Application of Blockchain in Managing Security Challenges Confronting the Adoption of Fourth Industrial Revolution Technologies in Smart Environments: The Case of a Multi-Hazard Early Warning System

by

MANEO NTSELISENG RAMAHLOSI

Submitted in fulfilment of the requirements for the degree

MASTER'S

IN INFORMATION TECHNOLOGY

In the

Faculty of Engineering, Built Environment and Information Technology:

Department of Information Technology

Central University of Technology, Free State

Supervisor: Dr. Adeyinka Akanbi

Co-Supervisor: Prof. Muthoni Masinde

2024

Copyright Notice

Disclaimer

This dissertation includes coloured figures that graphically explain the conclusions in a comprehensible manner. For best results, it is recommended that this dissertation be printed in colour, although printing it in black and white; grayscale, is an option.

Dedication

This dissertation is dedicated to my family, friends, and Central University of Technology.

Declaration

I, Maneo Ntseliseng Ramahlosi hereby declare that this dissertation is a presentation of my original work that has never been presented at any other university for the award of any qualification. I declare that all information gathered from other authors has been plainly acknowledged with citations and references of their work.

The completion of this dissertation was possible through the supervision of Dr. Adeyinka Akanbi, and co-supervised by Professor Muthoni Masinde from the Department of Information Technology at Central University of Technology, Free State, South Africa.

Maneo Ntseliseng Ramahlosi

Signature: _____

Date: 15th September 2024

As supervisors of this dissertation, we attest that the claims above are accurate to the best of our knowledge.

Doctor Adeyinka Akanbi

Signature: _____

Date: _____

Professor Muthoni Masinde

Signature: _____

Date: _____

Preface and Acknowledgements

This dissertation is the result of a Master's research study carried out from February 2020 to May 2024 at the Department of Information Technology, Faculty of Engineering, Built Environment and Information Technology, Central University of Technology, Free State, South Africa.

I would start praising and giving thanks to the Almighty God for bestowing upon me the patience, strength, and wisdom that enabled me to complete this research, the journey was long and hard, but by His grace, I was able to conquer it.

I would also like to express my genuine gratitude to the people mentioned below for their major involvement towards the completion of this research.

To my supervisors, Dr. Adeyinka Akanbi and Prof Muthoni Masinde, I would like to thank you for your continuous encouragement, guidance, support, and for never giving up on me throughout this long journey. Words fail me in extending the amount of gratitude I have. I have attained financial assistance during my research journey, attended numerous trainings, presented in seminars and conferences; and I was able to publish articles all because of your advice and guidance. Thank you for the significant roles you each played in order for me to attain my master's degree. Your constant assistance has been pivotal to the completion my research.

I would also like to extend a vote of thanks to the Central University of Technology (CUT), Free State for providing me with financial aid to cover all the costs relating to my study, and training that equipped me with the necessary skill.

I also wish to thank my colleagues who always lend me an ear during difficult times, and sharing sound research ideas together to ensure earlier completion of mine. Your motivation and support have not gone unnoticed. Mme Mbele, it would be unjust for me not to mention you, I called you at awkward times while I struggled and needed motivation, you never complained but always listened and offered advice and guidance. Tholoana Motaung, we embarked on this journey together, we laughed, cried, almost gave up; but with the encouragement we gave each other, we came out victorious. Ntate Mokone, thank you for your constant support and motivation throughout this study. Whenever things fell apart, I would call

you and go extra length to assist; for that, I thank you. I would also like to send my appreciation to Mr. Yolo Madani, who together we started this journey, and you made sure that we conclude and celebrate together. Your efforts have not gone unnoticed; thank you.

I would like to appreciate my family, starting from my father Maieane Makalo Khaketla, for your love, and for having you to call for assistance, and for rendering the assistance countless times. My mother, Machobane Khaketla, words fail me in expressing the amount of gratitude I have. Your prayers, support, and encouragement gave me the strength I needed most during this journey. To my sisters, Matoli Khaketla and Sekamotho Maitsi; thank you for your constant support and patience with me. To my children, Chobane, Pheello, and Mathabo, you were without your mom most nights when I had deadlines to meet, and you never complained. You supported me throughout, and for that, I am grateful. Chobane, the significant role and guidance you gave is the main success of this research, thank you very much.

Lastly, I would like to send my heartfelt gratitude to my husband. I was able to embark on this journey because of your support and patience; thank you.

Maneo Ntseliseng Ramahlosi

September 2024

Bloemfontein, Free State

South Africa

Abstract

Gaining access to data, both personal and public, has become a source of worry in our digital age, as it poses some security and privacy challenges. This raised consciousness is applicable to all digital applications as well as information systems. Intentions of hacking and violations of privacy have been proven to be a major concern, which has led to digital trust issues. Similarly, this notion is true in smart environments, where datasets that have been recorded and collected are used as inputs for monitoring systems and forecasts, which in turn must adhere to several rules due to the sensitive nature of the predictions. Progression in technology over the years has resulted in geometric enhancements in relation to expertise of monitoring devices and downsizing of devices, encouraging the transition from commonly utilised outdated systems to Internet of Things (IoT) smart devices. In an atmosphere where there is an augmentation of cyber security threats, updating legacy systems is also a great concern. These legacy systems have proven to possess characteristics that pose security vulnerabilities, and they are usually incompatible with current security features, and they also lack sufficient encryption methods. As a result of this shift in paradigms to the IoT age, more attention has been given to integrating various devices, guaranteeing technology compatibility and interoperability, and making the devices smaller over tackling security flaws of the endpoint solutions (. Therefore, even with the adoption and deployment of the Fourth Industrial Revolution (4IR) technology, security issues still exist. As a case study, a smart environment network of an Early Warning System (EWSs) in a Multi-Hazard Early Warning System (MHEWSs) is not an exception, as it is also susceptible to vulnerabilities; security of data and data pipelines is crucial, and it remains the focus of this study. Its importance is heightened by the integration of 4IR technology and the amalgamation of heterogeneous devices and systems. The objective of this study is to investigate how security issues that afflict smart environments, and consequently, a MHEWSs may be managed and eased by the implementation of Blockchain technology and solutions. This research was carried out with the hypothesis that

the implementing Blockchain technology on the MHEWSs will protect the data pipeline. The hypothesis proved to be true as the researcher was able to prove that Blockchain technology can be used to protect the data pipeline of a MHEWS.

List of Acronyms

AEMS - Adaptive Environmental Management System

AI- Artificial Intelligence

APT - Advanced Package Tool

EWS – Early Warning System

EWSs – Early Warning Systems

CAN bus - The Controller Area Network

CA - Certificate Authorities

CI/CD - Continuous Integration and Continuous Delivery

DIT - Diffusion of Innovation Theory

DLT- Distributed Ledger Technology

4IR – Fourth Industrial Revolution

IBM - International Business Machines Corporation

ICMEWS - Integrated Climate-Driven Multihazard Early Warning System

IoT – Internet of Things

IOTWS- Indian Ocean Tsunami Warning and Mitigation System

ITIKI – Information Technology with Indigenous Knowledge

JSON-LD – JSON for Linked Data

KVM - Kernel-based Virtual Machine

ML – Machine Learning

MHEWS – Multi-Hazard Early Warning System

MHEWSs – Multi-Hazard Early Warning Systems

NB-IoT - Narrowband-Internet of Things

NMHSs- National Meteorological and Hydrological Services

RFID - Radio Frequency Identification

Sub-Saharan Africa (SSA)

SDK – Software Development Kit

TAM - Technologies Acceptance Model

UTAUT - Unified Theory of Acceptance and Use of Technology

WMO - World Metrological Organisation

WSN - Wireless Sensor Networks

QEMU - Quick Emulator

Glossary

- *Artificial intelligence* – This is a technology that can accomplish tasks in a way that resembles human intellectual ability and can continually refine itself based on the data it collects
- *Blockchain technology* – Blockchain is a decentralised peer-to-peer ledger system that ensures the transparency and immutability of digital asset records, eliminating the need for a third-party intermediary. This innovative technology is attracting significant attention due to its transformative potential and because of its ability to reduce security challenges confronting the adoption of Fourth Industrial Revolution (4IR) technologies in smart environments.
- *Cyber threats* - This refers to a devious attempt to attack or disrupt a computer network or system with the goal of intruding or stealing information.
- *Cyber infrastructure* - It contains software applications, data storage systems, advanced devices and data repositories, visualisation climates, and people, all of which are linked together by firmware and high-performance networks to improve the quality of the research and enable new discoveries that would not have been possible otherwise.
- *Disaster* – is a significant occurrence that takes place either over an extended or brief amount of time and resulting in pervasive human, material, financial, or environmental loss that surpasses the affected society's or society's ability to manage its own resource base. This affects the environment and is mainly attributed by human activity.
- *Early Warning System (EWS)* – This is a set of technologies, guidelines, and procedures for predicting and mitigating the consequences of natural and human-caused disasters, as well as other occurrences
- *Fourth Industrial Revolution (4IR)* – This implies an amalgam of artificial intelligence (AI), robotics, the Internet of Things (IoT), genetic modification, quantum computing, and other technologies.
- *Internet of Things (IoT)* – It can be described as an internetworking of physical devices that connect and transmit information using sensors and APIs.
- *Multi-Hazard Early Warning System* (*MHEW)* – This is a technology that can warn of numerous hazards before their occurrence, enhancing the efficiency and reliability of warnings through synchronised and interoperable mechanisms and proficiencies, and

involves a holistic integration of systems for up-to-date and precise hazards information.

- *Smart environment* -This is defined as a small community in which various types of smart devices are constantly attempting to create the lives of its residents more convenient. By substituting hazardous tasks, heavy work, and repetitive tasks with computer-controlled agents, smart surroundings aim to improve the experience of people from all walks of life.

Table of Contents

List of Figures

List of Publications

This dissertation resulted in the publication of 2 papers. Below is the list of the published papers.

i. Ramahlosi, M. N., Madani, Y., & Akanbi, A. (2023). A Blockchain-based Model for Securing Data Pipeline in a Heterogeneous Information System. *South African Institute of Computer Scientists & In-Formation Technologists*, 167–179

ii. Ramahlosi, M. N., & Akanbi, A. (2024). Application of Blockchain in Managing Security Challenges Confronting the Adoption of 4IR in Smart Environments. *Advances in Artificial Intelligence and Machine Learning, 04(02),* 2276–2289. https://doi.org/10.54364/aaiml.2024.42131

CHAPTER ONE

INTRODUCTION

1.1 Background Information and Motivation

The availability, and accessibility of both public and personal data in todays' era have become an issue of concern due of the constant fear of privacy and security vulnerabilities. This increased concern is particularly important and valid for any kind of digital platforms, applications, and information systems. Information assurance in such systems must be implemented in every single aspect. Whether it is protecting sensitive information, conducting secure transactions, or preserving individual identities; a higher level of scrutiny is paramount. Due to the asynchronous nature of cyberspace, along with the potential for defamation and data breaches, this concern extends not only to those involved in development but also to the management and use of digital technologies.

Therefore, it is necessary to take measures to guarantee proper security solutions and policies in order to protect these systems from advanced threats. Vigilance must be increased in all areas of digital infrastructure, including but not limited to handling sensitive data, preserving personal information, and safeguarding online transactions. For anybody involved in creating, overseeing, or using digital technology, this concern is especially important given the prevalence of cyber threats, data breaches, and privacy concerns. Therefore, maintaining strong security policies and procedures is essential to protecting these systems from ever-changing threats. Some of the major concerns regarding digital trust are the violations on private information, and the increasing rates of incidences of hacking intentions that have been reported.

These issues are especially evident in the field of smart environments, where datasets that have been recorded or collected are used as inputs for monitoring and prediction systems, and because the forecasts are sensitive, they must adhere to several rules. Technology progression that has occurred over time has also resulted in a geometric improvement in the capability and compactness of monitoring systems (Li et al., 2021), and thereby fuelling the move from widely existing legacy systems to the IoT smart devices.

Updating legacy systems in the era of growing cyber perils is a constant worry (Scarfò, 2018). These systems typically have underlying security flaws and they are frequently incompatible with security measures and they do not have adequate encryption techniques. As the IoT era emerges, the emphasis has shifted toward integrating devices, ensuring technology interoperability, and enhancing device miniaturisation and ubiquity, while less attention is given to addressing the security vulnerabilities of endpoint solutions, (Akanbi and Masinde, 2015). As a result, the security challenges persist despite the adoption and implementation of 4IR technologies.

As a case study, a smart environment network of an Early Warning System (EWS) in a Multi-Hazard Early Warning System (MHEWS) is viewed like other digital applications and information systems. This is so because these systems have adopted 4IR technologies, and they are made up of an integration of heterogeneous devices and systems, which leads to security concerns of the data and mainly, the data pipelines. The issue of securing the data pipeline is critical, and it is the crux of this research. This study investigates whether Blockchain technology can be implemented in a MHEWSs to lessen the security issues that arise when 4IR technologies are adopted in smart settings. It also hypothesis that the integration of Blockchain-based solutions will address issues of securing the data pipeline of a MHEWSs.

1.2 Problem Statement

Ensuring that data is confidential and secured is a major challenge in the modern computer age. In MHEWSs, the flow of data packets from the sensors to the repository and processing unit through the communication medium poses a considerable number of risks and concerns to possible denial and manipulation of the data. These challenges are associated with every digital transmission on a wired and wireless network. The localisation of a smart environment of an EWS from attacks and encryption of data packets lacks robust mechanisms to address the problem in a MHEWS due to the complexities caused by the integration of several EWSs in a MHEWS. Resultantly, the system lacks proper security measures and remains openly accessible, making it vulnerable to digital attacks. It therefore becomes imperative to explore the application of Blockchain technology as a possible solution to create a sustainable information security framework to effectively protect these interconnected systems.

1.3 Research Aim and Objectives

This research is aimed at assessing the application of Blockchain technology in managing the security challenges of 4IR technologies adoption in an integrated MHEWS. Below is the list of research questions which were taken into consideration in order to address the aforementioned research concerns in the current study.

a) **RQ1:** What are the security challenges and vulnerabilities that arise from the adoption of 4IR technologies in a MHEWS?

b) **RQ2:** How can a secure data pipeline framework be developed for MHEWSs using Blockchain technology to secure data transmission from the sensing devices to the repository and processing unit?

c) **RQ3:** To what extent does the application of Blockchain technology in preventing the security vulnerabilities associated with 4IR technologies in a MHEWS efficient?

The specific objectives of this research project are to:

a) **RO1:** Identify security challenges and vulnerabilities from the adoption of 4IR technologies in a MHEWS in the form of risk assessment.

b) **RO2:** Develop a secure data pipeline framework for MHEWS using Blockchain technology to secure data transmission from the sensing devices to the repository or processing unit.

c) **RO3:** Test and evaluate the extent to which the application of Blockchain technology is efficient in preventing the security vulnerabilities associated with 4IR technologies in a MHEWS.

1.4 Limitation of the Research Scope

This research mainly focused on MHEWSs in the environmental monitoring domain. This work did not explore the implications of the proposed solution based on the difficulties associated with scalability of the adopted frameworks.

1.5 Significance and Contributions of the Study

The significance and contributions of this study cannot be overemphasised. First, it explores crucial aspects of deploying modern technology in delicate, complex and critical contexts. It also examines Blockchain's potential to secure 4IR technologies, which can provide creative ways to ensure data integrity, guaranteed transparency, and means to prohibit unauthorised access to data. All of the above are critical for systems such as the one in discussion. Additionally, the integration of 4IR technologies into critical infrastructures such as MHEWSs necessitates the protection of systems against cyber-attacks that might have dire repercussions for the environment, society, and economy.

Furthermore, the implementation of Blockchain in MHEWSs has the potential of increasing trust and dependability by guaranteeing that warning data and communications are unchangeable and verifiable, lowering the possibility of false alarms, and improving the credibility of warnings. EWSs have the potential to save lives and minimise financial losses in emergency and catastrophe scenarios, and it is therefore vital to augment trust in them to ensuring trust, and reliability.

1.6 Structure of the Dissertation

The dissertation is divided into five chapters, which are as follows.

a) **Chapter One: Introduction**

This chapter provides background information relating to study and outlines the research questions and objectives.

b) **Chapter Two: Literature Review**

Provides an exhaustive assessment of literature for the evaluation of theories and technology applicable. to this dissertation. It clarifies in detail what Blockchain is, and its use. The chapter also explores 4IR technologies, and security challenges they face.

c) **Chapter Three: Research Methodology and System Design**

Illustrates the methods adopted in carrying out this research. The major goal of this chapter is to clarify the research methodology, and to provide a general overview. of the implementation of Blockchain.

d) **Chapters Four: Results and Analysis**

This chapter outlines the results of the implemented Blockchain, and it also analyses its outcome.

e) **Chapter Five: Summary of Study and Conclusion**

This chapter concludes the dissertation by discussing and evaluating the research against the research objectives.

CHAPTER TWO

BACKGROUND AND RELATED WORK

2.1 Introduction

This chapter extensively reviews recent studies, and it is presented in two sections. The first segment addresses the background, and the second segment is based on theoretical literature review. The background section is further divided into six subsections. The main thrust focuses on security challenges brought forth by the adoption of the 4IR technologies in smart environments. It also discusses different types of hazards, and how MHEWS is used to combat these disasters. It further delves into the composition MHEWS, and then explores the different types of Blockchain technologies and their benefits. The discussion also delves into the proposed implementation of Blockchain technology as a viable solution to mitigate the security challenges associated with MHEWS. This section also explores how Blockchain can enhance data integrity, ensure secure communication, and address vulnerabilities, offering a robust approach to countering potential threats within MHEWSs.

The theoretical literature review focuses on the analysis of recent scholarly work carried out by other researchers in the topic under discussion. An overall conclusion is going to be presented at the end.

2.2 Background

Sub-Saharan Africa (SSA) is currently known for its frequent and severe droughts, which are a key cause of the chronic food insecurity, (Masinde & Bagula, 2011). Presently, there is no commonly recognized definition of drought. Intuitively, however, it can be considered as a long period when the amount of precipitation or the availability of water is clearly lower than average. In most cases, a drought does not have a clear beginning or end point, and it can last from months to several years (Fleming-Muñoz et al., 2023).

EWSs are frequently regarded as one of the most crucial components in lowering the effects and ramifications that dangerous natural catastrophes have on civilisations. Like the other terminologies used to describe catastrophe risk reduction, this idea has developed over time to become a complete framework. International efforts have recently concentrated on a multi-hazard approach, leading to the creation of the so-called MHEWSs, in order to improve the

efficacy of EWSs and strengthen coordination among the numerous agencies involved (Aguirre-Ayerbe et al., 2020).

Different EWSs can be integrated together for a more holistic system which is a MHEWS. This integration necessitates a high degree of standards that must be uniformly implemented across the board. As the number of devices that are connected to the network are huge, this generates a large volume of data that requires processing. Controlling this increase in data volume is essential, particularly when it comes to reducing security concerns like vulnerabilities to the data pipeline such as hacking, malicious codes, worms, viruses, and DoS attacks (Lee et al., 2008). To overcome such obstacles, cutting-edge innovations such as Blockchain technology must be employed to strengthen the security framework, and provide a robust environment for data management in this networked world, (Rifi et al., 2017).

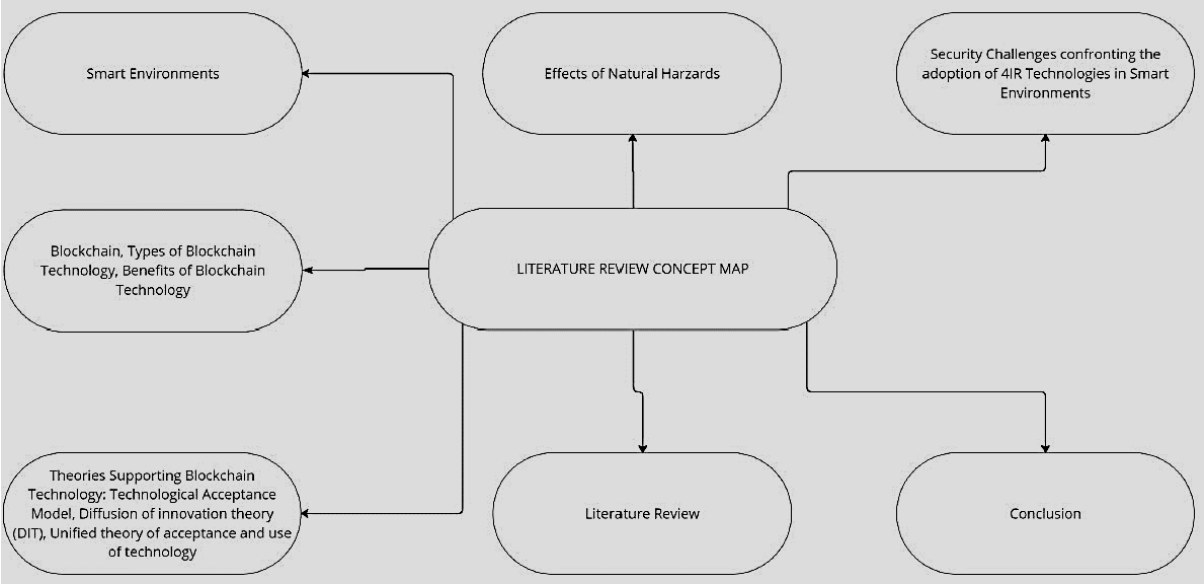

Figure 2.1: Chapter Concept Map, (: Ramahlosi, 2023)

2.3 Effects of Natural Hazards

This segment seeks to present the effects of natural hazards. Natural hazards can lead to data loss or not having enough data information or robust mitigation systems. Natural disasters such as hurricanes, floods, earthquakes, and wildfires can seriously jeopardize many facets of civilization, including information technology and data management. In the context of disaster preparedness and resilience, the effects of these risks on data loss, the sufficiency of accessible data, and the efficacy of mitigation mechanisms are crucial factors to consider. Based on a

research by Croft (2019), the following key aspects: loss of data, insufficient data, and ineffective mitigation systems are discussed below.

