A SMART CONTRACT APPROACH FOR CYBER THREAT INTELLIGENCE SHARING

WILSON MUIGAI MAINA

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY

JOMO KENYATTA UNIVERSITY OF AGRICULTURE AND TECHNOLOGY

2025

A Smart Contract Approach for Cyber Threat Intelligence Sharing

Wilson Muigai Maina

A Thesis Submitted in Partial Fulfilment of the Requirement for the Master of Science in Information Technology in the Jomo Kenyatta University of Agriculture and Technology

2025

DECLARATION

This thesis is my original work and has not been presented for a degree in any other University

Signature …….…….…….Date…….……

Wilson Muigai Maina

This thesis has been submitted for examination with our approval as the University Supervisors

Signature …….…….…….Date…….……

Dr. Lawrence Nderu, PhD

JKUAT, Kenya

Signature …….…….…….Date…….……

Dr. Tobias Mwalili, PhD

JKUAT, Kenya

DEDICATION

I dedicate this research to God for his grace, favour and faithfulness while doing this work. To my family, for believing in me and constant guidance and inspiration; Thank you.

ACKNOWLEDGEMENT

I wish to express my gratitude to the Almighty God for giving the inspiration, grace and determination of doing this work to the best of my ability. I am grateful to my supervisors Dr. Lawrence Nderu and Dr. Tobias Mwalili for their unfailing guidance and candid feedback that has formed and shaped this work. I would also wish to thank all my respondents for their cooperation, without whom, this piece of work would not have been possible.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

ACRONYMS AND ABBREVIATIONS

API	Application Programming Interface
APT	Advanced Persistent Threats
CA	Communications Authority of Kenya
CBK	Central Bank of Kenya
CERTs	Computer Emergency Response Teams
CIA	Confidentiality, Integrity and Availability
CII	Critical Information Infrastructures
CHIS	Covert Human Intelligence Sources
CIRT	Computer Incident Response Team
CTI	Cyber Threat Intelligence
CVE	Common Vulnerabilities and Exposures
DAM	Database Activity Monitoring tool
DNS	Domain Name Service
EMS	Electromagnetic Spectrum
EVM	Ethereum Virtual Machine
GDPR	General Data Protection Regulation
HUMINT	Human Intelligence

IMEI	International Mobile Equipment Identity
IoT	Internet of Things
IP	Internet Protocol
IRP	Incident Response Plan
IT	Information Technology
RAD	Rapid Application Development
PII	Personally Identifiable Information
PSP	Payment Service Provider
OSINT	Open Source Intelligence
SIEM	Security Information an Event Management
TECHINT	Technical Intelligence
TTPs	Tactics, Techniques, and Procedures
URL	Uniform Resource Locator
XML	Extensible Markup Language

DEFINITION OF OPERATIONAL TERMS

Cyber Threat An information technology entity, such as a host or website, which is suspected of performing attacks.

Cyber Threat Intelligence (CTI) This is any information that can help an organization identify, assess, monitor, and respond to cyber threats. Cyber threat intelligence includes indicators of compromise; tactics, techniques, and procedures used by threat actors; suggested actions to detect, contain, or prevent attacks; and the findings from the analyses of incidents (CREST, 2022). Organizations that share cyber threat information can improve their own security postures as well as those of other organizations (Johnson et al., 2016).

Computer Security Incident This is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices (Cichonski et al., 2012).

Ethereum A secure decentralised generalized transaction ledger (Wood, 2014).

IoT The interconnection of smart devices to collect data and make intelligent decisions (Panarello et al., 2018).

