedo, J. (2019). Bibliographical review on cyber attacks from a control oriented perspective. *Annual Reviews in Control*, *48*, 103–128. https://doi.org/10.1016/j.arcontrol.2019.08.002

Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. (2020). Cybersecurity data science: An overview from machine learning perspective. *Journal of Big Data*, *7*(1), 41. https://doi.org/10.1186/s40537-020-00318-5

Sean, L. (2020). *Taiwan's state-owned company CPC Corp. Suffers ransomware attack—CyberScoop*. https://cyberscoop.com/cpc-corp-ransomware-attack-taiwan-trend-micro/

Segovia, M., Cavalli, A., Cuppens-Boulahia, N., & Garcia-Alfaro, J. (2019). *A Study on Mitigation Techniques for SCADA-Driven Cyber-Physical Systems (Position Paper)* (pp. 257–264). https://doi.org/10.1007/978-3-030-18419-3_17

Ślusarczyk, B. (2018). INDUSTRY 4.0-ARE WE READY? *Polish Journal of Management Studies*, *17*. https://doi.org/10.17512/pjms.2018.17.1.19

SPSS. (2023). In *Wikipedia*. https://en.wikipedia.org/w/index.php?title=SPSS&oldid=1171239082

Stouffer, K. (2023). *Guide to Operational Technology (OT) Security* (No. NIST SP 800-82r3; p. NIST SP 800-82r3). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-82r3

Tahiru, A. (2018). *CYBERSECURITY IN AFRICA: THE THREATS AND CHALLANGES*. *3*(5).

Tariq, N., Khan, F. A., & Asim, M. (2021). Security Challenges and Requirements for Smart Internet of Things Applications: A Comprehensive Analysis. *Procedia Comput. Sci.*, *191*(C), 425–430. https://doi.org/10.1016/j.procs.2021.07.053

Team, T. (2021, October 21). *How IoT Works?* TechVidvan. https://techvidvan.com/tutorials/how-iot-works/

Thales. (2022). *Top IoT security issues and challenges (2022) – Thales*. https://www.thalesgroup.com/en/markets/digital-identity-and-security/iot/magazine/internet-threats

Thomas Brinkhoff. (2017). *Mfoundi (Department, Cameroon)—Population Statistics, Charts, Map and Location*. https://www.citypopulation.de/en/cameroon/admin/0207__mfoundi/

Tracey, T. (2024, January 3). *Phishing Attacks: A Recent Comprehensive Study and a New Anatomy*. CybSafe. https://www.cybsafe.com/research-library/phishing-attacks-a-comprehensive-study/

Ugur, N. G., & Barutcu, M. T. (2018). *A Critical Analysis on Internet of Things: Features and Vulnerabilities*.

wang wei. (2018). *Casino Gets Hacked Through Its Internet-Connected Fish Tank Thermometer*. The Hacker News. https://thehackernews.com/2018/04/iot-hacking-thermometer.html

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

Wells, L. J., Camelio, J. A., Williams, C. B., & White, J. (2014). Cyber-physical security challenges in manufacturing systems. *Manufacturing Letters*, *2*(2), 74–77. https://doi.org/10.1016/j.mfglet.2014.01.005

Zhang, X., Upton, O., Beebe, N. L., & Choo, K.-K. R. (2020). IoT Botnet Forensics: A Comprehensive Digital Forensic Case Study on Mirai Botnet Servers. *Forensic Science International: Digital Investigation*, *32*, 300926. https://doi.org/10.1016/j.fsidi.2020.300926

License