2.3.1 Loss of Data

Data Loss: Physical damage to data storage facilities caused by natural disasters like earthquakes, floods, or storms can result in data loss or corruption. This loss can seriously impair the timeliness and accuracy of hazard alarms in smart settings that depend on continuous data streams for EWSs, impeding quick actions, and putting infrastructure and human lives in jeopardy.

2.3.2 Insufficient Data

Inadequate Information: Data gathering methods may be interfered with by natural catastrophes, resulting in information shortages. The EWS's capacity to deliver precise and timely alerts may be hampered by this absence of complete and real-time data. Residents may not get timely or accurate warnings about potential threats from the system if there is insufficient data, which would diminish its dependability and efficacy.

2.3.3 Ineffective Mitigation Systems

Ineffective Mitigation Systems: The effectiveness of mitigation systems that are connected with Blockchain technology may be jeopardised in the absence of sufficient data or as a result of data loss. Accurate and consistent data inputs are necessary for Blockchain to fulfil its promise of providing transparent and unchangeable records for catastrophe management. Incomplete, or inaccurate data might result in poor decision-making, which can lower the efficacy of mitigation strategies used with Blockchain-based systems.

2.4 Early Warning Systems and Natural Hazards

EWSs for natural hazards are usually considered as the main instruments to avoid disasters throughout the world. The Indian Ocean tsunami, which occurred on December 26, 2004, generated renewed interest in the creation of systems that might notify nations to various types of catastrophes that could potentially emerge (Karki, 2019; Wang et al., 2017; Akanbi & Masinde, 2020; Masinde, 2015). The increasingly ubiquitous use of 4IR technologies in today's society autonomous systems represent the future of large-scale EWSs for applications ranging from environmental monitoring to in-situ sensing. EWSs exist for natural, geophysical, biological hazards and many other related risks (Masinde, 2015).

According to statistics that were recorded globally for the past five decades, financial defeats as a result of natural hazards have risen considerably in the past decade. Contrarily, during this same period, statistics relayed about the number of lives lost has declined significantly. This notable decrease is attributed to the introduction of EWSs in perilous countries worldwide. (Pecoraro et al., 2019). According to World Metrological Organisation (WMO), an effective EWS consists of the forecasting systems, communication and dissemination mechanism, risk assessment and information, with preparedness and early responses mechanisms (Luther et al., 2017) as shown in Figure 2.2 below.

Figure 2.2: WMO Schematics of the four operational components of effective EWSS, (Source: Luther et al., 2017)

A catastrophe triggered by a natural hazard can be described as 'a serious disruption of the functioning of a community or a society causing widespread human, material, economic or environmental losses which exceed the ability of the affected community or society to cope using its own resources' (ISDR 2004-http://www.unisdr.org/eng/library/lib-terminology-eng%20home.htm). In the current UN-ISDR terminology, early warning is defined as 'the provision of timely and effective information, through identified institutions, that allows individuals exposed to a hazard to take action to avoid or reduce their risk and prepare for effective response' (ISDR 2005a Disaster statistics 1994–2004).

Meanwhile, typical components of EWSs include sensors, sensing devices, radio satellite, cell phones, data transmission medium, repository/database, and the processing unit as depicted in Figure 2.3. These components are broadly divided into: the data acquisition layer, data transmission layer, and data processing layer.

The communication layer comprises of a physical "wired" or logical "wireless" medium connecting the sensing device to the data repository and processing units. This layer is where the security vulnerability is the highest, and the focus of this study.

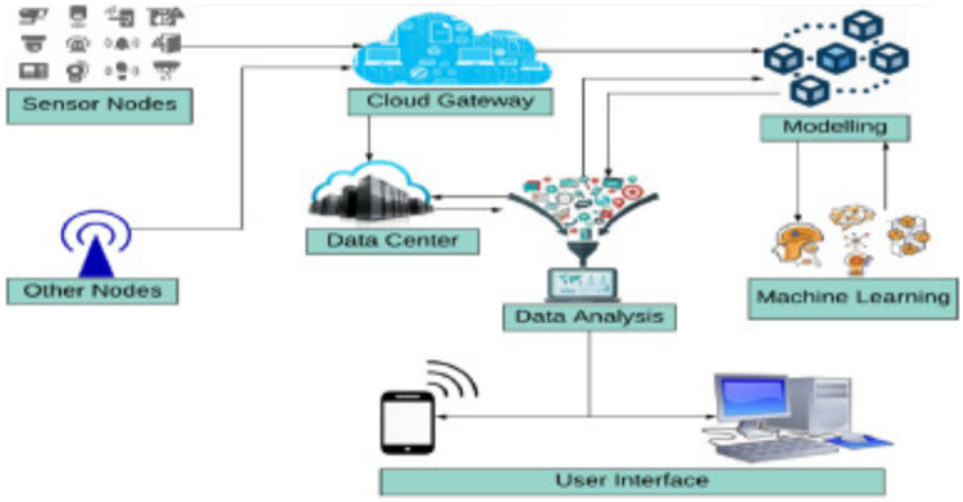

Figure 2.3: Overview of an Early Warning System, (EWS) (Source: Lan et al., 2019)

According to Kumar et al., (2018), there are different types of security that can be implemented on information systems or digital infrastructure. These are: application security, network security, internet security, information security, end-user security, and data security.

This study focuses on mitigating security challenges by improving data security through the use of Blockchain technologies/solutions. Data security means protecting digital data during transmission and use in applications or information systems from negative forces and the undesirable acts of unauthorised users such as a cyber-attack, or a data breach. This is required to satisfy strict security requirements of confidentiality, integrity, authenticity, and availability within the information system.

2.5 Multi-Hazard Early Warning System (MHEWS)

The World Meteorological Organization (WMO) and the National Meteorological and Hydrological Services (NMHSs) have always prioritized disaster risk reduction (Luther et al., 2017). Furthermore, with reference to the Hyogo Framework for Action, 2011; the sixteenth

World Meteorological Congress stressed the relevance of MHEWSs as a proven instrument for natural hazards and disaster prediction (Stanganelli, 2018).

MHEWSs are all-inclusive systems aimed at tracking, identify, and alerting users to a range of threats in a prompt and precise way, therefore averting fatalities and mitigating material and financial loss. A successful MHEWSs consists of a number of essential parts, each of which is essential to the overall effectiveness, and usefulness of the system. These elements frequently work together to ensure a smooth process from danger identification to community response. This involves the combination of several EWSs into an MHEWSs. There are numerous initiatives that exist globally, some of which were established and that begun with testing after the Indian Ocean Tsunami incident in Asia (Luther et al., 2017) to have an Integrated Climate-Driven Multihazard Early Warning System (ICMHEWS). Such initiatives include the establishment of Indian Ocean Tsunami Warning and Mitigation System (IOTWMS) in 2011 (Hettiarachchi, 2018); the establishment of 24 tsunami detection stations in the Indian Ocean, (raising the total number of sea-level gauges from 4 to 100); and extending the number of deep oceans tsunami meters for data exchange. As mentioned before, this study is focused on two EWSs, namely Information Technology with Indigenous Knowledge (ITIKI): bridge between African indigenous knowledge and modern science of drought prediction (Masinde, 2015); and Adaptive Environmental Management System for Lejweleputswa District: A Participatory Approach Through Fuzzy Cognitive Maps (Mbele & Masinde, 2020).

2.6 4IR Technologies

The Fourth Industrial Revolution (4IR) encompasses modern technology, particularly the internet; and it has brought forth significant changes that steer the progression on how we go around living our daily lives, how we perform tasks, and knowledge acquisition (Ashima et al., 2021). According to Figure 2.4, 4IR technology comprises of big data, cloud computing, artificial intelligence, autonomous systems as well as system integration (Strous et al., 2021). These technologies are used in different sectors, and for different purposes. For example, massive datasets from several sources may be analysed by AI and ML algorithms, which can spot patterns and trends that human forecasters would not detect. By using real-time inputs and previous weather data, these systems increase the accuracy of weather forecasts (Reichstein, et. al, 2019). In the health sector, mass production of drugs is possible due to 4IR technology. To add more, 4IR technology is also used by environmentalists in trying to reduce ecological disaster.

Security and data privacy concerns have arguably emerged as one of the foremost challenges in the context of the 4IR, in which technology plays a pivotal role (Manda & Dhaou, 2019). The integration of systems within this revolution necessitates the creation of fresh security features, and protective measures to support swifter and more adaptable collaborative value networks, and intelligent production systems.

Blockchain is the identified 4IR technology that will be applied to address the issues of security arising from the adoption of 4IR in MHEWSs.

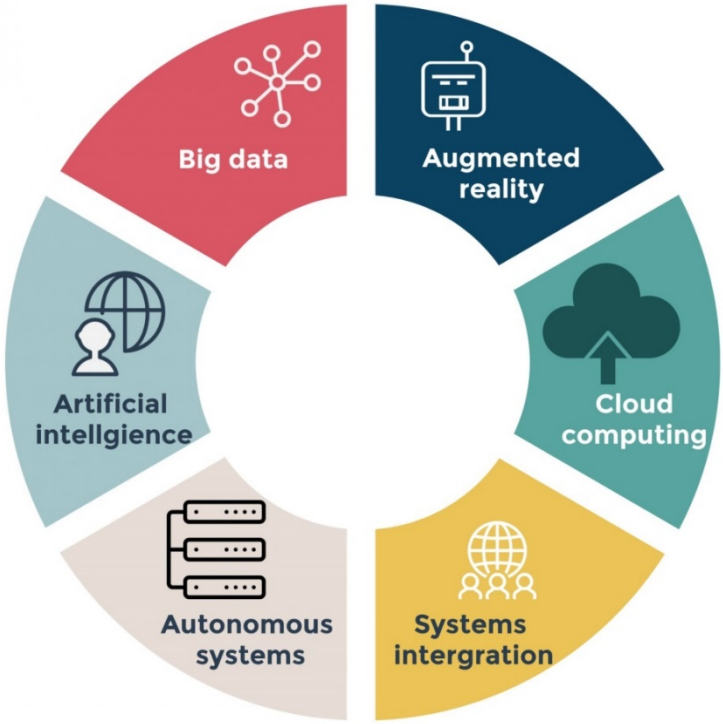

Figure 2.4: 4IR Technology (Source: ViaAfrika, 2020).

2.6.1 Types of 4IR Technologies and their Challenges

4IR technologies exist in diverse forms. This can be in the form of artificial intelligence, internet of things (IoT), big data, Blockchain, cloud and edge computing, robots and co-bots, autonomous vehicles, genomics and gene editing, the 5G network, and quantum computing (Singh et al., 2021). 4IR Technologies serve diverse purposes. This includes providing accurate information for effective decision-making (Lee et al., 2020). For example, due to technology a

community can take precautionary measures before a cyclone approaches. This will therefore help in reducing hazardous events in a community.

2.7 Smart Environment

Smart environments have grown recently as a result of 4IR technologies like the IoT, which enable people to monitor, manage, and better comprehend their surroundings through a variety of widely used networked gadgets (Ullo &Sinha, 2020). In smart environment applications and modern EWSs, IoT is employed to build a comprehensive, multi-level, and fully covered ecological monitoring network, which can be achieved using the integration of sensors and devices at all levels.

The data from leveraging IoT with spatial and temporal information and constructing a massive platform with a data centre and unified service support (Ullo & Sinha, 2020). Although significant progress has been achieved in 4IR technologies for smart-environmental applications, it can still be a challenging task to secure the data transmission pipelines and the overall systems to analyse the vast volumes of data computational intelligence techniques.

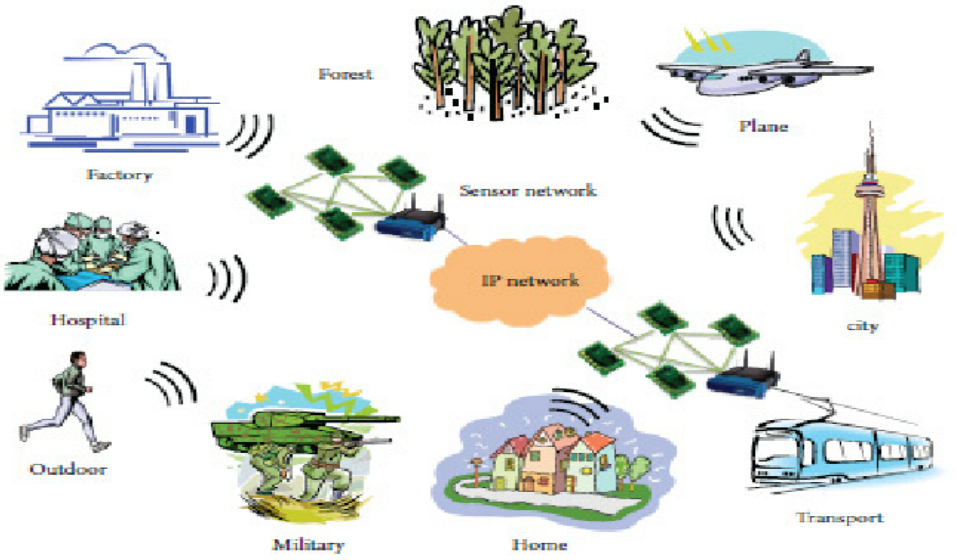

Figure 2-5: Smart environment topology (Source: Aletà, Alonso & Ruiz2017).

In this era, Mentsiev et al. (2020) suggest that contemporary farmers have access to a range of agricultural technologies, including:

- Sensors for monitoring temperature, humidity, light, water, and soil conditions;
- Customised software solutions designed to assist specific types of farms through IoT platforms;
- Artificial Intelligence applications, encompassing processing facilities, autonomous tractors, and robotic farm management;
- Location-based technologies like satellite, GPS monitoring, and data recording; and
- Data analytics tools that employ data pipelining solutions for data streaming and individualised analytics.

By utilising the devices, connections, equipment, and sensors mentioned above; farmers are informed timeously of any change in the environment that require urgent attention, and are able to act accordingly. This enables them to formulate strategic plans for the improvement of individual crops or the entire farm. The interconnection of these smart devices, and sensors, coupled with data-driven processes, enhances farm efficiency, marking a significant benefit derived from IoT (Mentsiev et al., 2020).

2.8 Security Challenges in Adopting 4IR Technologies

This section is based on the analysis of security vulnerabilities that are emanating from the adoption of 4IR technologies into smart environments. The 4IR, marked by the convergence of technologies that is erasing the boundaries between the physical, biological, and technological realms, and it has ushered in a set of both prospects and challenges (Xu et al., 2018). The 4IR has introduced fresh innovations and transformations that have led to emerging challenges, including concerns about security, trust, liability, and the privacy of personal data (Zhou et al., 2015). These issues underscore the need for more stringent regulations.

The IoT has achieved notable success across various domains, including business, healthcare, defence, smart environment (Mentsiev et al., 2020). The authors further state that, in order to grasp the intricacies of applying IoT in smart environment, one must first gain a comprehensive understanding of the IoT framework. Following a meticulous examination of the IoT structure and hands-on practical experience, a secure architecture consisting of a five-tier IoT model was introduced. These five layers have been thoroughly deliberated upon with agricultural experts, and they have garnered unanimous acceptance as outlined below.

- Perception layer is the first layer of discussion. Within this stratum, the integration of various devices including RFID tags, readers, Wireless Sensor Networks (WSN), agricultural machinery, terminal devices, and an array of other sensors is pivotal. Among these sensors, one can find those specifically designed for agriculture, sensors capturing data on plant and animal life, environmental sensors, climatic sensors, and temperature sensors. These sensors play a crucial role in acquiring essential information, encompassing vital indicators of plant and animal health, the presence of insect pests, plant diseases, wind speed, humidity, and temperature. This data is recorded and collected, serving as the initial step for further action. The embedded system thereafter processes, and subsequently uploads this data for additional procedures and evaluations as it traverses through the network layer to reach higher levels.
- Following is the network layer, which serves as the backbone of the IoT infrastructure because it amalgamates various communication networks, and the internet. It facilitates communication through wireless technologies like NB-IoT, LoRa, Bluetooth, Zigbee as well as wired tools such as RS485 and CAN bus. Its primary function is to transmit control instructions from the application layer to agricultural devices in the perception layer, enabling these sensors to take appropriate actions. Additionally, it is responsible for the exchange of agricultural data collected by the perception layer with higher-level layers. However, the IoT presents challenges due to device incompatibility stemming from differences in communication modules, power supply, and processors, leading to issues such as diversity and heterogeneity.
- The middleware layer resolves the challenges presented by collecting, combining, filtering, and analysing data from IoT devices. This streamlines the analysis process, reducing costs and saving time. It also provides developers with a more flexible approach to creating devices and applications. The middleware layer simplifies the operation of new agricultural devices and the development of services, enabling rapid integration with existing infrastructure. This, in turn, enhances the overall connectivity and performance of the Internet of Things.
- Lastly is the common platform layer. This later comprises of machine learning algorithms, Big Data, Edge computing, fog computing, cloud computing, and related application technologies as well as its constructed models. It is responsible for handling agricultural data, including statistics, storage, decision-making, and the development of

specialised algorithms and models for agricultural purposes. These models enable functions such as prediction, early warning, diagnostic reasoning, intelligent decision-making, and intelligent control in the realm of agricultural production.

2.8.1 Data Breach

The adoption of 4IR continues to be hampered by hacking. Hacking is the term used to describe activities aimed at compromising digital technology such as laptops, smartphones, tablets, and even corporate networks (Tsuchiya & Hiramoto, 2021). As the technological world changes, hackers also maximise the benefits of the changes in the digital era. Without resorting to physical force, attackers can still cause harm or disruption to physical infrastructure by breaching into the digital systems of smart environments that oversee physical operations, which may cause damage to specialised machinery, and stopping of essential services (Lehto, 2022).

2.8.2 Increased Cybercrime

Cybercrime can be explained as the use of a computer to achieve criminal goals such as fraudulent activity, embezzling identities, or invading privacy (Okutan & Çebi, 2019). This affects the smart environment at large as such criminal activity effect is illegal, and it has far ruinous effects. The adoption of the 4IR therefore comes with benefits such as increased efficiency, automation but cyber-crime costs are real too. Globally, South Africa is in the third position as far as cybercrime is concerned. A total loss of over R2.2 billion is recorded annually in South Africa, and this emanates from cybercrime (Mzekandaba, 2022).

2.8.3 Loss of Data

There is a huge risk of loss of information when cybercrime, or hacking activities are done. Companies, or organisations that have adopted the 4IR are prone to loss of confidential information. To address this menace, South Africa introduced the data privacy law. This law is called the Protection of Personal Information Act, 2013 (Republic of South Africa, 2021). As such, any violation of this law may expose organisations or companies to lawsuits.

2.8.4 Loss in Digital Rights

Digital rights refer to an individual's civil rights to connectivity, create, use, and publish digital media as well as to use and access computers, other digital devices, and network technologies (Garcia-Teruel & Simón-Moreno, 2021). Due to hacking and cybercrime, many individuals, and corporate organisations lose their digital rights.