Smart Contract A computerised transaction protocol that executes the terms of a contract. The general objectives of smart contract design are to satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement), minimize exceptions both malicious and accidental, and minimize the need for trusted intermediaries. (Caston et al., 2016)

Threat Actor An individual or a group posing a threat (Johnson et al., 2016)

ABSTRACT

The current practice of informal cyber threat intelligence (CTI) sharing among organisations is characterized with the use of emails and social media exchanges among individuals. This model is highly subjective and dependent on a specific individual's social networks. While international cyber threat intelligence is well covered by the traditional IT tools and firewalls, there exists a knowledge gap on locally manufactured and executed malware and cybercriminal activities. Financial institutions have CTI at their disposal that could protect each other from computer hacks and fraud. The effective sharing of this intelligence among financial institutions could help reduce the high-income leakages that is brought about by cyber-attacks. The challenge is how to share this intelligence confidentially and anonymously since the financial institutions are competitors, have a huge reputation to protect and thrive on business secrecy. To solve this problem effectively, trust-based computing must be used. Ethereum is a blockchain based technology that comes with the ability to write smart contracts, small programs that sit on the blockchain. As the contracts are on the blockchain, they become immutable thus providing an alternative protocol for building decentralized applications. This research was able to achieve the sharing CTI by a developed model utilizing Ethereum smart contract blockchain technology. The blockchain private ledger, based on Ethereum, was used in this research to ensure information is only passed among the trusted financial institutions. Sharing CTI on the developed model took an average of 45 seconds, costed an average of $0.45 with anonymity guaranteed. Anonymity was achieved by introducing a layer of abstraction to protect the identity of the participating nodes or the financial institutions in the private blockchain network when passing information. This model based on contract technologies will assist in sharing CTI securely among trusted parties.

Keywords: Blockchain, Cyber Threat Intelligence, Ethereum, IoT, Smart Contract

CHAPTER ONE

INTRODUCTION

1.1 Background

The reliance on computers and information systems has given rise to the proliferation of information security threats and incidents that have significantly impacted the security of the information held by organisations. (Serianu, 2018), estimated the reported annual cost of cybercrime in Kenya to be KES. 30B with over 90% of cybercrime not reported. Locally manufactured and re-engineered malware has been on the rise that bypass the traditional firewalls. These malware strains are both targeted and lethal with cybercriminals employing attack replication across multiple organisations. Also noted by (Javaheri et al., 2024), the banking sector in Kenya is the most targeted by cybercriminals followed by the government and financial services. According to (Interpol, 2025), cost of cyber in Africa is estimated to be 3 billion dollars. Information is in silos and not formally shared between organisations. Sharing information is key in mitigating cybercrime. While cybercriminals are well organised, financed and highly skilled, critical sectors in the Kenyan economy are largely unorganised, hence getting hit.

This research strives to introduce a novel approach to sharing information, with specific interest in CTI. Our approach was designed to complement and alleviate the current weaknesses of informal and subscription-based models. This was achieved by implementing a blockchain smart contract-based system. Smart contracts have features which include immutability, decentralization and can be deployed within a private network. This research introduced a feature that ensures anonymity of participating devices by generating and utilizing a hash function to mask the identity of the mobile device, Radio Frequency Identity (RFID) or the institution passing information. Anonymity will ensure that the organisation's privacy and reputation is protected. Our research interest was primarily focused on the financial sector, which is most affected (Mohammed et al., 2023).

To test and analyse our approach, we designed a system prototype which will be based on the smart contract technology and aligned to the NIST 800-150 framework Guide to Cyber Threat Information Sharing (C. Johnson et al., 2016). According to the NIST 800-150 standard, an information sharing mechanism should establish trust between participants and define the sharing scope and rules of exchange. The developed model utilized NIST 800-150 framework (C. Johnson et al., 2016) by using blockchain technology for private network to establish trust. One of the fundamental rules of the developed prototype was only registered entities will be able to exchange CTI within the blockchain private network. The results of the prototype showed that it is possible to hide the identity of participating devices on a smart contract while exchanging intelligence. The model seeks to improve the security posture of financial institutions by leveraging the collective knowledge and experience of the cyber security community.

1.2 Problem Statement

The gravity of cyber incidents has worsened worldwide particularly targeting financial institutions. Several factors contribute to the steady rise in cyber-attacks and incidents. Firstly, financial gain by the cybercriminals. It is estimated that cybercrime rates generated $1.5 Trillion in 2018 (Müller, 2019), clearly highlighting that the advanced persistent threats (APTs) are well financed constantly looking for opportunities for illegal financial gain. World bank (Vergara Cobos et al., 2024) noted the cost of cybercrime is not only direct but affects the entire ecosystem of a business. (Vergara Cobos et al., 2024), classified the costs as either direct or indirect costs.