2.9 Blockchain

Since its introduction, Blockchain has been associated with cryptocurrencies; nonetheless, recently, it was noticeable that a number of industries have accepted it because its main goal is to increase security. Beyond its use in banking, Blockchain technology is significant because it may provide safe, and immutable records that are distributed via a computer network (Nakamoto, 2008). Since data is visible and unchangeable thanks to decentralised ledger technology, security is enhanced by design (Swan, 2015). In the simplest of terms, Blockchain is referred to as an immutable digital ledger system (Котлер, 2008). Importantly, the Blockchain revolutionises the creation of both scalable information technology systems, and diversified applications by integrating the increasingly popular artificial intelligence, cloud computing, and big data (Zheng et al.,2017). Blockchain is an emerging paradigm that brings together originality and innovation in computer technology. These include distributed data storage, autonomous and decentralized peer-to-peer transactions, programmable smart contracts, and dynamic security encryption algorithms (Zheng, Xie, Dai, Chen & Wang, 2017). One important feature of Blockchain technology is security and this security is in the form of secured data sets.

Historically, Blockchain blueprint code was originally published in a whitepaper by Satoshi Nakamoto on 31 October, 2008 (Nakamoto, 2008). A Blockchain creates a continuous and irreversible chain of data by cryptographically connecting each block of data to the one before it. Without agreement from most network users, this relationship makes changing, or tampering with information extremely difficult, if not virtually impossible (Tapscott & Tapscott, 2016).

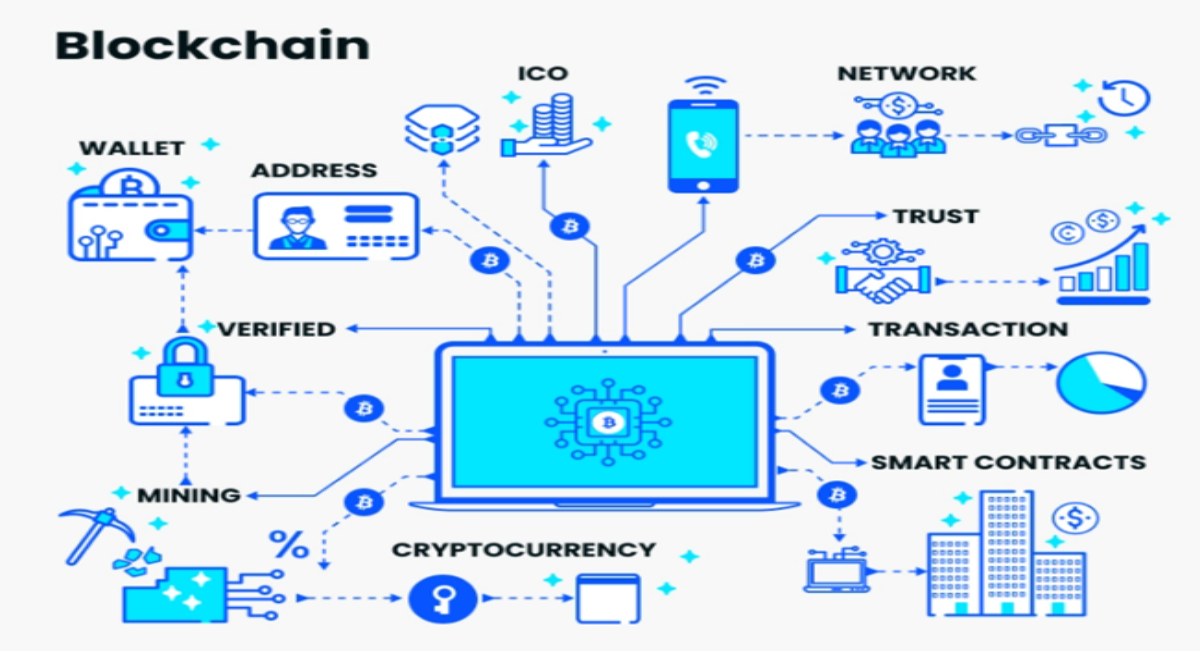

Figure 2.6: Blockchain Infrastructural Architecture (Source: Rifi et al., 2017)

It is further alluded by Zheng et al. (2017) that data structures produced by Blockchain technology show qualities that are inherent with security. Blockchain technology centres its principles on cryptography, decentralisation, and consensus. These principles ensure trust in transactions. Data collection, validation, and manipulation are mainly processed within data and network layers. Most Blockchain, or distributed ledger technologies (DLT) organize data into blocks, with each block containing a transaction, or a bundle of transactions.

As a new block is created, it connects to all the previous blocks that came before it in a cryptographic chain. This occurs in a way that it is almost impossible to manipulate. Each time a transaction occurs within the blocks, the transaction is validated and agreed upon by all blocks using a consensus mechanism that ensures that each transaction is true and correct (Zheng et al., 2017). The evolution of Blockchain has made it out to be one of the safest ways to carry out transactions over a digital network domain. As designed and intended, the technology has been credited for its information integrity assurance, hence, mitigating against any security challenges in the cyber sphere.

2.9.1 Types of Blockchain Technologies

This section seeks to present the various types of Blockchain technology. These are: public Blockchain, and private Blockchain.

2.9.1.1 Private Blockchain

A private Blockchain comes with certain restrictions, and in particular, the company that has rights is only the organisation that can record or perform a function (Robinson, Ramesh, & Johnson, 2021). Multi-chain and hype-ledgers are some of the private Blockchain technology (Reddy et al., 2021). The figure below shows the attributes of a private Blockchain.

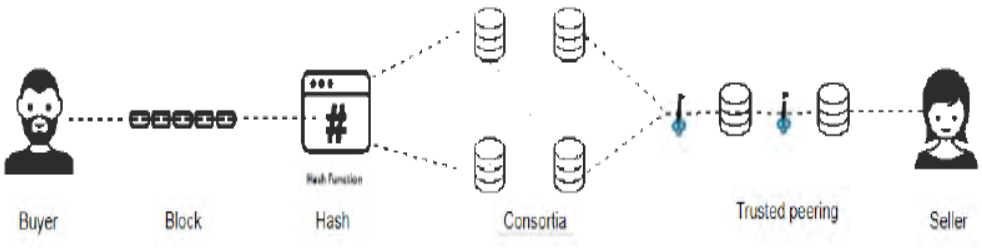

Figure 2.7: Private Blockchain (Source: SteemKr, 2017).

On a private Blockchain, it should be noted that the capacity and ability to read can be restricted or open to the public to some extent (Singh et al., 2021).

2.9.1.2 Public Blockchain

A public Blockchain enables anyone who is part of the network to have access to the data of the system (Wang & Wang, 2022). Some of the key activities that one can do include developing, writing as well as the recording of the blocks. An example of a public Blockchain is Bitcoin. The figure below shows the public Blockchain.

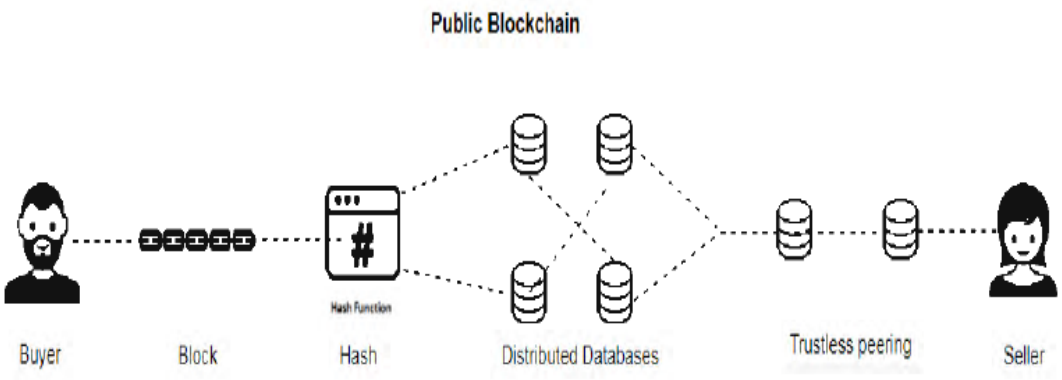

Figure 2-8: Public Blockchain (Source: SteemKr, 2017)

2.9.2 Differences Between Public and Private Blockchain

This section presents the key differences between a public, and a private Blockchain system.

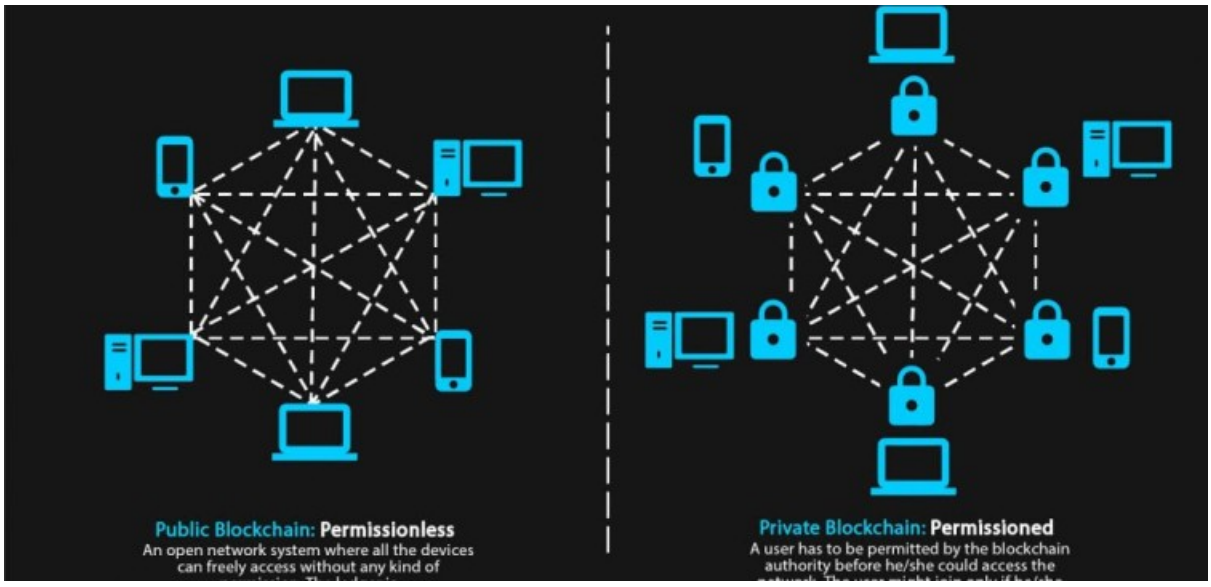

Figure 2.9: Differences between private Blockchain systems, source (https://medium.com/@yaonet/yao-network-the-futuristic-hybrid-3ba8c406f7aa)

Figure 2.9 shows the comparison diagram of the key differences between a public, and a private Blockchain system. It should be understood that identities are handled differently for each Blockchain type. In a private Blockchain, the identities are well known. However, under the public Blockchain, the identity is unknown, and the system makes use of pseudonyms (Jyothi & Chaudhari, 2020).

The gap between private and public Blockchains has a substantial impact on how identities are handled inside each Blockchain network. The identities of members in a private Blockchain are frequently pre-defined or permissioned, and they are openly known. The network is a closed system in which users can only be identified by pre-established credentials or authorization. It is appropriate for corporate or consortium-based applications since this identity transparency supports a regulated and managed ecosystem (Swan, 2015). Conversely, pseudonymous identities are maintained in a public blockchain, like the one that powers cryptocurrencies like Ethereum and Bitcoin. Rather than disclosing their true names, individuals are identified by pseudonyms or cryptographic addresses. These addresses, which are frequently a series of characters or alphanumeric codes, operate as network identifiers for individuals while hiding their actual identities. Moreover, participants' privacy and anonymity are guaranteed by the pseudonymous nature, which preserves transaction transparency while providing a layer of defence against any identity disclosure or monitoring (Antonopoulos, 2014).

In addition, in terms of security, pre-approval of participants is required under private Blockchain, whereas under a public Blockchain Proof of work or Proof of stake are used (Sunet al., 2021). To add more, under a private Blockchain, one must be authorised and be granted permission to access database whilst under a public Blockchain no permission required to access the database (Singh et al., 2021). Lastly, in terms of speed, a private Blockchain is faster than a pubic Blockchain.

2.9.3 Securing Data Using Blockchain

Data is described as “the input for various artificial intelligence (AI) algorithms”, (Wang et al., 2019). In smart environments, vast amounts of data are generated and transmitted from sensing devices to storage devices at rapid rates, which makes the data vulnerable and susceptible to threat actors. As stated before, this study hypothesises that the implementation of Blockchain-based technology will protect the data pipeline of a MHEWS. Blockchain technologies offers a promising avenue to attain data security by employing consensus mechanisms across the network to ensure secure and unchangeable data sharing while incorporating economic incentives. Consequently, Blockchain-secured data sharing can enhance the capabilities of artificial intelligence (AI) (Wang et al., 2019).

In every technological sector, the necessity for both scalability and data security is paramount. Given the current role of Blockchain technology in safeguarding data, one can contemplate a means of using Blockchain to secure IoT data (Tchagna et al., 2022).

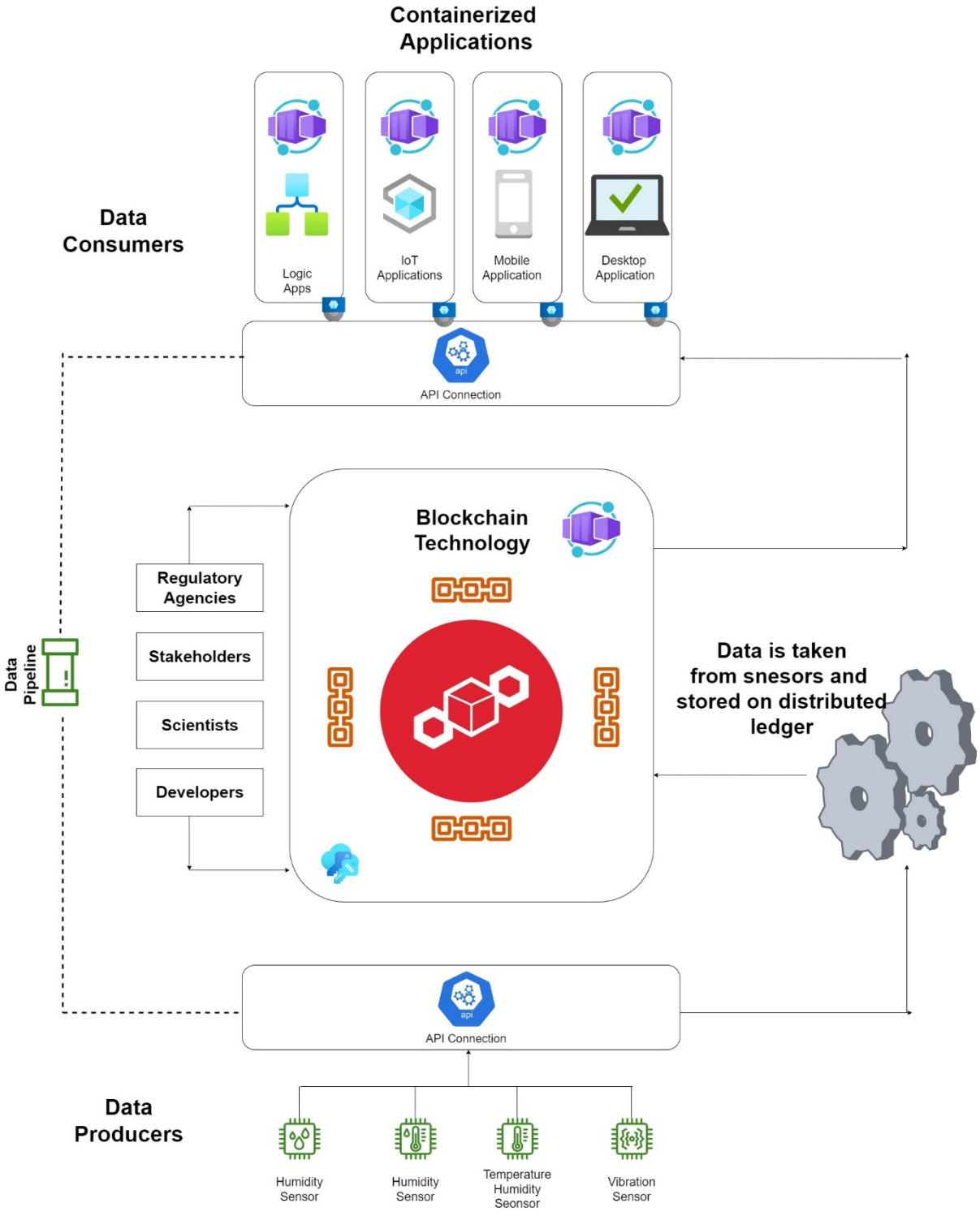

Figure 2.10: Blockchain implementation, (Ramahlosi, 2023)

2.9.4 Potential Benefits of Blockchain

Blockchain has been proven to possess many benefits when adopted within an IOT environment, (Atlam et al., 2018).

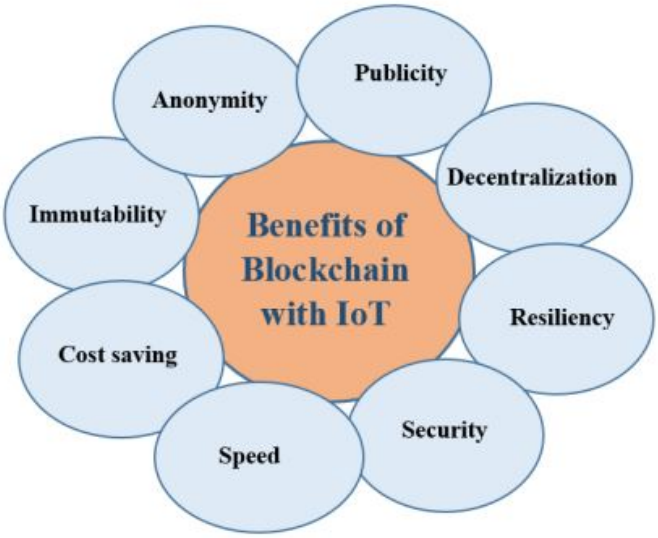

Figure 2.11: Benefits of Blockchain Technology (Source: Atlam et al., 2018)

These benefits depicted in Figure 2.11 can be summarised as follows.

Publicity: Since each participant has an own ledger, everyone can see every transaction and every block. Even though every participant may view the transaction's content, it is secure because of the participant's private key. The IoT is a dynamic system that allows all connected devices to share information while maintaining user privacy.

Decentralisation: Before a transaction can be approved and added to the distributed ledger, it must be verified by the majority of participants. No one body has the capacity to grant approval for transactions or establish requirements for transaction acceptance. As a result, a great deal of trust is involved since transaction validation requires agreement from the majority of network participants. Resultantly, the Blockchain will give IoT devices a safe foundation. Moreover, getting rid of the present centralised IoT architecture's single point of failure and centralised traffic flows.

Resilience: Every node has a copy of the ledger on hand, which houses every transaction ever done within the network. Therefore, the Blockchain is more resilient to assault. Every other node in the Blockchain would continue to maintain it even in the event that one was hacked. Importantly, an IoT node's copy of its data will enhance information exchange requirements. It does however bring up additional processing and storage problems.

Security: With so many disparate and varied devices in the IoT, a safe network across untrusted parties is essential. Blockchain can help with this. Put another way, not every IoT network node has to be hostile in order to launch an assault.

Speed: A Blockchain transaction may be executed at any time of day and is dispersed around the network within in a few minutes.

Cost saving: The high infrastructure and maintenance costs of centralised design, massive server farms, and networking equipment make current IoT solutions pricey. The sheer number of communications that has to be managed when there are tens of billions of IoT devices will drive those costs up considerably.

Immutability: One of the key benefits of Blockchain technology is its immutable ledger. Most network nodes have to verify any amendments made to the distributed ledger. As such, it is tricky to alter or remove the operations. Immutable ledgers for IoT data would improve privacy and security, which are the two main issues facing this current technology and all emerging ones.

Anonymity: To safeguard their identities, each buyer and seller uses unique, and anonymous address numbers to complete the transaction. This feature has come under fire as it promotes the usage of cryptocurrencies on the black market on the internet. On the other hand, it could be useful in other situations.

2.10 Difficulties Faced When Incorporating Blockchain with IoT

Integrating Blockchain would undoubtedly offer a lot of benefits. As Figure 2.12 illustrates, the Blockchain technology is not a flawless model and has its own drawbacks and difficulties. These difficulties can be summed up as follows.

Scalability: Challenges with the Blockchain's scalability might result in centralisation, which would be detrimental to the cryptocurrency's development. As the number of nodes in the network rises, the Blockchain performs badly in terms of scaling. Given that a significant number of nodes are anticipated in IoT networks, this problem has proven to be of grave disadvantage.

Processing Power and Time: The amount of time and processing power required to encrypt every object in a Blockchain system. Not every sort of device in an IoT system will be able to perform the same encryption methods at the necessary speed since different types of devices have highly varying computational capabilities.