Another factor is the large variety and constant change in attack vectors and malware landscape.(IBM XForce Security, 2021), observed that the malware and threat landscape metamorphosed in 2019/2020 period, with threat actors going back to ransomware, data theft and botnets. The Communication Authority of Kenya (CA) detected 2,538,283,798 cyber threats between January 2025 and March 2025 and issued 13,227,909 advisories during the same period (Communication Authority of Kenya, 2025) to the affected CTI. Despite the huge number of detected threats, Kenya

cybersecurity infrastructure remains underdeveloped to disseminate actionable intelligence to various sectors (Ogunrinde & Peter, 2024).

Lastly, lack of structures to support anonymous sharing of cyber threat intelligence. While the banking sector in Kenya is the most affected by cyber incidents, banks tend to protect their reputation at all costs, thereby limiting information sharing to their peers. (Abu et al., 2018), observed that most information security service providers have come out with their own definition of CTI to suit their business and marketing strategies. Multiple definitions of CTI are due to lack of exhaustive academic literature discussing CTI between the various communities, unclear definition of CTI and absence of clear CTI sharing standards. Existing smart contract technology provides inadequate controls to ensure data is shared anonymously. (Chatziamanetoglou & Rantos, 2024), suggest the use of access control protocols to protect access to a blockchain environment. The access control feature allows for controlled exchange of specific CTI, corresponding to the need for granular control over information dissemination. However, the various users will know who has shared a specific intelligence.

1.3 Objectives of the Study

1.3.1 General Objectives

The main goal was to develop an approach that will utilize smart contract technology to share cyber threat intelligence anonymously.

1.3.2 Specific Objectives

1 To evaluate the existing mechanisms of exchange of cyber threat intelligence including their strengths and weaknesses.
2 To develop a smart contract model for CTI exchange that masks the identity of participating mobile devices and internet of things (IoT) devices.
3 To evaluate the efficiency of the developed model in anonymizing participants.

1.4 Research Questions

1 What are the existing mechanisms of exchange of cyber threat intelligence in financial institutions?
2 How will smart contract-based architecture be designed and the cyber-intelligence sharing model be developed?
3 What level of efficiency is expected for the proposed model in hiding identity of participating devices?

1.5 Justification

The system will be beneficial to the following:

The Financial Institutions. The system will provide a new and more effective way of sharing intelligence guaranteeing both the privacy and reputation of individual institutions, breaking the existing information silos. The financial institutions will minimize attack replication and financial leakages.

The Government. By adopting blockchain based CTI across various ministries, the government will be able to effectively reduce income leakages because of cyber related fraud and exposures. This in turn will have a positive impact on the economy which is currently affected substantially by income leakages.

The Researchers. Much data regarding CTI is still needed. This study has generated information on the status of cyber intelligence in the financial institutions and Kenya as a whole. The goal here is a move towards liberating the financial institutions from replicated cyber-attacks through developing approaches that enable efficiency CTI sharing.

1.6 Knowledge Contributions

While this research adopted similar methods used in related works, the main contributions are:

1. *Develop a new innovative mechanism for hiding the identity of devices when passing information in the smart contract technology*.
   Related research focused on proving the identity of nodes could be unmasked. Our research focused on masking identity on devices specifically on Internet of Things (IoT) and mobile devices. The participating IoT and mobile devices on the network were assigned new identities to mask the radio-frequency identity (RFID) and international mobile equipment identity (IMEI) and thus anonymised when contributing to the blockchain.
2. *Introduce the concept of using block chain, smart contract technology for sharing CTI Kenya.*
   While blockchain the underlying technology for smart contract was first envisioned in 2008 (Nakamoto, 2017), this technology is yet to be utilized in sharing CTI among peers in Kenya.

1.7 Scope

This research was limited to and concerned with sharing CTI in financial institutions. The limitations of the model are:

1. It does not alter the information being passed. The model assumed the information being passed is processed and actionable CTI. In mitigation we will use common vulnerabilities and exposures (CVE) database by Mitre Corporation that includes IoT vulnerabilities.
2. A significant proportion of cyber security professionals are very secretive, thus were not comfortable to respond to the survey. In mitigation the importance of study was provided to improve the sector in terms of cyber threat intelligence sharing. It was further clarified that the study was for educational purposes only and that the regulator was not involved.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

The cost of CTI has doubled, from US$5.5bn in 2019 to $11.6bn in 2021, with estimates for 2027 as high as $20.2bn (CREST, 2022). Cyber-attacks and related risks have increased both in complexity and occurrences, presenting major challenges for organisations who must protect their information and systems from these threat actors. These actors can either be individual attackers or well-financed gangs operating in a coordinated approach. Threat actors employ a variety of tactics, techniques, and procedures (TTPs) to compromise and disrupt systems, commit financial fraud or steal sensitive information. It is obligatory that organisations exchange and utilize CTI effectively to develop and enhance their security posture (Johnson et al., 2016). . From a financial sector in Kenya perspective, while cybercriminals have continued to act in a well-coordinated manner, financial institutions have continued to operate in silos and withholding CTI thereby getting hit (TransUnion, 2025). This chapter will detail the CTI concepts and structures, the different cyber-threat intelligence exchange mechanisms, with focus on their adequacy, strengths and weaknesses. (Aayush et al., 2024), noted the importance of protecting the identity of participating devices when sharing intelligence. The subsequent sections of this chapter will detail and critique all these CTI sharing methodologies and draw out their inadequacies to build up on the proposed prototype.

2.2 CTI Levels

Cyberspace domain is made up of six domains: air, land, maritime, space and the electromagnetic spectrum (EMS) exist naturally. However, cyberspace is entirely man-made and only through continued attention and maintenance that it persists. The Internet that binds cyberspace together utilizes the EMS (Bank of England, 2016).

(CREST, 2022), defines three levels of CTI, Tactical, Operational and Strategic. Tactical threat intelligence is material regarding to the techniques, tactics and

procedures (TTPs) used by threat actors. Operational threat intelligence concerns details of impending or ongoing operations against an organisation. This is typically atomic Indicators of Compromise (IOCs) for example IP addresses, hashes, hostnames, filenames which are consumed by automated security solutions. Strategic threat intelligence exists to inform executives and senior management of high-level changes in the threat landscape (Aljuhami & Bamasoud, 2021).

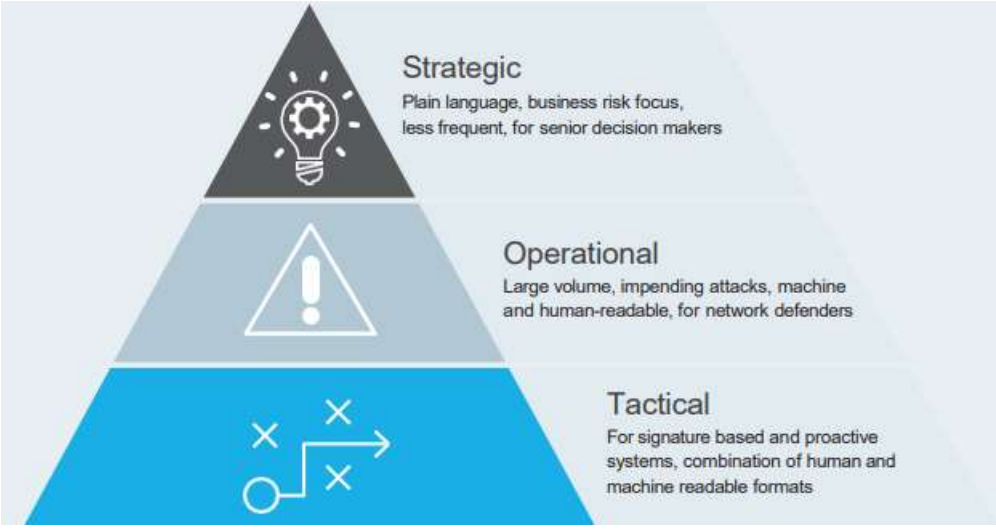


Figure 2.1: Cybersecurity Levels

Source: (CREST, 2022)

(Bank of England, 2016), defines threat as actions undertaken by an agent with the intention to weaken, undermine, deceive, or harm a target. It is important to note that a threat is a resource (person or system) that exploits a vulnerability in a target. Vulnerabilities, include software bugs or weak passwords, and is not the threat itself; the threat is a person or resource that takes advantage of vulnerabilities. To get the most out of a CTI system or platform it is essential to understand the difference between threat data, information, and intelligence. Figure 2.2 is an illustration of intelligence.