Storage: One of the major advantages of Blockchain technology is that it does away with the requirement for a central server to hold device IDs and transaction histories; nevertheless, the ledger must be kept on the nodes themselves. With time and the number of nodes in the network growing, the distributed ledger will get larger. IoT devices, as previously stated, have extremely little storage space and very little processing power.

Lack of expertise: The use of Blockchain technology is still in its beginning stages. As a result, only a limited number of people have extensive understanding of the distributed ledger, particularly in the other industries. There is a general ignorance about the Blockchain's operation in other applications. Adopting the Blockchain with IoT would be very challenging without public understanding of the Blockchain because IoT devices are widely available.

Legal and compliance: A major concern for businesses and manufacturers alike is that the Blockchain technology, which aims to link individuals from several nations does not yet have any regulations or standards to adhere to. This obstacle will be the primary factor preventing Blockchain from being used in numerous industries and applications.

Naming and discovery: Nodes are not intended to locate one another inside the network since Blockchain technology is not intended for the IoT. One such application is Bitcoin, where nodes use the IP addresses of certain "senders" that are incorporated in the Bitcoin client to create the network topology. This strategy is not feasible for IoT devices as those devices will regularly be shifting and changing the network topology. Figure 2.12 summarises the challenges that were just discussed the in the previous section.

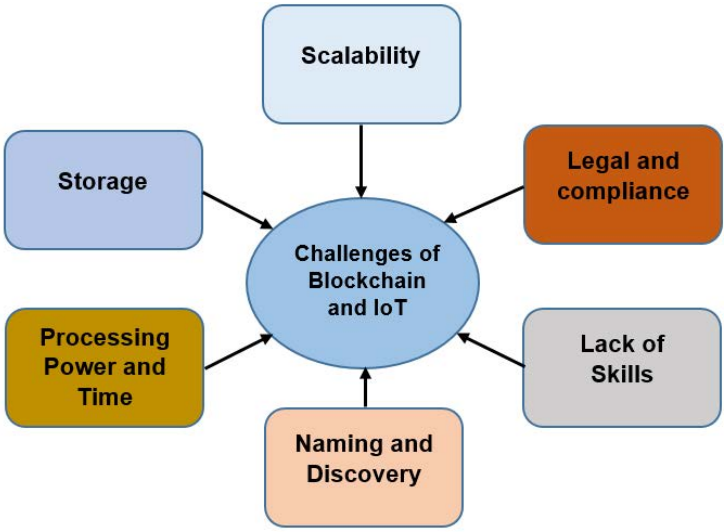

Figure 2.12: Challenges of Blockchain and IoT (Source: Atlam et al., 2018)

2.11 Empirical Literature Review

This section is based on the critical analysis of recent works that were carried out on the subject matter. Different authors, for example, (Akanbi and Masinde 2020) carried out a study that was oriented towards environmental monitoring. This study, therefore, is an addendum to the above-mentioned research, and literature as it aims to explore how the incorporation of Blockchain-based technologies could address the security challenges associated with smart environments with the main focus on a MHEWS.

Research was conducted on the use of Blockchain technology in mitigating disaster management and national security by (Panesir 2018), which showed that Blockchain technology could be used to store highly confidential information useful in ensuring that national security is maintained. It was also realised that Blockchain is a useful tool that helps to overcome the loss of time and ensure that urgent help is rendered to victims of different disasters. Another research was conducted by (Sobha & Sridevi 2019) regarding the use of Blockchain in disaster management in a research study that was based on a systematic literature review. From the study, it was discovered that Blockchain has many advantages such as safe recording of disaster information and ensuring confidentiality, resulting in timeous response to disasters (Sobha & Sridevi, 2019 p.5).

Meanwhile, investment in new technology requires technical experts as well as huge financial resources. As such, there is also a need for developing economies, especially in Africa to tap into this technology. This will help in alleviating the adverse effects of disasters. Notably, any

security challenge that affects the full adoption of 4IR technologies in smart environments should be addressed. This will help to ensure that sustainable technology is maintained in these environments. This can also help in solving other challenges that affect different continents. For example, drought affects SSA, and EWSs are required (Akanbi & Masinde, 2018).

Furthermore, World Bank carried out research on Blockchain technologies and the enhancement of climate markets. From the research, it was realised that "Blockchain technology can synthesises and support the transaction of all types of emission-related data" (World Bank, 2018). This shows that Blockchain technology can be used for weather related aspects, and it can therefore be useful in achieving the goals of this research study.

Blockchain as well as other digital technologies in the smart environment require a clear roadmap for their usage. This can be a security challenge that can limit the full adoption of the 4IR technologies if there is no pellucid road map. The roadmap will help to ensure that the collected environmental data possesses integrity which will assist in the development of robust MHEWSs.

Furthermore, one security issue that the adoption of 4IR technologies in smart environments faces is the lack of knowledge about how other contemporary technologies, such as the IoT can effectively supplement Blockchain technology in terms of creating a reliable MHEWS (World Bank, 2018). This suggests that more investigation into this security issue is necessary. A lack of high-quality pilot studies that shows how the new technology interfaces the existing technology in as far as the development of MHEWSs is also another challenge that needs to be addressed. This implies that diverse stakeholders such as technological companies, entrepreneurs as well as other climate change stakeholders should partner together to build and diffuse the knowledge on how the existing technology can complement Blockchain technology in disaster management.

This is very essential especially when looking at the global village at large given that the increase in the population generally can also bring adverse consequences to the environment and this should be resolved (Ankani, 2013). If no research is thereby carried out to examine the compatibility of emerging technology and existing technology, the adoption of 4IR will be limited in the smart environment. The development of a MHEWS can be affected too, and this leaves the bulk of people and communities exposed to different hazards, or even hunger, especially in SSA (Masinde et al., 2012).

2.12 Conclusion

The goal of this chapter was to present a review of the previous research works conducted by some scholars. A closer look at the EWSs and natural hazards was also presented in this chapter. This chapter also discussed the effects of natural hazards. Some of these effects are infrastructure destruction, loss of lives, destruction of fauna and flora. Additionally, two types of Blockchain technologies were discussed as the associated benefits of using Blockchain technology. In this chapter there was also a discussion on security vulnerabilities confronting the incorporation of 4IR technologies in smart environments. Some of the challenges discussed are hacking, cyber-crime, loss of information, loss of financial resources, disruption in services as well as loss in digital rights. Under empirical literature review, it was realised that Blockchain technology is very useful in the smart environment though there is still need for more efforts towards supporting research on the compatibility of emerging technology, and existing technology.

CHAPTER THREE

RESEARCH DESIGN AND METHODOLOGY

3.1 Introduction

Driven by the preceding chapter, this chapter presents the research methodology. The research design and methodology are aimed at outlining the structured approach and methodological framework used to examine the effectiveness of Blockchain-based technologies in addressing security vulnerabilities that arise with the incorporation of 4IR technologies in smart environments, especially in the context of a MHEWSs.

In this chapter, the research paradigm, the research design, and the target population are discussed. Data analysis techniques adopted for this research are also explored at length. Furthermore, Blockchain technology implementation procedures, and steps followed to secure the data pipeline are also discussed, and these include implementing all relevant software. This is essential to solve the identified research gap and get the answers to the research questions outlined in Chapter One of this study.

As mentioned in Chapter One, this study focuses on mitigating security challenges by improving data security through the application of Blockchain technologies in smart environments. All the components of the research methodology are therefore crucial as far as the use of Blockchain in addressing security challenges associated with the incorporation of 4IR into smart environments using a MHEWS as a case study. Succinctly, this chapter is comprised of the following sections: research onion, research design (which is further broken down into experimental design, and research philosophy), data collection (which entails pilot experiments, and case study with experimental design), system analysis, testing, and lastly, the chapter conclusion.

3.2 Research Onion

Developed by (Saunders et al. 2012), the Research Onion is a conceptual framework that demonstrates the several processes or layers that go into conducting research. It offers a methodical framework for comprehending the successive phases, and methodological decisions that researchers make throughout the course of their work. The intricacies and depths of research methodology are symbolised by the metaphor of an onion.

Six interconnected layers make up the Research Onion, and each one represents a distinct step in the research process. These processes are:

- Research philosophy
- Research approach
- Research strategy
- Choices
- Time horizon
- Techniques and procedures

This six-step approach was employed in this research methodology and design. Research can further be grouped on the basis or grounds of its applicability, targeted research objectives or the research's mode of inquiry, which can be structured, or not (Maclennan, 2019).

Based on the research objectives outlined in the Chapter One of this study, the following approaches were used.

a. Applied descriptive structured - The main thrust was to identify security challenges and vulnerabilities that followed the adoption of 4IR technologies in an MHEWS, and in the form of risk assessment (Queen & Boakye, 2022).

b. Applied exploratory structured- The primary objective was to develop a secure data pipeline framework for the MHEWS, utilising Blockchain technology to safeguard data transmission from the sensing devices to the central repository and processing unit (Jardim et al., 2021). Apart from that, this technique was also used to assess and evaluate the degree to which the implementation of Blockchain-based technology goes in alleviating the security issues associated with 4IR technologies in an MHEWS.

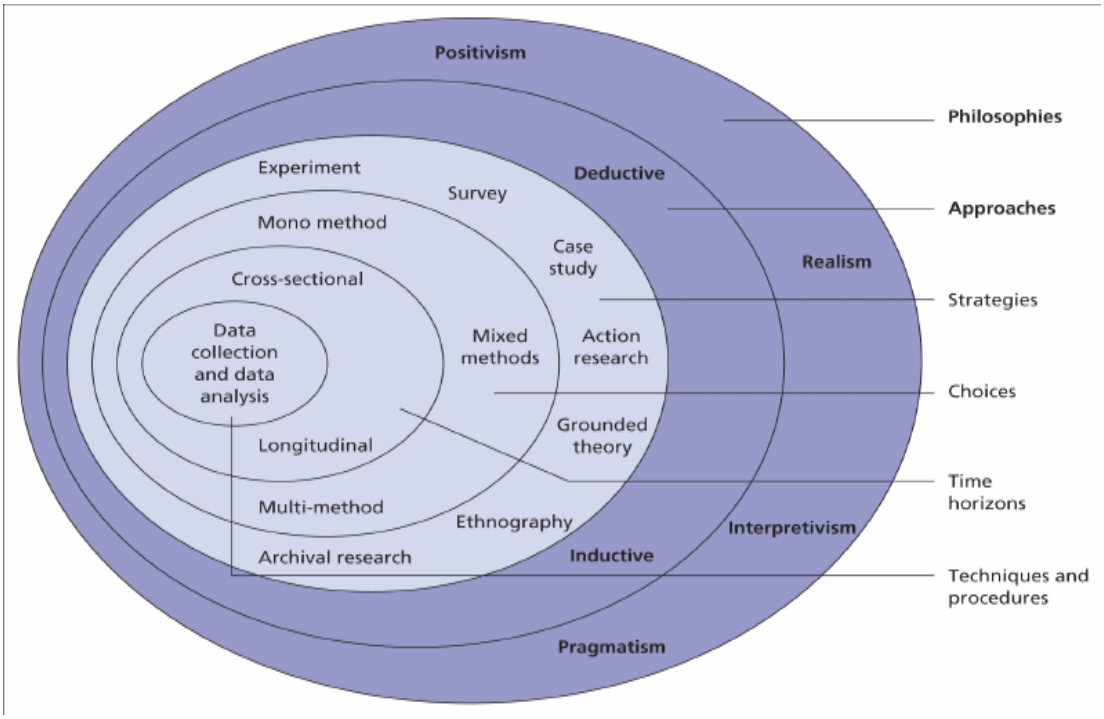

Figure 3-.13 Research Onion (Source: Melnikovas, 2018)

3.2.1 Research Philosophy

Every research project is carried out from a researcher's perspective or from a philosophical standpoint, founded on elements like truthfulness and legitimacy, and that specifies the appropriate research methodologies to be used (Project, 2020). (Guba, 1990) asserts that the research philosophy, which is made up of five options for carrying out the study, calls for a thorough specification of the research design. Ontology is first, followed by epistemology, methodology, data gathering techniques, and data analysis approaches (Jelonek et al., 2020), (Saito, 2021). The figure below summarises the above explained aspects.

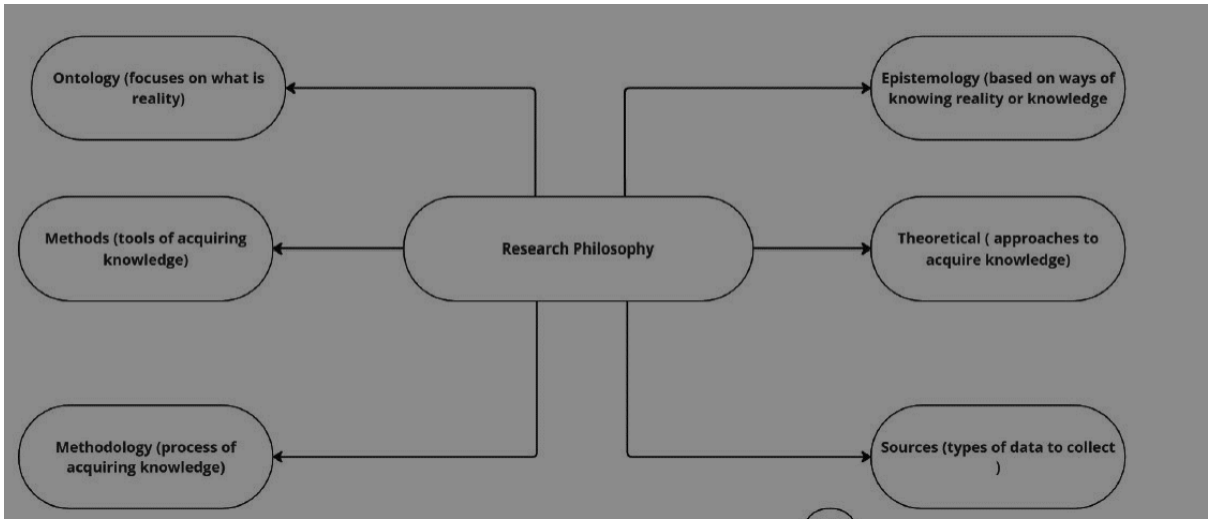

Figure 3.14: Research design steps based on research philosophy (Source Guba, 1990)

In this empirical research, the ontological assumption is towards having an intricate comprehension of the adoption of Blockchain-based technologies in mitigating security challenges that come with the adoption of 4IR technologies in smart environments with a specific focus on MHEWSs.

According to (Myers 1997), the three paradigms for information systems research are: positivist, interpretive, and critical. For this study, a positivist viewpoint was adopted, and from a positivist vantage point, "truth" exists, and can be recognised and assessed. The implementation of Blockchain technology, or solution according to this research, can be utilised to control, or alleviate the security difficulties posed by smart settings, and consequently, a MHEWS, and such implementation can be documented for knowledge representation (Hua et al., 2022).

3.2.2 Research Approach

The next layer of the above onion is a selecting a research approach. This step usually entails deductive (theory-driven), or inductive (data-driven) reasoning. Inductive approach uses data collection and analysis to produce theories, or insights, whereas deductive approaches begin with a theory and test assumptions. This research used the theory-driven approach. The research hypothesises that the application of Blockchain technology can mitigate the security challenges faced by the adoption 4IR technologies. The research used legacy data to test the hypothesis.

3.2.3 Research Strategy

This layer describes the entire study strategy for conducting the research study. This includes quantitative, qualitative, or mixed methods. While quantitative research prioritises numerical data and statistical analysis; qualitative research concentrates on investigating meanings, experiences, and context. Both qualitative and quantitative methodologies are combined in mixed methods research. This research used the qualitative approach as it experimented with different software to achieve the goal of the study which was to protect the data pipeline of a MHEWS.

3.2.4 Techniques and Procedures

The methods used for collecting data and analysis in the study make up the outermost layer of the research onion. Depending on the chosen research strategy and choices, these techniques may include approaches such as content analysis, theme analysis, statistical testing, or modelling procedures. The study adopted already existing MHEWS and therefore utilized existing legacy data that was collected. The data was cleaned and converted into Yamel file for experimental purposes.

3.3 Research Design

A research design can be described as a set of methodologies and strategies selected by a researcher to combine the numerous components of an analysis in a reasonably coherent way so that the research problem may be solved in an effective manner. (Sileyew, 2020). It can also be defined as the outline of a research endeavour and provides instructions for carrying it out step-by-step (Bazen et al., 2021). There are a number of different research designs, and some of these are: descriptive, experimental, correlational, diagnostic and explanatory (Nyhan & Howlin, 2021; Ghosh et al., 2019).

The methodology for the proposed secure data pipeline framework development was based on qualitative research methods from in-depth analysis, and risk assessment of the adopted 4IR technologies of EWSs making the MHEWSs (Anderson et al., 2022). The risk assessment for identifying the security vulnerabilities findings was used in determining the components of the proposed framework for the chosen implementation environment. The framework was developed iteratively, integrating the overall logic. To accommodate the change request process until the core research objectives are met.

3.4 Experimental Design

An example of an experimental research design is one in which a scientific methodology is used to investigate (Pesti et al., 2013). Any research carried out in situations that are suitable for science uses experimentation (Pesti et al., 2013). Furthermore, researchers' confirmation that a variable change is only caused by changing the constant variable, and it is necessary for experimental investigations to be effective (Lendvai & Joó, 2020). The study design adopted for this study is an experimental approach using already developed EWSs in the context of an MHEWS (Frøysa et al., 2020).

EWSs are commonly recognised as a pivotal element in mitigating the adverse effects and outcomes of perilous natural occurrences on communities. Like other terms associated with the reduction of disaster risks, this notion has developed progressively to culminate in a holistic framework that encompasses elements from initial stages to later stages. The intial stages include prediction and detection models and tools; while the later stages prioritise a people-centric approach. In recent years, global efforts have centred on adopting a comprehensive approach to various hazards. This has led to the emergence of what is known as the MHEWS, aimed at improving the efficiency of EWS and fostering collaboration among the diverse agencies participating in this endeavour (Aguirre-Ayerbe et al., 2020).

The EWSs under evaluation in this study are ITIKI: bridge between African indigenous knowledge and modern science of drought prediction (Masinde, 2015), and Adaptive Environmental Management System (AEMS) for Lejweleputswa, Vhembe, and uMgungundlovu district municipalities. In their study, (Garcia & Fearnley, 2012) state that EWSs are comprehensive structures that bring together various elements of disaster risk reduction with the goal of issuing timely alerts to mitigate the loss of life and alleviate the economic and social repercussions on susceptible communities. These warning systems stand as a pivotal instrument in the realm of disaster risk reduction strategies, tailored to diminish the consequences of a perilous event, and when executed successfully, can significantly boost the count of individuals who emerge unscathed.

As the number of devices are connected to the network are huge in MHEWS, this generates a large volume of data that requires processing. There are three important aspects of data protection in consideration, namely confidentiality, integrity, and availability, and they are known as the CIA triad (Kumar et al., 2018). To address the security issue in an integrated

environment such as this, Blockchain technology thereby comes as a rescue along with some other emerging technology (Rifi et al., 2017).

The implementation of Blockchain technology in an infrastructure involves the following three main components: launch and manage the environment, model smart contracts, and build and extend the application.

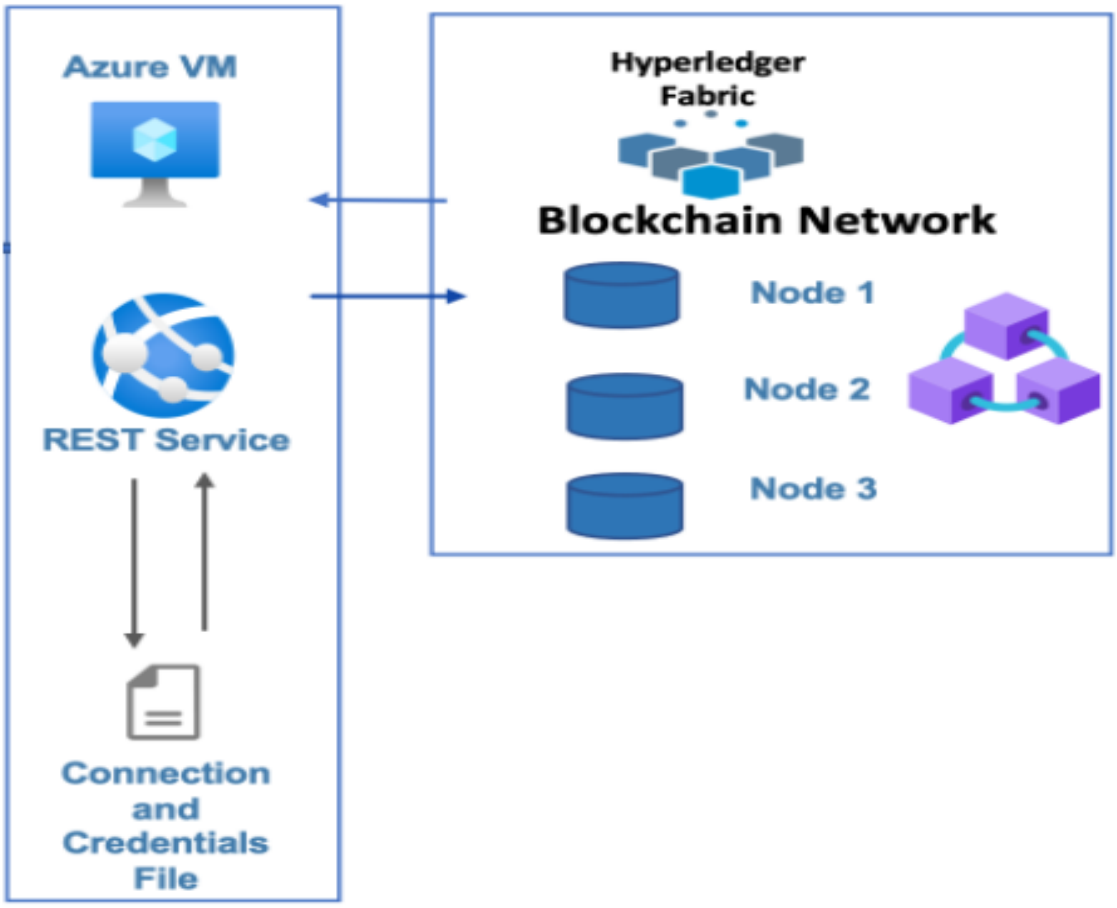

Figure 3.15: Loosely coupled implementation components in deployed environment (Source: Hughes, 2009)

Based on the data transmission architecture that will be built, the sensing nodes of the EWS and MHEWSs will record, transmit, read, and alter transactional data that is encrypted into their Blockchain (Kim et al., 2019). This procedure ensures a high standard of data integrity while also building confidence. Fundamentally, the distributed architecture of Blockchain eliminates any "hackable" entryway, or one point of malfunction that might potentially compromise the whole database (Arulprakash & Jebakumar, 2022).

3.5 Data Collection

Data collection refers to particular approaches, guidelines or techniques used to define, pick, process, and evaluate research knowledge. In research, data can be collected using different techniques (Pucken et al., 2021).

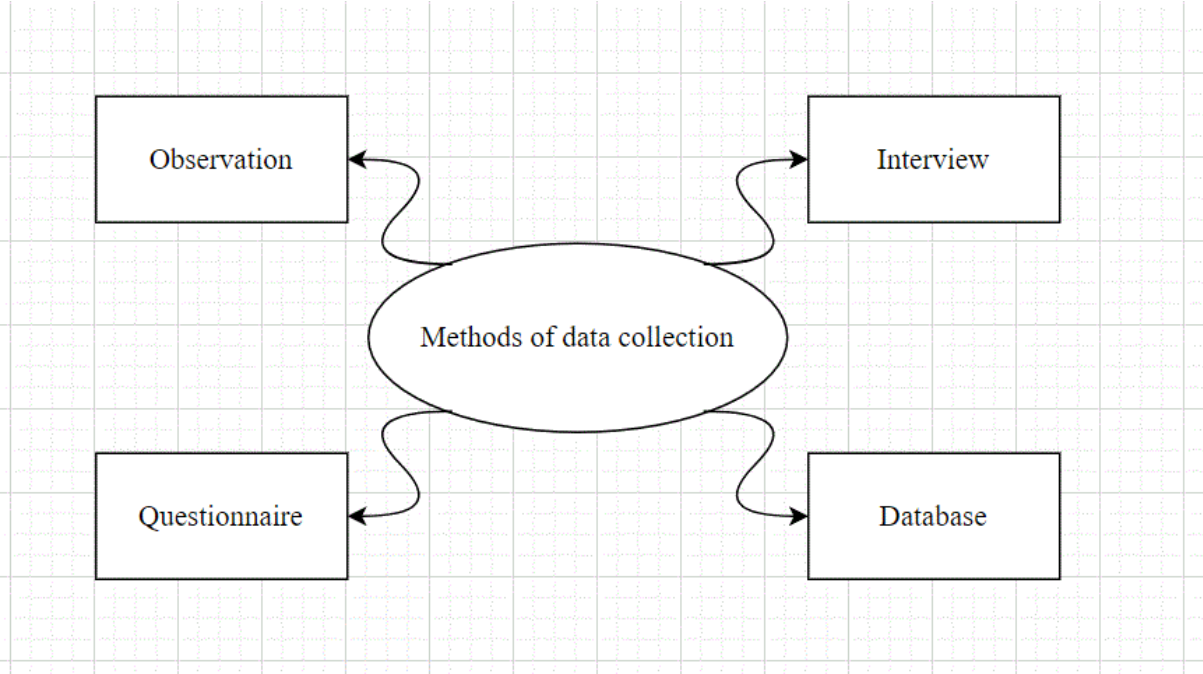

Figure 3.16: Data Collection Methods (Ramahlosi, 2024).

Figure 3-4 shows that data can be collected through observation, interviews, questionnaires, or from the databases (Petersen et al., 2021). In the context of information and communication technology studies, data can be collected through laboratory, and field sensor experiments, observation of digital information, and analysis of documents just to mention a few (Goertzen et al., 2020).

Environmental data used by the MHEWSs was collected using sensors. In a site with an internet connection, a sensor with smart computational capabilities was installed. The network allowed anything, at any time, and from anywhere to communicate with this sensor. The process of collecting data was facilitated by data collection systems that found and sent data across several such communication devices within the IoT architecture (Hajjaji et al., 2021).

The data flow from the IoT sensing devices was received through either wired or wireless connections based on the architecture of the EWSs under study. A detailed data security risk assessment was conducted to identify the security challenges and inherent vulnerabilities in the data pipeline of the system.

3.6 Securing the Data Flow with Blockchain

The research has provided a report from its' findings on the integration of the proposed Blockchain-based solution for securing data pipelines in the cloud and on-premises environment. A good consideration is the use of Hyperledger Fabric. In the research by (Cachin et al., 2017), Hyperledger Fabric is said to represent the execution of a decentralised ledger platform designed for executing smart contracts, harnessing well-established and recognised technologies, featuring a flexible structure that permits the integration of diverse functions through plug-and-play modules.

The Blockchain ledger was installed and coordinated as a containerised application in the cloud with a fully managed Kubernetes service. Leveraging serverless Kubernetes from AKS, data streams from the IoT sensing devices within the MHEWS were consolidated into a central repository and processed via cloud-based applications, enabling continuous integration and delivery (CI/CD). Moreover, a comprehensive CI/CD data pipeline was integrated into the AKS clusters, automating dataset security, detecting issues early, and enhancing processes with deep traceability to monitor and address security vulnerabilities. Below are some characteristics of the current fabric release.

- A permissioned Blockchain with immediate and irrevocable finality.
- Execution of customisable smart contracts (referred to as chaincode) written in Go (golang.org).
- User-designed chaincode is encapsulated within a Docker container.
- System chaincode operates within the same process as the peer.
- Robust security is provided through Certificate Authorities (CAs)

Adding a full Continuous Integration and Continuous Delivery (CI/CD) data pipeline to the AKS clusters with automated security of the datasets, detection of failures early, and optimises pipelines with intense traceability features that will enable monitoring of security vulnerabilities.

The distributed ledger technology (DLT) consumer application will fetch the data from the Service Bus, or node, and send it to the transaction builder, which signs and builds the transaction for authentication (Khan et al., 2022). These signed transactions will be forwarded through a ledger-specific Logic App connector to the cloud or on-premises platform. After

obtaining block and transaction data from preset transaction nodes, the Blockchain data manager decodes the data and transmits it to predetermined locations (Yadav et al., 2021).

Through smart contracts, Blockchain containers will protect data flows, data-in-use, and it will secure the code and maintain data integrity of consuming applications. Messages are written to the ledger, retrieved by the application dealing with the ledger network, and routed to the appropriate databases and applications (Merdjanovska & Rashkovska, 2022). The proposed Blockchain-based solution was designed to ensure the security and integrity of critical datasets, providing robust protection against potential breaches or unauthorized access. By implementing this structure, the solution will significantly mitigate the security vulnerabilities associated with the MHEWSs, offering a reliable safeguard for sensitive information. This added layer of security will strengthen the overall resilience of the system, reducing risks and enhancing the confidentiality, integrity, and availability of essential data used in the MHEWSs. For an on-premises solution, Gourisetti et al. (2021). suggest the implementation of the Blockchain Distributed Ledger Technology (DLT) solution as a container in a virtual machine located in an on-premises environment. An EWS's smart environment is localised, and data flows are tracked and directed via virtualised containers from sensing devices to the processing application and repository.

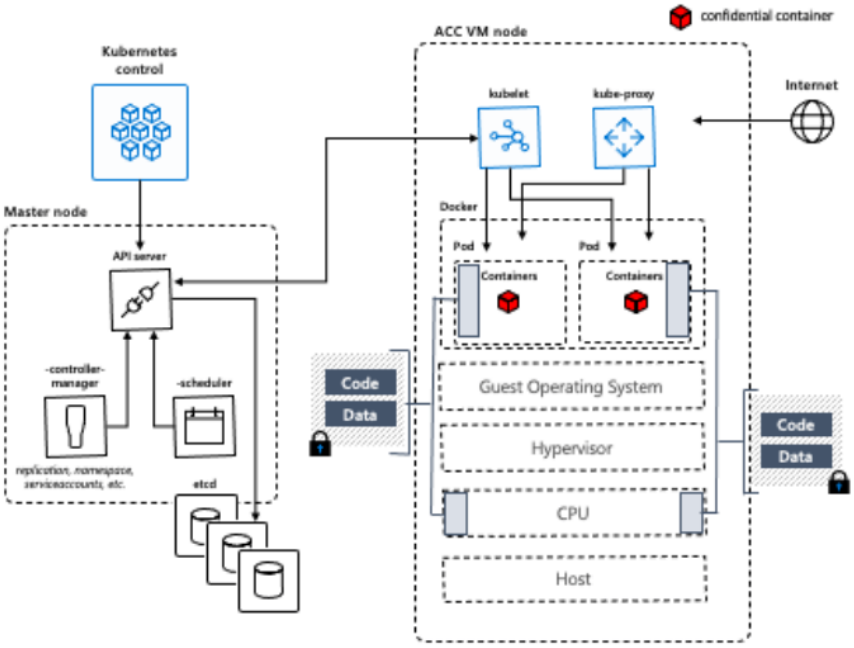

Figure 3.17: CI/CD Data pipelines in Azure Kubernetes Service (AKS) (Source: (https://docs.microsoft.com/en-us/azure/aks/)

3.7 System Analysis

As stated before, the study adopts two existing frameworks. System analysis is intended to understand the hardware and systems software of the EWSs making up the MHEWS. This involves the decomposition of a system into its components (Kendall & Kendall, 2011). The methodologies, techniques, and tools for the integrated system are evaluated. Each component of the EWS was analysed to identify the underlying structure of the system's modules and by extension the entire MHEWS and helps towards securing the data pipeline. The communication medium was also evaluated to understand the inherent security flaws and vulnerability from the sensing node to the destination.

ITIKI stands for Information Technology and Indigenous Knowledge with Intelligence, representing a drought EWSs that harmoniously blends traditional wisdom and scientific through drought predictions. This innovative system empowers small-scale farmers by providing them with valuable insights to enhance their decision-making processes, including optimal timing, crops, methods, and locations for planting. The system's reliability hinges on its utilisation of artificial neural networks, which bolster forecast models and yield remarkable accuracies ranging from 70% to 98% for prediction lead-times extending up to four years, (Masinde, 2022).

Moreover, the Adaptive Environmental Management System (AEMS) is a distinctive integration framework specifically engineered to bridge the gap between indigenous wisdom and scientific expertise; and tailored for implementation within the mining communities of Lejweleputswa. Subsequently, the framework underwent transformation into a prototype for an Adjustable Environmental Pollution Management System, comprising three key elements: (1) the collection of environmental pollution data, (2) environmental monitoring, and (3) environmental information sharing and communication (Mbele, 2017).

3.7.1 Steps of Blockchain Technology in Data Security

The goal of the next section is to provide the exact steps that were followed and the procedure that was used in the application of Blockchain technology in a data security.

Step 1: Defining the scope

The main focus on this step is to ensure that the proper steps are taken in verifying that the application of Blockchain technology on a MHEWS can assist in handling security vulnerabilities that follow the implementation of 4IR in smart environments. This is the central objective of this study. As such, the framework will provide guidance to the overall thrust of this empirical research. Overall, the framework developed for the application of Blockchain technology should be aligned towards a MHEWS.

Step 2: Data gathering

The sample data will be applied through the means of Blockchain technology to ensure that data security is achieved. The data to be used will be from the previous research conducted on the subject matter, and it will be applied and analysed to meet the research objectives of this study.

Step 3: Launching and managing the network

Smart contracts can be defined as blocks defined to execute when specific events occur as stated in the agreement. These contracts are frequently employed to automate the execution of an agreement so that there is no need for a middleman or further delay, and all parties involved may be confident of an immediately outcome (Chondrogiannis et al., 2022). Smart contracts are deemed useful for this stage because of speed, trust and transparency, security, efficiency and a high degree of accuracy. The management of the network will be done after the network is launched and it has to be managed too. This will be done to ensure that efficiency is attained.

Step 4: Build and extend the application

Based on the data transmission framework that will be created, the sensing nodes of the EWS, and the MHEWS will record, transmit, examine and alter transactional data that is encrypted into the respective Blockchain (Guo & Yu, 2022). The system will therefore be safe because of the nature of Blockchain technology. This means that it will not be susceptible to any potential threats like hacking or system failure. In other words, such a system will be efficient, and can be used to meet the intended purpose.

Step 5: Evaluation

This phase will be based on the evaluation of the build model in meeting the intended objectives. The Blockchain technology will therefore be evaluated based on the set criteria of managing the security challenges (Li & Gong, 2022). In other words, the application of Blockchain solutions will protect the data channel necessary for a MHEWS, and the system

should be very effective. Overall, the Blockchain should be useful in securing the data pipeline; if this is achieved, the demands of the study will have been met.

3.8 Hyperledger Fabric Implementation and Supporting Software

3.8.1 Ubuntu Installation

Kubernetes is an open-source container orchestration technology used to manage and distribute containerised applications in a variety of settings. Although Kubernetes is intended to be platform-neutral and work with a variety of operating systems and distributions, some environments may exhibit better than average performance with it. Research and real-world observations indicate that Kubernetes typically operates quite well in the Ubuntu environment.

Ubuntu is a popular Linux distribution that offers comprehensive support and easily accessible packages for the implementation of Kubernetes. Installing and maintaining Kubernetes components is made easier by its package management system, Advanced Package Tool (APT). This package also makes setting up Kubernetes clusters on Ubuntu easier for users.

Advantages of Ubuntu

All things considered, Ubuntu Landscape is a strong and adaptable system management tool that can assist in more successfully, safe, and economically managed Linux desktops (Zhou et al., 2021). Its advantages are shown below.

- Simplified server management: Landscape offers an easy-to-use dashboard with an intuitive design that makes complicated operations simpler, allowing the administration on Linux desktops more quickly and efficiently.
- Heightened security: Server infrastructure can be kept safe and compliant with Landscape's extensive security capabilities, which include vulnerability detection and security patch management.
- Better server performance: The server performance can be observed in real time using Ubuntu, which makes it easier for to detect and fix problems on time.

- Uncostly: The landscape may assist in cutting server administration expenses by optimizing server management, decreasing downtime, and enhancing security. Ubuntu was then installed successfully on the local machine [1].

[1] https://github.com/mramahlosi/Installation/blob/main/Ubuntu%20Install_Better%20pic.png

3.8.2 Kubernetes Installation

Once Ubuntu was installed, the next step was to install Kubernetes on the local machine and assign it rights to modify files on the local root. This process involves a number of steps such as installing, configuring, and providing the required permissions.

In this study, Kubernetes was chosen as the software for containerisation, as it merely share the host operating system (OS) as opposed to mimicking the entire operating system (OS) as in a Virtual Machine (VM). Because of this property, containers weigh less than virtual machines. Notably, micro-services are only meant to run in containers. Container orchestrators, which offer effective environment provisioning and auto-scaling, can be advantageous for any kind of production. Due to the deployment of Machine Learning (ML) applications, which require incredibly quick knowledge extraction in order to make quick choices; Big Data Analytics hosted on the Cloud are compute, or data-intensive (Zhou et al., 2021).

In this study, the researcher installed Kubernetes, and it was successful. [2]. When Kubernetes is initially installed, it by default installed in the root directory, resulting in lengthy access needs, that require persistent administrative credentials. In order to mitigate this problem, Kubernetes was moved from the root directory to a local folder, which eliminated the need for continuous administrator rights while in use[3].

As mentioned in previous chapters, the data flow is tracked and directed from the sensory devices to the processing application/repository through the Dockers in a virtualised environment. Docker is a popular containerisation technology for managing and delivering applications in virtualised environments. It is a vital tool for orchestrating and directing data streams when it comes to controlling data flows from sensing devices to processing applications or repositories. Docker makes it easier to track and route data flows coming from a variety of sensors. It possesses capabilities to encapsulate applications and their dependencies into lightweight containers, guaranteeing consistent deployment across various environments and devices. It also establishes a standardized information source for the designers of container-based solution, vendors, and end users, making resource use audits and analysis pertaining to the sequence of completed processes easier (Marques et al., 2022). Docker was then installed while updating Ubuntu to the latest version[4].

[2] https://github.com/mramahlosi/Installation/blob/main/K8%20Installation.png
[3] https://github.com/mramahlosi/Installation/blob/main/K8%20moved%20from%20root%20directory.png
[4] https://github.com/mramahlosi/Installation/blob/main/Docker%20Install%20and%20Ubuntu%20update.png

3.8.3 Minikube

For setting up a test environment for Blockchain components or applications inside of a Kubernetes cluster, Minikube has been proven to be a useful tool (Schwarzer, 2022) as it is a miniature, lightweight Kubernetes implementation (Rathore & Rajavat, 2022). It is a tool used particularly for configuring and maintaining a local Kubernetes cluster with one node. It is also a great platform for learning, testing, and development when it comes to Blockchain technology. With just one node, Minikube makes it possible to establish a small Kubernetes cluster that resembles a large-scale cluster. Within a Kubernetes environment, this local cluster makes it easier to build and test blockchain-related apps, smart contracts, or other components.

Minikube may have resource constraints in comparison to a fully functional production Kubernetes cluster because it runs on a single node. Minikube, on the other hand, includes commands and utilities that simplify cluster setup, configuration, and operation, making it an appropriate and controllable environment for testing and smaller-scale Blockchain applications or experiments. Minikube was chosen as the platform to orchestrate the experimenting purposes. The researcher also installed Minikube successfully to the local machine[5].

Similar to default storage of Kubernetes, Minikube was also stored in the root directory. To maximize accessibility and operational effectiveness of Minikube, it was moved to a local folder[6]. The purpose of this repositioning was to improve efficiency in the management process by offering a more accessible and ordered structure that would provide easier accessibility and smoother activities inside the system's environment.

Following the successful installation of Minikube, running it helped to verify that the local Kubernetes cluster was up and operating as expected. In this stage, Minikube was initialized, the Kubernetes cluster was also started, and its status was checked to make sure it was operational. This success suggests that there were no major problems or failures throughout the installation of Minikube, including the configuration, dependencies, and setup of Kubernetes components.

Several verification procedures were carried out to make sure Minikube was ready for use, including examining the version and status.

[5] https://github.com/mramahlosi/Installation/blob/main/Minikube%20Up%20and%20running.png
[6] https://github.com/mramahlosi/Installation/blob/main/K8%20moved%20from%20root%20directory.png

The Minikube version number is usually retrieved by running a programme or gaining access to particular system data. When dealing with certain configurations or upgrades, it is especially important to confirm the version to ensure compliance with the needed Kubernetes features or functions. The Minikube cluster's status was examined after the Minikube version was verified. To test if the Kubernetes cluster is up and operating, this step entails accessing the Minikube environment to ascertain its operational state and evaluating its health. To make sure the Minikube environment was operational and ready for use, information such as node status, services that were operating, and the general health of the cluster were examined[7].