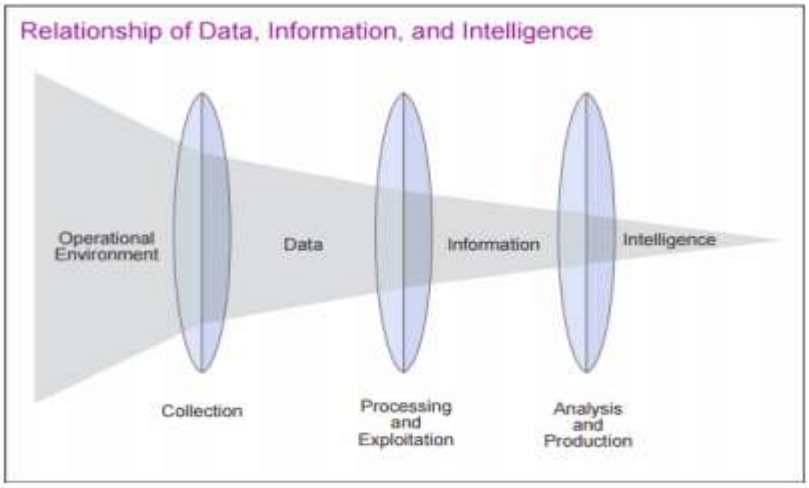


Figure 2.2: Relationship of Data, Information and Intelligence

Source: (Abu et al., 2018)

Aljuhami & Bamasoud, (2021) highlights the recommended characteristics of CTI as:

- Timely: Intelligence must be conveyed quickly.
- Accurate: Intelligence must be complete and true.
- Specific: Intelligence must be well detailed.
- Actionable: Intelligence must enable the recipient to respond.
- Relevant: CTI must be in the context of the organization.

CREST, (2022) includes CTI must also be centralized, accessible and enable continuous review. This research will focus on cyber threat intelligence.

2.2.1 CTI Types

Major types of cyber threat intelligence include the following (Johnson et al., 2016):

a) **Indicators -** Technical evidence that suggests an impending attack or an active compromise. Indicators are mostly used to identify and defend against possible threats or attacks. Examples of indicators include malicious email containing links or attachments, an Internet Protocol (IP) address of a suspected malicious device or command and control server, a device implant in the network, a

Uniform Resource Locator (URL) that points to a malicious actor, a compromised Domain Name System (DNS) or a hash for a malicious executable.

b) **Tactics, Techniques, and Procedures (TTPs) –** Information sets that describe the behavior of a malicious actor. Tactics are highest-level description of behaviour, techniques are detailed description of behaviour, and procedures are even lower-level, highly detailed description in the context of a technique (Omer Eltayeb, 2024). Examples include descriptions of an actor's tendency to use a specific IP address, operating systems, malware variant, attack tool, exploit delivery methods, order of operations (e.g., user phishing or a malicious actor conducting reconnaissance in an environment). (S. Zhang et al., 2022) suggests ATT&CK presents a curated and actionable repository of adversarial Tactics, Techniques and Procedures.

c) **Security Alerts** – Comprises of brief technical statements and notifications containing information on current exploits and vulnerabilities or other forms of security briefs. Security alerts originate from sources such as national Computer Incident Response Teams KE-CIRT/CC, commercial security vendors, security scholars and investigators (Interpol, 2025).

d) **Threat Intelligence Reports** – These are detailed documents which describe target systems, breaches, system logs, threat actors and other threat information that provides cyber situational awareness to an organisation. Threat intelligence reports may include graphical and pictorial representation of facts (Gorodenkoff, 2024).

e) **Tool Configurations -** Recommendations for hardening enterprise infrastructure. Tool configurations include specific instructions and guides to install and configure systems or how to include firewall rules, intrusion detection signatures, intelligent switch access lists, or network access controller configuration rules and other forms of configuration guidelines (S. Zhang et al., 2022).

2.2.2 CTI Sources

CTI gathers information about potential cyber hazards from a variety of data sources (Omer Eltayeb, 2024). (CREST, 2022) notes that even though most sources are technically open, it requires technical capability to consume the intelligence.

a) Internal Sources: includes output from a security information and event management (SIEM) tool, database activity monitoring tool (DAM), output from an endpoint detection and response (EDR) tool, firewall logs and other logs covering system or network events provide a vital data and information source.
b) Atomic indicators of compromise (IoCs): are typically delivered in feeds consisting of malicious domain names, IP addresses (hosts) and hashes of malware samples associated with malicious campaigns (CREST, 2022).
c) Messaging platforms and social media: Includes tools like Telegram, WhatsApp and emails. The more private the platform the higher the adoption. These platforms are also usually used by cybercriminals to engage and create communities (CREST, 2022).
d) Deep Web and Dark Web: Deep Web is part of the web that index-based search engines cannot access. Researchers estimate this part at more than 90% of the entire web. Dark Web is part of the Deep Web that uses tools to hide users' identities. Software such as Onion Router (TOR) and Invisible Internet Project (I2P). Researchers suggest dark web is the primary platform for cyber-criminal activities (Basheer & Alkhatib, 2021).
e) Vulnerability feeds and exploit databases: CTI programmes increasingly assess the implications of CVEs (common vulnerabilities and exposures) as they are released, to understand the potential implications for consumers. (Laszka et al., 2023), suggests the use of MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) framework to analyse the applicability of CTI. (S. Zhang et al., 2022) proposed a model that uses ATT&CK to assess CTI reports automatically to extract Indicators of Compromise (IoC) in a timely manner. Common Vulnerabilities and Exposures (CVEs) can be linked

to specific exploitation strategies and then mapped to ATT&CK techniques (Laszka et al., 2023).

f) Government publications: The role of computer emergency response teams (CERTs), intelligence agencies and national cyber security bodies is to respond to incidents and aggregating activity across multiple sectors and to provide visibility into nation-state activity. The National KE-CIRT/CC is mandated to provide reports on Cyber Threat Landscape ((Communication Authority of Kenya, 2025)

Baraniuk & Marszałek (2024) categorized CTI sources as either open source, proprietary or classified source.

CREST (2022) suggests CTI sources can either be standalone deliverables or continued threat monitoring service, the latter is more sustainable.

2.2.3 CTI Actors

While this research focused on the financial sector, however the financial sector does not exist in isolation, it needs other players in the economy as well. There is a huge variety of threat actors each with specific interests, perspectives, and needs. On the other hand, organisations view resource value in different ways which as a result greatly influence the formation of any information exchange or community (gorodenkoff, 2024). It is also worth noting that threat actors have varying degrees of technical proficiency, risk appetites and diverse motivations. Given the huge divergence in backgrounds of those involved, discovering and meeting the unique needs and requirements is a precondition for building trust (Goodwin et al., 2015).

a) **Government –** Governments have cyber security duties that include the need to defend their own information and systems, fight cybercrime within and outside its borders though diplomacy, and help in mitigating the cybersecurity risk to its all citizens and residents (Communication Authority of Kenya, 2025).

According to (Mucheru, 2016), the Kenyan Government will continuously review and implement the Cyber Security Strategy and develop relevant legislation to achieve the cyber security policy objectives. The Kenyan government has recognised cyber security as one of the key pillars of national security. As cyber security is a shared responsibility the ICT ministry will continue to foster a multi-agency approach in the management of national cyber security to promote trust and confidence in the cyber-spatial dimension of the battlespace of today and the future.

In the financial sector, the Payment Service Providers (PSPs) should notify the Central Bank of Kenya within 24 hours period of any significant cybersecurity incident(s) that could have adverse impact on the PSP's service delivery. (Central Bank of Kenya, 2018).

b) **Private Critical Infrastructure** - Although the protection of critical information infrastructure (CII) is often in the private sector hands, its security is essential to the government's goal of safeguarding such critical national interests as food security, financial stability, public education, health and transport.