Nodes are the basic processing units of a Kubernetes cluster, using nodes in the context of Minikube necessitates the existence of a cluster. Minikube installs and automatically spins up a single node local Kubernetes cluster to help with containerised application deployment and maintenance. Cluster status was thereby checked to verify that the Minikube-managed Kubernetes cluster was live[8], operational, and ready for usage. By confirming that the fundamental infrastructure needed to coordinate containerized applications is in place, this verification phase gives users peace of mind and facilitates experimentation, deployment, and maintenance of the local Minikube cluster.

Additionally, by going through this process, users can make sure that the Minikube-started Kubernetes environment is healthy and ready, giving them confidence in the cluster's functionality and dependability for a variety of Kubernetes and container orchestration-related development, testing, and learning objectives.

3.8.4 Smart Contract

Previously, certificates were generated on paper and needed design and production by issuing authorities. The personal data of the holders of certificates was critical to the issuing procedure. Holders were responsible for storing and presenting paper certificates upon receiving them. However, certificates issued on paper have problems such as difficulty in preservation, verification, and avoiding counterfeiting. Certificates became electronic as technology advanced. Noticeably, electronic certificates offer simplicity by being kept on electronic devices and supported by apps and interfaces for easy issuance, inquiries, and authentication, (Wankhede et al., 2023). Blockchain technology utilises smart contracts, which self-executing agreements that could be designed to dynamically implement data security rules. Examples of

[7] https://github.com/mramahlosi/Installation/blob/main/Minikube%20Status%20check.png
[8] https://github.com/mramahlosi/Installation/blob/main/Verification%20of%20cluster%20created.png

these agreements might include terms of service encoded into code between a data producer, and a data consumer.

A smart contract is an agreement between two or more Blockchain nodes. These are Blockchain-based applications that respond to certain contract events. In simple terms, they have the responsibility of automating the execution of an agreement to ensure that its members may be confident in the conclusion without the need for an intermediary. Once the stated conditions are achieved and validated, the Blockchain nodes carry out the actions and update the blockchain. As a result, the transaction cannot be modified. The nodes with the appropriate permissions are the only ones that can view the results (Farao et al., 2024). Sathiyamurthy et al. (2014) further define smart contracts as pre-built, rule-based programmes that are integrated into the Blockchain and run automatically to make sure each transaction satisfies the necessary conditions in order for a transaction to be completed. Transactions that occur between two parties are verifiably, efficiently, and irreversibly recorded on a Blockchain.

A smart contract can trigger action or transaction without the need for human interaction if it meets predetermined criteria set in the contract. Ethereum is an example of a Blockchains that can be used to write and execute smart contracts (Metcalfe, 2020). Ethereum is also an open source Blockchain network that allows the implementation and deployment of decentralized applications using smart contracts, (Alaba et al., 2023).

Figure 3.18: Smart Contract, (Ramahlosi, 2023)

To guarantee the smart contract's functionality and performance, the smart contract is initially installed and examined on a local server. In this stage, a local development environment is created, the smart contract is built, deployed into a simulated Blockchain or private Blockchain network, and its desired capabilities are tested. Debugging in a controlled environment and rapid iterations are made possible by testing on a local server.

It is further tested in the Remix testing environment before it is deployed to the cloud. Remix, an online integrated development environment (IDE) was developed especially for solidity smart contract deployment. It is a language that is used for writing smart contracts on Ethereum and other compatible Blockchains. Remix's smart contract testing feature adds further validation and debugging power. With Remix's functionality, developers may run functions, simulate different scenarios, and conduct extensive testing before deployment.

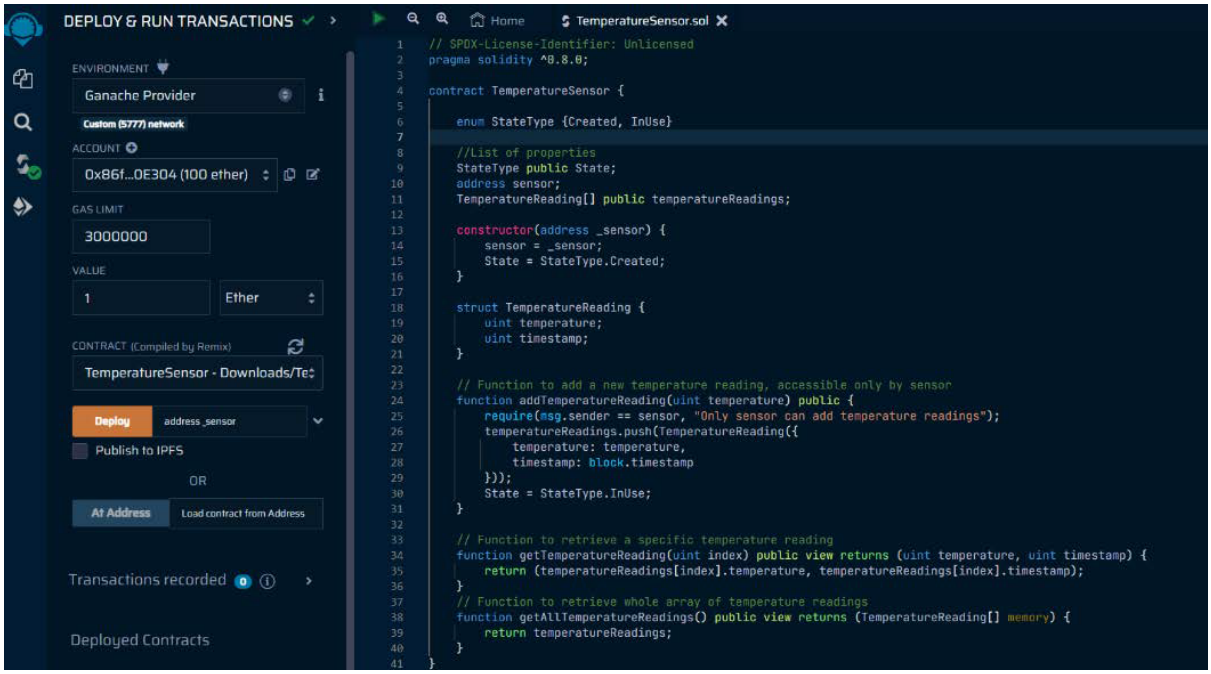

Figure 3.19: Kubernetes Cluster (Ramahlosi, 2023)

3.9 Testing

Testing is defined as operating a system, device, or component under predetermined, monitored settings while recording and observing the behaviour that is displayed (Balzan et al., 2021). For this study, the exploration testing method was utilized. This method states that before adding new concepts into the main solution, designers might test them electronically or physically. It is important to carry out this type of first verification testing. Early testing may help in the following ways: (i) determine whether an idea merits more investigation, (ii) specify how the product should be evaluated, and (iii) provide insight into the design's capabilities, (Balzan et al., 2021).

In IoT settings, security testing is a hard and difficult process. Different risks that might affect the approaches and expenses of security testing are exposed by heterogeneous devices. By utilizing the attack templates and the specifications of the IoT system model, model-based security testing methodologies facilitate the methodical creation of test cases for the evaluation of security requirements (Lonetti et al., 2023). He further states that presently, the most widely used security testing methods in the IoT are: (i) the technique of penetration testing, which finds vulnerabilities by modelling actual assaults; and (ii) fuzz testing, which stresses the device being tested with erroneous inputs of information or messages.

The Blockchain configured Docker file will be tested before the final image, which will be used for production and implementation. The functional testing approach will be achieved by

running the Docker file in standalone mode, and in an execution box to determine the processing of the data flow using the Blockchain network. This testing approach was chosen because Balzan et al. (2021) suggest that virtual testing (also known as computer-aided engineering modelling and simulation software) is a viable substitute for conducting testing for providing immediate feedback on the design or input for additional physical testing.

3.10 Conclusion

This chapter presented the research methodology. From the discussion, it was realised that applied descriptive structured and applied exploratory structured were used in the research. It was also established that an experimental approach was adopted as the study design using already developed EWSs in the context of a MHEWS. On data collection phase the primary focus was to gather information in support of the security risk assessment. Lastly, it was discussed that a system analysis was used in the research, and the major goal of the system analysis is to understand the hardware and systems software of the EWSs making up the MHEWS. Chapter 4, which addresses data analysis and presentation comes next.

CHAPTER FOUR

RESULTS AND ANALYSIS

4.1 Introduction

This chapter lays out the results obtained during the process of applying Blockchain in mitigating security vulnerabilities faced by the adoption of 4IR technologies in smart environments, i.e., in the case of a MHEWS. The chapter presents the finding on how Blockchain was used to manage security challenges faced in the integration of 4IR in MHEWSs. This is shown in the form of simulations that include the steps followed to install all software, and the creation of smart contracts step-by-step installations. The results are shared and analysed in the same sequence detailed in Chapter 3. The data analysis section is made up of the following: Ubuntu Installation, Kubernetes Installation, Git Installation, cURL installation, Docker and Docker Compose, Docker Images, Go Programming Language installation, Node.js Runtime and NPM, Python Installation and Hyperledger setup. Analysis of the system and Blockchain integration is also discussed at length in this chapter. The overall conclusion is also presented at the end.

This section is divided into two sub-sections:

- Discussions on the successful installation of the relevant software, and
- Discussions on whether the objectives of the research were met.

This research aims to examine the ways in which the usage of Blockchain technology or solutions might be applied to control or lessen the security risks associated with smart environments, and consequently, a MHEWS. The objectives of the study research are restated below.

- Determine security issues and weaknesses resulting from the integration of 4IR technologies in a MHEWS through risk assessment (Balistri et al., 2021).
    - Data Security
        - Data breaches, data theft, and unauthorised access to data, which may lead to data manipulation are major concerns for organisations as it could cost the affected companies millions due to issues such as lack of trust from stakeholders (Mustard, 2014). This issue is due to the

adoption of 4IR technologies and amalgamation of heterogeneous tools and systems in MHEWS.

- One of the reasons why Blockchain technology was chosen is its ability to ensure high levels of security, privacy, and data integrity without requiring a go-between to supervise transactions (Nayak et al., 2017).

- Create a secure data pipeline framework for a MHEWS utilising Blockchain technology to ensure the secure transmission of data from sensing devices to the central repository and processing unit.
    - Cachin et al. (2017) says that Blockchain-based applications possess inherent attributes such as authenticity, immutability, and consensus. Moreover, the records stored on a Blockchain ledger can be retrieved at any time and from any location. This makes Blockchain a promising technology for the management, and preservation of educational records.
- Examine, and assess how effectively Blockchain technology can mitigate security risks linked to 4IR technologies in a MHEWS.
    - One characteristic of Blockchain is its ability to deliver elevated levels of security, privacy, and data integrity autonomously, with no engagement of any additional entities. overseeing the transactions (Balistri et al., 2021).

The next section focuses on the software installation.

4.2 Results and Discussion

This following section is aimed at presenting the results and the discussion.

4.2.1 Ubuntu Installation

Hyperledger Fabric is the Blockchain Technology that has been chosen to be implemented to serve the objective of ensuring that the data pipeline of the MHEWS in discussion are secured. For this technology to run smoothly, a number of software's were installed on the local machine. Firstly, Ubuntu 22.04.2 was installed. As stated in the previous chapter, Kubernetes has been found to work best in the Ubuntu environment (Lundgren, 2021). Kubernetes has made tremendous progress in ensuring the smooth running of Windows workloads. It is however imperative to keep in mind that Windows support in Kubernetes is typically seen as being less developed than in Linux. This is also supported by (Khan 2020).

Kubernetes was designed primarily for Linux-based environments and has its roots in the Linux ecosystem. It has better documentation, and more tools and resources are accessible for Linux

distributions like Ubuntu. Due to the above benefits, Kubernetes is more widely supported by the community. Kubernetes installations on Linux frequently gain from earlier feature availability and more thorough testing. Based on the above reason. Ubuntu was installed on the local machine for the purpose of this study.

4.2.2 Kubernetes Installation

As mentioned earlier in the paper, Google created Kubernetes (AKSs), which is an open-source container orchestration platform that assists in managing applications composed of thousands of containers in various settings (Khan, 2023). It is scalable, allows disaster recovery, and ensures a high level of availability, which means that users can always access the application at all times. In the event that data is lost on the server, it must be recovered, indicating that there is a need for it to be stored in a secure and reliable location. Its design and characteristics may be used to simulate immutability principles, which are critical for guaranteeing that once a container is deployed, it does not change. If changes are required, a new container is deployed. This strategy improves deployments' predictability, security, and dependability. It is also frequently used for advanced microservices architectures and applications that demand scalability, reliability, and fine-grained control over containerized workloads (Malhotra et al., 2024). It was successfully installed for the purpose of simulating its functionality and achieving the objectives as set out in the research study. To deploy Kubernetes, several software are needed to be installed.

4.2.3 Git Installation

Git is among one of the prerequisite software that needs to be installed for Hyperledger Fabric to function. Popular permissioned Blockchain architecture Hyperledger Fabric enables a group of businesses to create Blockchain-based applications and do business among themselves. Private data collection (PDC), a fine-grained access control method introduced by Hyperledger Fabric permits a limited number of users access to share sensitive data. Hyperledger utilises Git as its version control system, allowing the downloading of repositories. Historically, Git was designed to interact with the Linux kernel; therefore, it has had to manage big repositories since its inception. Git was built in C, and thereby capable of reducing the runtime overhead associated with higher-level programming languages. Since its inception, Git has prioritized speed and performance. Git's data architecture protects the cryptographic integrity of your whole project. “Every file and commit are check summed and retrieved by its checksum when

checked back out. It's impossible to get anything out of Git other than the exact bits you put in.", (Git, 2023). Git was then successfully installed on the local machine[9].

4.2.4 cURL Installation

cURL is a useful Linux tool for data transfer and connection, troubleshooting as well as any other URL manipulations. Running a Docker-based Fabric test network in a local system requires cURL. The environment is set up such that one may launch the Fabric test network using the cURL command in the local machine. It specifically accomplishes the following things. It clones the repository for Hyperledger, or fabric-samples and it downloads and tags the most recent Hyperledger Fabric Docker images. It is also useful for downloading platform-specific Hyperledger Fabric CLI tool binaries and configuration files unto fabric-samples, or bin and or configure directories. Furthermore, one can communicate with the test network using these binaries.

[9] https://github.com/mramahlosi/Installation/blob/main/Git%20Install.png

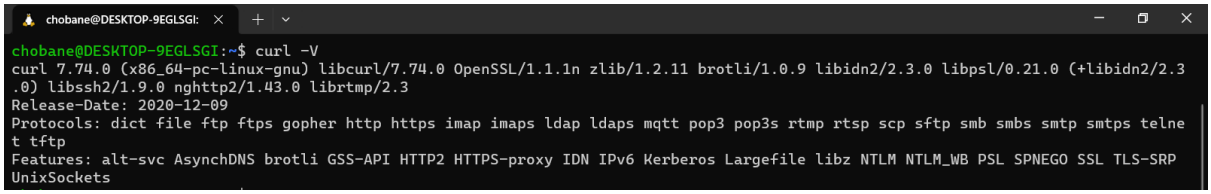

Figure 4.20: cURL installation, (Ramahlosi, 2023)

4.2.5 Docker and Docker Compose

Docker and Docker Compose is one of the other prerequisites for Hyperledger Fabric. Docker is used to provide our containerised environments. Docker compose is used by Hyperledger Fabric for defining fabric application services (Show, 2018). The location for defining all peer services and associated containers is the Docker-compose-cli.yaml service section. This technology utilizes several developments in Computer Science over the past ten years. It is used to run software in isolated environments.

Docker can be compared to a lightweight virtual machine even if it is not implemented that way. Docker simply isolates processes while using the same Linux kernel, as opposed to virtualising hardware for the guest operating system to use. The top-level constructs that make up Docker are Images, Containers, Networks, and Volumes. Docker is a versatile tool that enables the packaging of software components into containers, making deployment across various platforms hassle-free (Rad, Bhatt & Ahmad, 2017). Within the Ubuntu 18.04 repositories, Docker is readily accessible.

Docker Compose is a tool used for defining, and setting up multi-container Docker applications (Piedade, Dias & Correia, 2022). These applications are described in a pre-configured source file using YAML, enabling easy instantiation and management. Docker running on the local machine[10].

4.2.6 Docker Images

Like executables, Docker images contain all the data needed to run a programme. The 'docker image' command can be used to maintain Docker images, and the 'docker build' command can be used to create them, (Lane-Walsh et al., 2021). A list of Docker images that were successfully loaded on to the local machine is available here[11].

[10] https://github.com/mramahlosi/Installation/blob/main/Verify%20Docker%20running.png
[11] https://github.com/mramahlosi/Installation/blob/main/Docke%20images%20list.png

4.2.7 Go Programming Language Installation (GoLang)

Al-Sumaidaee et al. (2023) explicate that in the Fabric network, a variety of programming languages can be used to create smart contracts. For this paper, GoLang was installed and chosen as the language to create smart contracts. Fabric is predominantly coded in Go, necessitating the presence of a Go runtime for installation. Since chaincode programmes are written in Go, there are two crucial environment variables that must be appropriately configured. To make these variables permanent, you can add them to the suitable startup file such as your personal ~/.bashrc file when operating with the bash shell on Linux. GoLang installation was successful done by the researcher[12].

4.2.8 Node.js Runtime and NPM

Node.js is an open-source server platform that works across several platforms. It enables JavaScript to run on the server. Node serves as one of the main runtimes for Fabric, and is frequently employed for production deployments. It eradicates delays by executing the upcoming request (Chhetri, 2016). Sun, Bonetta, Humer and Binder (2018) posit that Node.js can perform numerous tasks such as the ones listed below.

- Create dynamic page content.
- Create, open, read, write, delete, and close files on the server.
- Collect form data.
- Add, delete, modify data in a database.

NPM manages packages for Node.js. This programme is automatically installed on the local machine when Node.js is installed. After installing Node.js, it is crucial to verify its successful installation by checking the version using the command "npm -v." Successful installation of Node.js Runtime and NPM respectively were achieved.

4.2.9 Python Installation

Python is a well-known programming language with a clear syntax that is frequently used for handling data or creating machine-learning models (Pajankar, 2017). It is also commonly used to construct block chain systems because of its role in the data ecosystem and the speed at which it may be used for prototyping. Python was successfully installed by the researcher[13].

[12] https://github.com/mramahlosi/Installation/blob/main/GoLang%20successfully%20installed.png
[13] https://github.com/mramahlosi/Installation/blob/main/Python%20Installation.png

4.2.10 Hyperledger Setup

As mentioned before, Hyperledger Fabric is a framework for developing Blockchain-based apps and solutions. Due to its support for modular consensus protocols, and general-purpose programming languages; it is known for being adaptable (Hang & Kim, 2021). It also encourages the application of Chaincodes, or smart contracts, to the control of the Blockchain network. Additionally, it uses a permissioned approach, making it suitable for usage in scenarios where membership and identity management are necessary. The decision to select Hyperledger Fabric as the framework was based on its permissioned Blockchain nature, which aligns with the data privacy requirements (Pulmano et al., 2023).

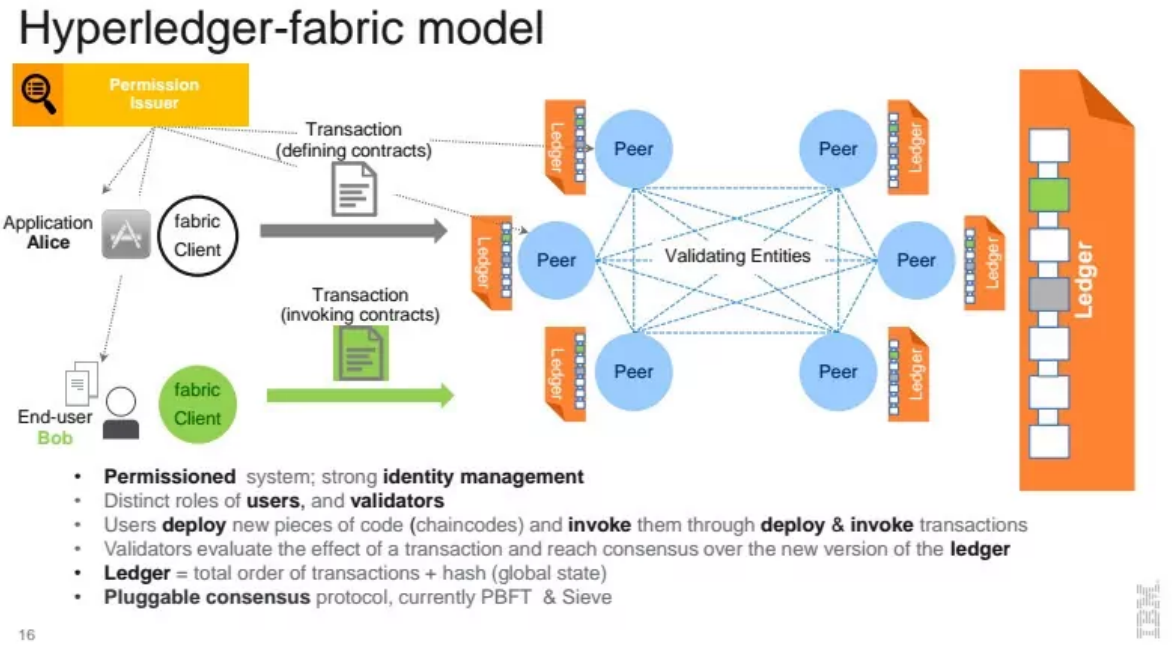

Figure 4-21: Hyperledger-fabric model (Source: (https://explorer.globe.engineer/?q=i+want+to+learn+about+blockchain+implementation)

4.3. Discussion

A secured data pipeline was developed for MHEWS that ensured that data transmitted from the sensing devices to the repository and processing unit was secure. This was possible by applying Blockchain technology. This successfully answers the second research objective of this study. Based on the findings obtained in the study, it is plausible to draw the conclusion that the application of Blockchain technology is useful to prevent securities vulnerabilities. Overall, the Blockchain proved to be useful in tracking environmental information as well as detection of hazards.