   One of the key objectives of private organisations is maintaining the security of sensitive information, such as personally identifiable information (PII), trade secrets and other intellectual property (gorodenkoff, 2024).

   While the computer misuse and cybercrime act 2018 has mandated the national computer and cybercrime coordination committee to designate critical systems as critical infrastructure, but it is no doubt that interruption of a banking system will result to a disruption in the money market in Kenya (The Republic of Kenya, 2018).

c) **IT Companies** - Businesses selling IT products have an interest in and the responsibility of preserving the confidentiality, integrity and availability (CIA) of their installations. Established IT companies frequently share software updates to their customers, or information on discovered vulnerabilities in their products so that security organisations or communities can design and implement relevant solutions to remedy the vulnerabilities (IBM, 2025). Also

closely related to IT companies are security firms, such as endpoint security and firewall vendors. IT security vendors gather and sell cybersecurity intelligence to those in their network or ecosystem.

IT companies provide a good and reliable source for CTI for financial institutions.

d) **Security Researchers** – There are several security researchers and research firms that have been established to meet the demand for cyber security services (Sailio et al., 2020). They basically track malicious actors, malicious programs and targeted attack campaigns, in order to discover vulnerabilities in software, hardware, and services through academic work, business, or voluntary individual or collaborative efforts. They may choose to either notify relevant responders to help mitigate threats and remedy weaknesses or report their findings publicly. Examples of these companies include IBM, Serianu Limited and Anomali.

2.2.4 CTI Sharing Scope

CTI can take multiple dimensions; information exchange initiatives rely on people or devices to actively exchange intelligence with their counterparts.

a) **Sectorial** – Also known as sector Computer Incident Response Team (CIRT). These are organisations in each sector like finance coming together to form a standard and mechanism to exchange CTI. Sector-specific intelligence sharing has become a popular means of information exchange for critical information infrastructure providers. This research thesis will focus on the financial sector.
b) **National –**Also known as federal scope covers the exchange of CTI within a countries' boarders. The Kenya Information and Communications Act, 1998, has mandated the Communications Authority of Kenya (CA) to establish national cyber security management frameworks through the formation of a national CIRT (Communication Authority of Kenya, 2025).
c) **International** – With the advent of the internet and the push towards globalization, cyber-threats are often global in scope and nature, so it is prudent for information exchange participants to share information across borders

(Sailio et al., 2020). For governments, sharing free intelligence can be difficult since passing sensitive or classified information normally only takes place with reference to diplomatic ties and arrangements. As a result, efforts intended at establishment of international exchange programs that include governments have made little progress. For organisations with international presence, these exchanges have proved to be quite helpful in curbing cyber threats in multiple countries. Establishing exchange programs on sectorial level, local organisations will benefit from such arrangements.

2.3 NIST 800-150 CTI Mechanisms of Exchange

According to National Institute of Standards and Technology (NIST) guide to cyber threat information sharing, NIST 800-150, one of the major challenges of sharing CTI is establishing trust and safeguarding sensitive information. Intelligence sharing is a vital component in the enabling of security coordination across organisations. As guided NIST 800-150 (C. S. Johnson et al., 2016), the first task is establishing CTI exchange relationship, identify sources of intelligence, establishing scope and providing for CTI sharing privacy. Every organisation should have in place an incident response plan (IRP) and perform periodic intelligence sharing throughout the incident response life cycle. It is prudent not wait until an incident has been fully resolved before sharing details of it with peers (Nelson et al., 2025).

An incident is a matter of when, not if a compromise or attack to an organisation's security will happen. The preparation of the computer incident response team (CIRT) through planning, documentation, communication, and periodic simulation of the incident response process will provide the necessary experience needed should an incident occur within an organisation (Kral, 2020). The different stages of an IRP are highlighted in figure 2.1.