Furthermore, the installation of Hyperledger Fabric enabled the prevention of vulnerabilities from the adoption of 4IR technologies in a MHEWS in the form of risk assessment. This answers the first research objective of the study. The third research objective of the study was set to test and evaluate the effectiveness of Blockchain technology in mitigating risks in inhibiting the security challenges associated with infusion of 4IR technologies in a MHEWS. In this research, this was achieved through Docker file. The findings of this research are similar to the views stated by Ebrahim at al. (2022), and Alnahari and Ariaratnam (2022) that the use of Blockchain is very essential in the smart environment.

4.4. Conclusion

This chapter presented how Blockchain was used toward mitigating security vulnerabilities faced in the adoption of 4IR in MHEWS. Different steps that were followed to install all software, and the creation of smart contracts comprising step-by-step installations were presented. All the states objectives of the research study were successfully met. The following chapter discusses the summary, and the conclusion of the study.

CHAPTER FIVE

SUMMARY OF STUDY AND CONCLUSION

5.1 Introduction

This chapter focuses on the summary and conclusion of the study. It pesents a recap of the study objectives, research questions, and gives recommendations. It is essential to emphasise that the recommendations were formulated using the results of both the primary study and the empirical literature evaluation, ensuring they are well-supported by the evidence gathered throughout the research process. This chapter also summarises the conclusions of the literature review and the actual data. The research topic for the study serves as the foundation for the study's conclusions. Future recommendations are presented based on the findings of this study. At the end a conclusion is provided.

5.2 Summary

This section recaps and summarises all the chapters presented in this research paper.

5.2.1 Chapter One

This chapter was aimed at elaborating on the background, context of the research study, research questions and research objectives. This was all meant to introduce the topic in discussion and lay a foundation for the introduction of MHEWS, 4IR technology, and Blockchain.

5.2.2 Chapter Two

The chapter explored previous research conducted by experts in the fields of environmental warning systems, focusing mainly on MHEWS, Blockchain implementation and integration into heterogeneous IoT systems, challenges faced by incorporating 4IR in smart environments, and security challenges faced by these systems.

5.2.3 Chapter Three

The methodology chapter explicated the techniques and procedures which the researcher intended to use in order to meet the objectives set out in Chapter One. It further discussed the research philosophy, approach, design, and different data collection techniques. It also delved into detailing Blockchain technology, particularly, Hyperledger fabric, which is the proposed

Blockchain technology to successfully accomplish the objective of this paper. Smart contracts and testing methodology were also discussed.

5.2.4 Chapter Four

This chapter discussed the findings and results of the study based on the proposed methodology. This chapter elaborated on the installation of different software, which supports the proposed solution.

5.3 Discussion

In this section, the main objectives of the study are revisited, and reference is made to establish whether they were successfully met. The objectives paved a way in securing the data pipeline of MHEWS.

RO1: Identify security challenges and vulnerabilities from the adoption of 4IR technologies in a MHEWS

- Empirical literature conducted stipulated and indicated that the adoption of 4IR technologies in IoT devices brought with it numerous security and vulnerability challenges.
- The different challenges faced by these systems were explored at length.

RO2: Develop a secure data pipeline framework for MHEWS using Blockchain technology to secure data transmission from the sensing devices to the repository or processing unit.

- Blockchain was implemented on the local machine successfully with the aim to protect the data pipeline of MHEWS.

RO3: Test and evaluate the extent to which the application of Blockchain technology is efficient in preventing the security vulnerabilities associated with 4IR technologies in a MHEWS.

- The findings from both the experimental methods and the literature review provided clear evidence that Blockchain can effectively address and overcome the security vulnerabilities linked to the adoption of 4IR technologies in a Multi-Hazard Early Warning System (MHEWS).

5.4 Key Findings from the Literature Review

This section is intended to outline the key findings from the literature review. The focus of this research was to investigate how the implementation of Blockchain technology and solutions could address or alleviate the security challenges faced by smart environments. By extension, it could enhance the security of a Multi-Hazard Early Warning System (MHEWS).

According to the literature, technology is critical for dealing with climate hazards. It was also shown that several EWS can be merged for a more holistic system, which is a MHEWS. (Karki, 2019). This however demands a high degree of standards that must be uniformly executed across the board (Karki, 2019).

Under the literature review section, several challenges concerning the implementation of 4IR technology were identified. Some of these are: hacking, loss of information, cybercrime, financial loss, disruption in services, and loss in digital rights networks (Tsuchiya & Hiramoto, 2021; Masthead, 2021). The first research objective, which was to identify the security risks and vulnerabilities associated to the integration of 4IR technologies in a Multi-Hazard Early Warning System (MHEWS) was effectively addressed based on the security challenges found in the study. This was accomplished through the use of an extensive risk assessment approach..

Different types of Blockchain technology were discussed, including public Blockchain and private Blockchain. Furthermore, different benefits of Blockchain technology were articulated, and these included risk reduction, clean energy, and regenerative agricultural production, among others.

According to the empirical literature study, Blockchain technology can be used to store highly private information useful in safeguarding national security (Panesir, 2018). Aside from that, it was revealed that Blockchain has numerous advantages, including safe recording of disaster information, timely reaction to disasters, and a high degree of keeping information private and confidential (Sobha & Sridevi, 2019). From an environmental standpoint, it has been discovered that Blockchain technologies such as SolarCoin help to decrease the effects of climate change by providing incentives to solar energy providers for every unit of power produced using solar (Howson, 2019).

5.5 Findings from the Primary Research

The main conclusions drawn from the study's primary research are presented in this section. Creating a secure data transfer system to guarantee the safe flow of information from sensing

devices to the processing unit or central repository inside a Multi-Hazard Early Warning System (MHEWS) was the major focus of the study. In order to achieve this Blockchain was successfully implemented on the local machine.

The goal in incorporating Blockchain was to provide a decentralised, tamper-proof environment where data could safely and reliably move across different MHEWS components. By using Blockchain technology, it was possible to guarantee that data integrity would be upheld at every stage, avoiding loss, alteration, or unwanted access to sensitive data. The system will be able to protect critical data produced by sensors that collect environmental data.

This successfully answers the study's second research purpose. Based on the findings of this study, it is possible to conclude that the use of Blockchain technology is beneficial in preventing securities vulnerabilities. Overall, Blockchain proved effective in providing a tamper-proof environment.

Furthermore, the installation of Hyperledger Fabric enabled the prevention of vulnerabilities resulting from the use of 4IR technologies in an MHEWS in the form of risk assessment, which addresses the study's primary research objective. The third research goal of the project was to test, and assess the effectiveness of Blockchain technology in mitigating security vulnerabilities related to 4IR technologies in an MHEWS. This was accomplished in this study using Docker file as evidenced by the results provided in Chapter Four. Therefore, all the research objectives of this study were successfully met.

5.6 Recommendations and Future Scope

It has just been proven that Blockchain can counter the effects of incorporating 4IR in smart environments. In the future, there could be an exploration on how Artificial Intelligence (AI) and Machine Learning (ML) could also be incorporated to enhance Blockchain's capabilities in predicting, preventing, and mitigating security threats in real-time within smart environments.

As stated as one of the limitations of the study, scalability issues could also be investigated to find out how Blockchain technology can further be optimised to handle the massive scale of data generated by IoT devices in MHEWS without compromising performance, or security.

Future studies could focus on ensuring that the implementation of Blockchain-based solutions is more cost-effective for large-scale IoT deployments, particularly in resource-constrained environments.

Security should be in the forefront from the designing and implementation of IoT systems such as MHEWS. This can be achieved by incorporating Blockchain and other cryptographic methods to protect endpoint devices from vulnerabilities in the development phase.

There should be a collaboration between academic institutions, governments, and industry players to develop robust security frameworks for smart environments that integrate Blockchain technology.

Recommend ongoing assessment and adaptation of Blockchain security frameworks to respond to evolving cyber threats, ensuring the security of smart environments remains up to date. Develop training and awareness programmes for stakeholders to enhance understanding and implementation of Blockchain-based security solutions in MHEWS and similar smart environments.

5.7 Conclusion

This study explored how Blockchain technology may be used to manage and handle the various security issues that smart environments confront. These smart settings are more susceptible to cybersecurity attacks because of the increasing integration of new technologies, making it critical to investigate novel approaches to strengthen their resilience. The research also examined how Blockchain, with its immutable and decentralised ledger system, may provide reliable solutions to protect private information and guarantee safe device-to-device communication in smart settings. Additionally, this study explored the potential for extending these Blockchain-based solutions to improve the effectiveness and security of Multi-Hazard Early Warning Systems (MHEWS). Ensuring MHEWSs' resistance against cyberattacks is crucial due to its significant role in disaster risk management. This research used Blockchain to show how it may offer a tamper-proof, transparent, and secure architecture that reduces risks, and fortifies data integrity. The goal of the study was to contribute to the development of early warning systems and smart settings that are more robust and reliable.

The research hypothesised that the deployment of Blockchain-based solutions would successfully safeguard the data pipeline of a MHEWS. Through extensive testing, the research eventually confirmed this idea. The findings from the empirical analysis aligned closely with those derived from the initial, primary research phase, further reinforcing the reliability and accuracy of the results.

Furthermore, the study achieved all its specified research objectives, proving that a thorough effort was taken to solve the security problems that were first discovered. The study was also successful in filling in the knowledge void that had previously identified in the literature about the use of Blockchain in this context, and thereby offering fresh perspectives, and a deeper understanding of its possible benefit in securing MHEWS.

REFERENCES

Aguirre-Ayerbe, I., Merino, M., Aye, S. L., Dissanayake, R., Shadiya, F., & Lopez, C. M. (2020). An evaluation of availability and adequacy of Multi-Hazard Early Warning Systems in Asian countries: A baseline study. International Journal of Disaster Risk Reduction, 49, 101749. https://doi.org/10.1016/j.ijdrr.2020.101749

Akanbi, A.K. and Masinde, M., 2015, December. Towards semantic integration of heterogeneous sensor data with indigenous knowledge for drought forecasting. In Proceedings of the Doctoral Symposium of the 16th International Middleware Conference (pp. 1-5).

Akanbi, A. K., & Masinde, M. (2018). Towards the Development of a Rule-Based Drought Early Warning Expert Systems Using Indigenous Knowledge. 2018 International Conference on Advances in Big Data, Computing and Data Communication Systems, IcABCD 2018. https://doi.org/10.1109/ICABCD.2018.8465465

Akanbi, A., & Masinde, M. (2020). A distributed stream processing middleware framework for real-time analysis of heterogeneous data on big data platform: Case of environmental monitoring. Sensors (Switzerland), 20(11), 1–25. https://doi.org/10.3390/s20113166

Alnahari, M. & Ariaratnam, S. (2022). The Application of Blockchain Technology to Smart City Infrastructure. Retrieved from: https://www.researchgate.net/publication/362714447_The_Application_of_Blockchain_Technology_to_Smart_City_Infrastructure

Al-Razgan, M., Alrowily, A., Al-Matham, R. N., Alghamdi, K. M., Shaabi, M., & Alssum, L. (2021). Using diffusion of innovation theory and sentiment analysis to analyze attitudes toward driving adoption by Saudi women. Technology in Society, 65, 101558. https://doi.org/10.1016/j.techsoc.2021.101558

Al-Sumaidaee, Rami Alkhudary, G., Zeljko, Z., Andraws S. (2023). Performance analysis of a private Blockchain network built on Hyperledger Fabric for healthcare, Information Processing & Management, Volume 60, Issue 2. Retrieved from: https://www.sciencedirect.com/science/article/abs/pii/S0306457322002618

Anderson, K. M., Falah, N., Dempers, R., Talmadge, B., Hughes, J., Mirabal-Beltran, R., Gibson, S., Eisenberg, S., & Shara, N. (2022). Healthy Outcomes for All Pregnancy Experiences -

Cardiovascular-Risk Assessment Technology (Hope-Cat): Predicting Cardiovascular Risk in Pregnancy Through Machine Learning. Journal of the American College of Cardiology, 79(9), 1959. https://doi.org/10.1016/s0735-1097(22)02950-3

Antonopoulos, A. M. (2014). Mastering Bitcoin: Unlocking Digital Cryptocurrencies. O'Reilly Media

Arulprakash, M., & Jebakumar, R. (2022). Towards developing a Block Chain based Advanced Data Security-Reward Model (DSecCS) in mobile crowd sensing networks. Egyptian Informatics Journal, xxxx. https://doi.org/10.1016/j.eij.2022.03.002

Ashima, R., Haleem, A., Javaid, M., & Rab, S. (2021). Understanding the role and capabilities of Internet of Things-enabled Additive Manufacturing through its applications. Advanced Industrial and Engineering Polymer Research. https://doi.org/10.1016/j.aiepr.2021.12.001

Atlam, H. F., Alenezi, A., Alassafi, M. O., & Wills, G. B. (2018). Blockchain with Internet of Things: Benefits, challenges, and future directions. International Journal of Intelligent Systems and Applications, 10(6), 40–48. https://doi.org/10.5815/ijisa.2018.06.05

Balistri, E., Casellato, F., Giannelli, C., & Stefanelli, C. (2021). BlockHealth: Blockchain-based secure and peer-to-peer health information sharing with data protection and right to be forgotten. ICT Express, 7(3), 308–315. https://doi.org/10.1016/j.icte.2021.08.006

Balzan, E., Vella, P., Farrugia, P., Abela, E., Cassar, G., & Gauci, M. V. (2021). Towards a verification and validating testing framework to develop bespoke medical products in research-funded projects. Proceedings of the Design Society, 1(August), 3199–3208. https://doi.org/10.1017/pds.2021.581

Bazen, A., Barg, F. K., & Takeshita, J. (2021). Research Techniques Made Simple: An Introduction to Qualitative Research. Journal of Investigative Dermatology, 141(2), 241-247.e1. https://doi.org/10.1016/j.jid.2020.11.029

Cachin, C., Schubert, S., & Vukolić, M. (2017). Non-determinism in Byzantine fault-tolerant replication. Leibniz International Proceedings in Informatics, LIPIcs, 70, 24.1-24.16. https://doi.org/10.4230/LIPIcs.OPODIS.2016.24

Chhetri, N. (2016). A Comparative Analysis of Node.js (Server-Side JavaScript). Retrieved from: https://core.ac.uk/download/pdf/232792216.pdf

Chondrogiannis, E., Andronikou, V., Karanastasis, E., Litke, A., & Varvarigou, T. (2022). Using Blockchain and semantic web technologies for the implementation of smart contracts

between individuals and health insurance organizations. Blockchain: Research and Applications, 3(2), 100049. https://doi.org/10.1016/j.bcra.2021.100049

Croft, P. J. (2019). Environmental hazards: A coverage response approach. Future Internet, 11(3). https://doi.org/10.3390/fi11030072

Ebrahim, M., Hafid, A., & Eli, E. (2022). Blockchain as privacy and security solution for smart environments: A Survey. Retrieved from: https://www.researchgate.net/publication/359309707_Blockchain_as_privacy_and_security_solution_for_smart_environments_A_Survey

Etherisc (2023). ETHERISC teams up with Chainlink to deliver crop insurance in Kenya. Retrieved from: https://acreafrica.com/etherisc-teams-up-with-chainlink-to-deliver-crop-insurance-in-kenya/

Fadele Ayotunde Alaba, Hakeem Adewale Sulaimon, Madu Ifeyinwa Marisa, & Owamoyo Najeem. (2023). Smart Contracts Security Application and Challenges: A Review. Cloud Computing and Data Science, 5(1), 15–41. https://doi.org/10.37256/ccds.5120233271

Farao, A., Paparis, G., Panda, S., Panaousis, E., Zarras, A., & Xenakis, C. (2024). INCHAIN: a cyber insurance architecture with smart contracts and self-sovereign identity on top of blockchain. International Journal of Information Security, 23(1), 347–371.

Fleming-Muñoz, D. A., Whitten, S., & Bonnett, G. D. (2023). The economics of drought: A review of impacts and costs. Australian Journal of Agricultural and Resource Economics, September 2021, 501–523. https://doi.org/10.1111/1467-8489.12527

Frøysa, H. G., Skaug, H. J., & Alendal, G. (2020). Experimental design for parameter estimation in steady-state linear models of metabolic networks. Mathematical Biosciences, 319(November 2019), 108291. https://doi.org/10.1016/j.mbs.2019.108291

Garcia, C., & Fearnley, C. J. (2012). Evaluating critical links in early warning systems for natural hazards. Environmental Hazards, 11(2), 123–137. https://doi.org/10.1080/17477891.2011.609877

Garcia-Teruel, R. M., & Simón-Moreno, H. (2021). The digital tokenization of property rights. A comparative perspective. Computer Law and Security Review, 41, 105543. https://doi.org/10.1016/j.clsr.2021.105543

Ghosh, F., Abdshilla, H., Arnér, K., Voss, U., & Taylor, L. (2019). Corrigendum to “Retinal neuroinflammatory induced neuronal degeneration - Role of toll-like receptor-4 and

relationship with gliosis" [Experimental Eye Research 169 (2018) 99–110](S0014483517307510)(10.1016/j.exer.2018.02.002). Experimental Eye Research, 180, 260. https://doi.org/10.1016/j.exer.2019.02.009

Goertzen, L., Mehr, N., Lopez, M., Udell, C., & Selker, J. S. (2020). Low-cost and precise inline pressure sensor housing and DAQ for use in laboratory experiments. HardwareX, 8, e00112. https://doi.org/10.1016/j.ohx.2020.e00112

Gourisetti, S. N. G., Cali, Ü., Choo, K. K. R., Escobar, E., Gorog, C., Lee, A., Lima, C., Mylrea, M., Pasetti, M., Rahimi, F., Reddi, R., & Sani, A. S. (2021). Standardization of the Distributed Ledger Technology cybersecurity stack for power and energy applications. Sustainable Energy, Grids and Networks, 28, 100553. https://doi.org/10.1016/j.segan.2021.100553

Guba, E. (1990). The Paradigm Dialog, Sage, California.

Guo, H., & Yu, X. (2022). A survey on Blockchain technology and its security. Blockchain: Research and Applications, 3(2), 100067. https://doi.org/10.1016/j.bcra.2022.100067

Hajjaji, Y., Boulila, W., Farah, I. R., Romdhani, I., & Hussain, A. (2021). Big data and IoT-based applications in smart environments: A systematic review. Computer Science Review, 39, 100318. https://doi.org/10.1016/j.cosrev.2020.100318

Hang, L. & Kim, D. (2021). Optimal Blockchain network construction methodology based on analysis of configurable components for enhancing Hyperledger Fabric performance. Retrieved from: https://www.sciencedirect.com/science/article/pii/S209672092100004X

Howson, P. (2019). Tackling climate change with Blockchain. Nature Climate Change, 9(9), 644–645. https://doi.org/10.1038/s41558-019-0567-9

https://github.com/IBM/Blockchain-application-using-fabric-java-sdk

https://git-scm.com/about/info-assurance

Hua, W., Chen, Y., Qadrdan, M., Jiang, J., Sun, H., & Wu, J. (2022). Applications of Blockchain and artificial intelligence technologies for enabling prosumers in smart grids: A review. Renewable and Sustainable Energy Reviews, 161(February 2021), 112308. https://doi.org/10.1016/j.rser.2022.112308

Jardim, L., Pranto, S., Ruivo, P., & Oliveira, T. (2021). What are the main drivers of Blockchain Adoption within Supply Chain? - An exploratory research. Procedia Computer Science, 181, 495–502. https://doi.org/10.1016/j.procs.2021.01.195

Jelonek, Z., Drobniak, A., Mastalerz, M., & Jelonek, I. (2020). Jo ur na l P re of. Science of the Total Environment, 141267. https://doi.org/10.1016/j.isci.2022.104706

Jilcha Sileyew, K. (2020). Research Design and Methodology. Cyberspace, August. https://doi.org/10.5772/intechopen.85731

K. Zhou, Taigang Liu and Lifeng Zhou, "Industry 4.0: Towards future industrial opportunities and challenges," 2015 12th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD), Zhangjiajie, China, 2015, pp. 2147-2152, doi: 10.1109/FSKD.2015.7382284

Khan, M. D., Schaefer, D., & Milisavljevic-Syed, J. (2022). A Review of Distributed Ledger Technologies in the Machine Economy: Challenges and Opportunities in Industry and Research. Procedia CIRP, 107(2021), 1168–1173. https://doi.org/10.1016/j.procir.2022.05.126

Khan, S. (2023). Microsoft Azure Kubernetes Container Instances, Docker Brief Introduction, and Implementation Process. Retrieved from: https://www.researchgate.net/publication/370924759_Microsoft_Azure_Kubernetes_Container_Instances_Docker_Brief_Introduction_and_Implementation_Process

Khan, U. (2020). Comparative Study Of Linux and Windows. Retrieved from: https://vixra.org/pdf/2004.0247v1.pdf

Kim, J., Li, B., Scheideler, O. J., Kim, Y., & Sohn, L. L. (2019). Visco-Node-Pore Sensing: A Microfluidic Rheology Platform to Characterize Viscoelastic Properties of Epithelial Cells. IScience, 13, 214–228. https://doi.org/10.1016/j.isci.2019.02.021

Котлер, Ф. (2008). No TitleМаркетинг по Котлеру. 282

Krishna Jyothi, K., & Chaudhari, S. (2020). A novel Blockchain based cluster head authentication protocol for machine-type communication in LTE network: Statistical analysis on attack detection. Journal of King Saud University - Computer and Information Sciences, (xxxx). https://doi.org/10.1016/j.jksuci.2020.08.014

Kumar, P. R., Raj, P. H., & Jelciana, P. (2018). Exploring Data Security Issues and Solutions in Cloud Computing. Procedia Computer Science, 125(2009), 691–697. https://doi.org/10.1016/j.procs.2017.12.089

Kwee-Meier, S. T., Mertens, A., & Jeschke, S. (2019). Recommendations for the design of digital escape route signage from an age-differentiated experimental study. Fire Safety Journal, 110, 102888. https://doi.org/10.1016/j.firesaf.2019.102888

Lane-Walsh, S., Stillerman, J., Santoro, F., & Fredian, T. (2021). Introduction to MDSplus using Docker. Fusion Engineering and Design, 165(January). https://doi.org/10.1016/j.fusengdes.2020.112121

Lee, D. G., Kim, G. W., J. W. Han, Jeong, Y. -S., and Park, D. -S., "Smart Environment Authentication: Multi-domain Authentication, Authorization, Security Policy for Pervasive Network," 2008 International Symposium on Ubiquitous Multimedia Computing, Hobart, TAS, Australia, 2008, pp. 99-104, doi: 10.1109/UMC.2008.28

Lee, H., Kang, S. W., & Koo, Y. (2020). A hybrid energy system model to evaluate the impact of climate policy on the manufacturing sector: Adoption of energy-efficient technologies and rebound effects. Energy, 212, 118718. https://doi.org/10.1016/j.energy.2020.118718

Lehto, M. (2022). Cyber-Attacks Against Critical Infrastructure. In: Lehto, M., Neittaanmäki, P. (eds) Cyber Security. Computational Methods in Applied Sciences, vol 56. Springer, Cham. https://doi.org/10.1007/978-3-030-91293-2_1

Lendvai, A., & Joó, A. L. (2020). Improvement of stressed skin design procedure based on experimental and numerical simulations. Journal of Constructional Steel Research, 168, 105874. https://doi.org/10.1016/j.jcsr.2019.105874

Li, Y., Wu, Y., Zhang, X., Hamed, E., Hu, J. and Lee, I., 2021, May. Developing a Miniature Energy-Harvesting-Powered Edge Device with Multi-Exit Neural Network. In 2021 IEEE International Symposium on Circuits and Systems (ISCAS) (pp. 1-5). IEEE.

Lonetti, F., Bertolino, A., & Di Giandomenico, F. (2023). Model-based security testing in IoT systems: A Rapid Review. Information and Software Technology, 164(September). https://doi.org/10.1016/j.infsof.2023.107326

Lundgren, J. (2021). Kubernetes for Game Development Evaluation of the Container-Orchestration Software. Retrieved from: https://www.diva-portal.org/smash/get/diva2:1562637/FULLTEXT01.pdf

Luther, J., Hainsworth, A., Tang, X., Harding, J., Torres, J., Franchiotti, M. (2017). World Meteorological Organization (WMO)—Concerted International Efforts for Advancing

Multi-Hazard Early Warning Systems. Retrieved from: https://link.springer.com/chapter/10.1007/978-3-319-59469-9_9

Maclennan, K. M. (2019). The importance of research applicability. Retrieved from: https://www.researchgate.net/publication/348044219_The_importance_of_research_applicability

Malhotra, R., Bansal, A., & Kessentini, M. (2024). A Systematic Literature Review on Maintenance of Software Containers. ACM Computing Surveys. https://doi.org/10.1145/3645092

Manda, M. I., & Dhaou, S. Ben. (2019). Responding to the challenges and opportunities in the 4th industrial revolution in developing countries. ACM International Conference Proceeding Series, Part F1481, 244–253. https://doi.org/10.1145/3326365.3326398

Marques, M. A., Miers, C. C., Rodrigues Obelheiro, R., & Simplico Jr., M. A. (2022). Clustered event2ledger: Docker event traceability using consortium Hyperledger blockchains. XXII Simpósio Brasileiro de Segurança Da Informação e de Sistemas Computacionai, 0–26.

Masinde, M. (2014). An Effective Drought Early Warning System for Sub-Saharan Africa: Integrating Modern and Indigenous Approaches. Retrieved from: https://www.semanticscholar.org/paper/An-Effective-Drought-Early-Warning-System-for-and-Masinde/6de15ccb57f903fba5c2fb849d76c1ffa53b0ce9

Masinde, M., "ITIKI Success Story: Classic Application of Design Thinking," 2020 IST-Africa Conference (IST-Africa), Kampala, Uganda, 2020, pp. 1-9.

Masinde, M., & Bagula, A. (2011). ITIKI: bridge between African indigenous knowledge and modern science of drought prediction. Knowledge Management for Development Journal, 7(3), 274–290. https://doi.org/10.1080/19474199.2012.683444

Masinde, M., Bagula, A., & Muthama, N. J. (2012). The role of ICTs in downscaling and up-scaling integrated weather forecasts for farmers in Sub-Saharan Africa. ACM International Conference Proceeding Series, 122–129. https://doi.org/10.1145/2160673.2160690

Mbele, M. J. (2017). Development of an Adaptive Environmental Monitoring System for Lejweleputswa District : A Participatory Approach through Fuzzy Cognitive Maps Masters Dissertation by Mpho Josephine Mbele Supervised by Prof . Muthoni Masinde and Itumeleng Kgololo-Ngowi Thi.

Melnikovas, A. (2018). Towards an explicit research methodology: Adapting research onion model for futures studies. Journal of Futures Studies, 23(2), 29–44. https://doi.org/10.6531/JFS.201812_23(2).0003

Mentsiev, A. U., Mentsiev, A. U., & Amirova, E. F. (2020). IoT and mechanization in agriculture: Problems, solutions, and prospects. IOP Conference Series: Earth and Environmental Science, 548(3). https://doi.org/10.1088/1755-1315/548/3/032035

Merdjanovska, E., & Rashkovska, A. (2022). Comprehensive survey of computational ECG analysis: Databases, methods and applications. Expert Systems with Applications, 203(September 2020), 117206. https://doi.org/10.1016/j.eswa.2022.117206

Metcalfe, W. (2020). Ethereum, smart contracts, DApps. In Economics, Law, and Institutions in Asia Pacific. Springer Singapore. https://doi.org/10.1007/978-981-15-3376-1_5

Mustard, S. (2014). The NIST cybersecurity framework. InTech, 61(1–2), 1–6. https://doi.org/10.4018/978-1-6684-3698-1.ch003

Myers, M. D. (1997). Qualitative Research in Information Systems. Management Information Systems Quartely, 21(2), 241–242.

Mzekandaba, S. (2023). Cyber crime's annual impact on SA estimated at R2.2bn. Retrieved from: https://www.itweb.co.za/content/JN1gPvOAxY3MjL6m

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System

Nayak, A,. & Dutta, K., "Blockchain: The perfect data protection tool," 2017 International Conference on Intelligent Computing and Control (I2C2), Coimbatore, India, 2017, pp. 1-3, doi: 10.1109/I2C2.2017.8321932

Nyhan, T., & Howlin, F. (2021). From registered nurse to nursing student - Exploring registered nurses' transition to nursing student during a post-registration children's nurse programme: A qualitative descriptive research study. Nurse Education Today, 105(July), 105046. https://doi.org/10.1016/j.nedt.2021.105046

Okutan, A., & Çebi, Y. (2019). A Framework for Cyber Crime Investigation. Procedia Computer Science, 158, 287–294. https://doi.org/10.1016/j.procs.2019.09.054

Pajankar, A. (2017). Introduction to Python. Retrieved from: https://link.springer.com/chapter/10.1007/978-1-4842-2677-3_1

Panesir, M. S. (2018). Blockchain Applications for Disaster Management and National Security. ProQuest Dissertations and Theses, 115. Retrieved from https://search.proquest.com/docview/2057242991?accountid=188395

Pecoraro, G., Calvello, M., and Piciullo, L. (2019). Monitoring strategies for local landslide early warning systems. Retrieved from: https://www.researchgate.net/publication/328509222_Monitoring_strategies_for_local_landslide_early_warning_systems

Pesti, G. M., Aggrey, S. E., & Fancher, B. I. (2013). Symposium: Experimental design for poultry production and genomics research. Poultry Science, 92(9), 2487–2489. https://doi.org/10.3382/ps.2012-02733

Petersen, M. W., Ørnbøl, E., Dantoft, T. M., & Fink, P. (2021). Assessment of functional somatic disorders in epidemiological research: Self-report questionnaires versus diagnostic interviews. Journal of Psychosomatic Research, 146. https://doi.org/10.1016/j.jpsychores.2021.110491

Piedade, B., Dias, J. & Correia, F. (2022). Visual notations in container orchestrations: an empirical study with Docker Compose. Retrieved from: https://link.springer.com/article/10.1007/s10270-022-01027-8

Project, T. T. (2020). Beyond internal validity: Towards a broader understanding of credibility in development policy research. World Development, 127, 104802. https://doi.org/10.1016/j.worlddev.2019.104802

Pucken, V. B., Bodmer, M., Lovis, B., Pont, J., Savioli, G., Sousa, F. M., & Schüpbach-Regula, G. (2021). Antimicrobial consumption: Comparison of three different data collection methods. Preventive Veterinary Medicine, 186. https://doi.org/10.1016/j.prevetmed.2020.105221

Pulmano, C. E., Estuar, M. R. J. E., De Leon, M. M., Tan, H. C. L., Co, N. A. S., & Tamayo, L. P. V. (2023). Towards the Development of a Blockchain-based Decentralized Digital Credential System using Hyperledger Fabric for Participatory Governance. Procedia Computer Science, 219, 99–106. https://doi.org/10.1016/j.procs.2023.01.269

Queen, C., & Boakye, D. N. (2022). A qualitative description (QD) analysis of community-level experiences of healthcare delivery in rural, post-structural adjustment Ghana. SSM -

Qualitative Research in Health, 2(March), 100079. https://doi.org/10.1016/j.ssmqr.2022.100079

Rad, B., Bhatt, H. & Ahmad, M.(2017). An Introduction to Docker and Analysis of its Performance. Retrieved from: https://www.researchgate.net/profile/Harrison-Bhatti/publication/318816158_An_Introduction_to_Docker_and_Analysis_of_its_Performance/links/61facc0c007fb504472fd6c7/An-Introduction-to-Docker-and-Analysis-of-its-Performance.pdf

Raj Kumar Reddy, K., Gunasekaran, A., Kalpana, P., Raja Sreedharan, V., & Arvind Kumar, S. (2021). Developing a Blockchain framework for the automotive supply chain: A systematic review. Computers and Industrial Engineering, 157, 107334. https://doi.org/10.1016/j.cie.2021.107334

Rathore, N., & Rajavat, A. (2022). Scalable Edge Computing Environment Based on the Containerized Microservices and Minikube. International Journal of Software Science and Computational Intelligence, 14(1), 1–14. https://doi.org/10.4018/ijssci.312560

Reichstein, M., Camps-Valls, G., Stevens, B. et al. Deep learning and process understanding for data-driven Earth system science. Nature 566, 195–204 (2019). https://doi.org/10.1038/s41586-019-0912-1

Republic of South Africa (2021). What is South Africa's Protection of Personal Information Act (POPIA)?

Rifi, N., E. Rachkidi, N. Agoulmine and N. C. Taher, "Towards using Blockchain technology for IoT data access protection," 2017 IEEE 17th International Conference on Ubiquitous Wireless Broadband (ICUWB), Salamanca, Spain, 2017, pp. 1-5, doi: 10.1109/ICUWB.2017.8251003.

Robinson, P., Ramesh, R., & Johnson, S. (2021). Atomic Crosschain Transactions for Ethereum Private Sidechains. Blockchain: Research and Applications, 100030. https://doi.org/10.1016/j.bcra.2021.100030

Saito, H. (2021). The imaginary and epistemology of disaster preparedness: The case of Japan's nuclear safety failure. Poetics, January 2021, 101594. https://doi.org/10.1016/j.poetic.2021.101594

Saito, H., Uchiyama, S., & Teshirogi, K. (2021). Rapid vegetation recovery at landslide scars detected by multitemporal high-resolution satellite imagery at Aso volcano, Japan. Geomorphology, 398, 107989. https://doi.org/10.1016/j.geomorph.2021.107989

Saunders, M., Lewis, P., & Thornhill, A. (2012). Research Methods for Business Students (6th ed.). Pearson Education Limited.

Scarfò, A., 2018. The cyber security challenges in the IoT era. In Security and Resilience in Intelligent Data-Centric Systems and Communication Networks (pp. 53-76). Academic Press.

Schwarzer, M. (2022). Explaining and Visualizing Autoscaling Behavior of Microservice Systems Deployed on Kubernetes.

Show, (2018). A Blockchain Testbed For Dod Applications. Retrieved from: https://apps.dtic.mil/sti/pdfs/AD1065507.pdf

Singh, C., Chauhan, D., Deshmukh, S. A., Vishnu, S. S., & Walia, R. (2021). Medi-Block record: Secure data sharing using Blockchain technology. Informatics in Medicine Unlocked, 24(April), 100624. https://doi.org/10.1016/j.imu.2021.100624

Sobha, G. V, & Sridevi, P. (2019). Usecase of Blockchain in Disaster Management- A Conceptual View. Seventeenth AIMS International Conference on Management. Retrieved from http://www.aims-international.org/aims17/17ACD/PDF/A374-Final.pdfb

Sobrosa Neto, R. de C., Sobrosa Maia, J., de Silva Neiva, S., Scalia, M. D., & de Andrade Guerra, J. B. S. O. (2020). The fourth industrial revolution and the coronavirus: a new era catalyzed by a virus. Research in Globalization, 2. https://doi.org/10.1016/j.resglo.2020.100024

Stanganelli, M., (2018). Hyogo Framework for Action: An Analysis Ten Years Later and a Prospective for Future Decades. In Handbook Of Disaster Risk Reduction & Management (Pp. 499-521).

Strous, L., von Solms, S., & Zúquete, A. (2021). Security and privacy of the Internet of Things. Computers and Security, 102, 102148. https://doi.org/10.1016/j.cose.2020.102148

Sun, H., Bonetta,D., Humer, C., & Binder, W. (2018). Efficient dynamic analysis for Node.js. Retrieved from: https://dl.acm.org/doi/abs/10.1145/3178372.3179527

Sun, Y., Yan, B., Yao, Y., & Yu, J. (2021). DT-DPoS: A Delegated Proof of Stake Consensus Algorithm with Dynamic Trust. Procedia Computer Science, 187, 371–376. https://doi.org/10.1016/j.procs.2021.04.113

Swan, M. (2015). Blockchain: Blueprint for a new economy. " O'Reilly Media, Inc.".

Tang, B., Li, J., Kang, S., Wang, P., & Orlandini, L. C. (2017). PO-0807: Practical advantages of a transmission chamber in relative dosimetry of Brainlab conical applicators. Radiotherapy and Oncology, 123, S431. https://doi.org/10.1016/s0167-8140(17)31244-6

Tapscott, D., & Tapscott, A. (2016). Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World. Penguin

Tchagna Kouanou, A., Tchito Tchapga, C., Sone Ekonde, M. et al. Securing Data in an Internet of Things Network Using Blockchain Technology: Smart Home Case. SN COMPUT. SCI. 3, 167 (2022). https://doi.org/10.1007/s42979-022-01065-5

Tøge, A. G., Malmberg-Heimonen, I., Søholt, S., & Vilhjalmsdottir, S. (2022). Protocol: Feasibility study and pilot randomised trial of a multilingual support intervention to improve Norwegian language skills for adult refugees. International Journal of Educational Research, 112(August 2021). https://doi.org/10.1016/j.ijer.2022.101925

Tsuchiya, Y., & Hiramoto, N. (2021). How cryptocurrency is laundered: Case study of Coincheck hacking incident. Forensic Science International: Reports, 4, 100241. https://doi.org/10.1016/j.fsir.2021.100241

Ullo, S.L. and Sinha, G. R. (2020). Advances in Smart Environment Monitoring Systems Using IoT and Sensors. Retrieved from: https://www.mdpi.com/1424-8220/20/11/3113

United Nations Climate Change, (2017). How Blockchain Technology Could Boost Climate Action. Retrieved from: https://unfccc.int/news/how-blockchain-technology-could-boost-climate-action#:~:text=For%20example%2C%20IBM%20and%20Energy,are%20valid%20and%20settled%20automatically.

Wang, K., Dong, J., Wang, Y., & Yin, H. (2019). Securing Data with Blockchain and AI. IEEE Access, 7, 77981–77989. https://doi.org/10.1109/ACCESS.2019.2921555

Wang, L., & Wang, Y. (2022). Supply chain financial service management system based on Blockchain IoT data sharing and edge computing. Alexandria Engineering Journal, 61(1), 147–158. https://doi.org/10.1016/j.aej.2021.04.079

Wang, X., Zha, X., Ni, W., Liu, R. P., Guo, Y. J., Niu, X., & Zheng, K. (2019). Survey on Blockchain for Internet of Things. Computer Communications, 136, 10–29. https://doi.org/10.1016/j.comcom.2019.01.006

Wankhede, D., Gaikwad, V., Karnik, M., Mishra, V., Kekane, A., Kapase, S., & Bakkam, O. (2023). The Decentralized Smart Contract Certificate System Utilizing Ethereum Blockchain Technology. Procedia Computer Science, 230, 923–934. https://doi.org/10.1016/j.procs.2023.12.035

World Bank (2018). Blockchain and Emerging Digital Technologies for Enhancing Post-2020 Climate Markets. Retrieved from: https://documents1.worldbank.org/curated/en/942981521464296927/pdf/124402-WP-Blockchainandemergingdigitaltechnologiesforenhancingpostclimatemarkets-PUBLIC.pdf

Xu, M., David, J. M., & Kim, S. H. (2018). The fourth industrial revolution: Opportunities and challenges. International Journal of Financial Research, 9(2), 90–95. https://doi.org/10.5430/ijfr.v9n2p90

Yadav, A. S., Agrawal, S., & Kushwaha, D. S. (2021). Distributed Ledger Technology-based land transaction system with trusted nodes consensus mechanism. Journal of King Saud University - Computer and Information Sciences, xxxx. https://doi.org/10.1016/j.jksuci.2021.02.002

Zhou, N., Georgiou, Y., Pospieszny, M., Zhong, L., Zhou, H., Niethammer, C., Pejak, B., Marko, O., & Hoppe, D. (2021). Container orchestration on HPC systems through Kubernetes. Journal of Cloud Computing, 10(1). https://doi.org/10.1186/s13677-021-00231-z