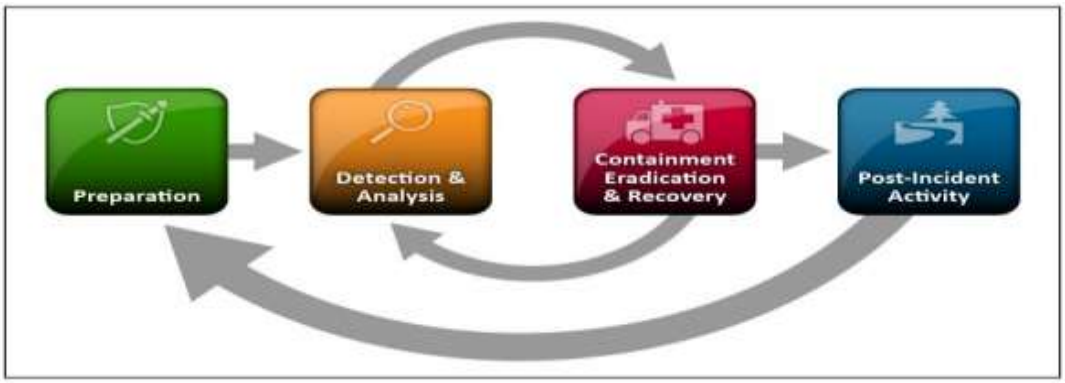


Figure 2.3: Incident Response Life Cycle

Source: (Nelson et al., 2025)

Collaboration for CTI among different organisations is established in the preparation stage, while CTI is normally shared in the detection and post-incident activity stages of the incident response life cycle. Collaboration with peers in incident management would enable an organisation to respond to the incident more efficiently than an organisation operating in seclusion.

One of the most critical features of IRP coordination is the exchange of incidents. Incident information sharing is most of the time beneficial to all because threats and attacks often replicated across organisations or may affect multiple organisations simultaneously (Nelson et al., 2025).

It is equally important for organisations to identify internal sources of CTI, without which there will be knowledge gaps and no CTI to share (Courage Ojo et al., 2024). The process begins at conducting an inventory of all internal threat information sources such as firewall, security information an event management (SIEM) and database activity monitoring tools (DAM). After inventory identification and development of use cases an organisation will better identify knowledge gaps (Courage Ojo et al., 2024). The process of identifying internal threat information sources includes the following steps (Johnson et al., 2016):

- Identify systems, devices, sensors, feeds, and other sources that generate threat information, and confirm that the information is produced is relevant and can support cybersecurity decision making.
- Identify threat information that is currently collected and analysed as part of the organisation's continuous monitoring strategy. This will enable classification of CTI according to the organisations CTI labeling standards and disseminating to peers.

Incident response plan cyber threat intelligence sharing approach is heavily reliant of the specific organisations' strategy, culture, and leadership (Nelson et al., 2025). It is critical for every institution to have a well elaborate incident response plan with specific clauses with sharing intelligence with peers. Institutional incident response plans form the building blocks for a cyber-threat intelligence community.

2.3.1 Simple Alerts

Most cyber threat intelligence (CTI) exchange mechanisms have traditionally occurred through casual methods, such as email, text messages, and phone calls. Simple alert CTI exchange approach is heavily dependent on individual employee's links with partner organisations (CREST, 2022). In case of staff attrition, these connections are lost impacting the entire incident response arrangements. Organisations should attempt to formalise its CTI sharing strategies with partner organisations and work towards automating the CTI sharing mechanisms (Omer Eltayeb, 2024).

2.3.2 Detailed Reports

Detailed reports CTI exchange comprises narratives enriched with tables, numbers, graphics and multimedia. Financial institutions are highly regulated globally and as such, it is at the best interest for any regulator to have visibility in the financial institutions under its jurisdiction(Courage Ojo et al., 2024). The theft of USD 81 million by cyber criminals from the central bank of Bangladesh prompted the Society for Worldwide Interbank Financial Telecommunication (SWIFT) to call for tighter antifraud controls and more collaboration among its over 11,000 members. The attempt for the cyber criminals was to get away with USD 1 billion (KPMG, 2016).

This incident had a ripple effect in the financial institutions in Kenya. The CBK has formulated two guidelines after this incident that requires mandatory reporting of cyber incidents within twenty-four hours and on a quarterly basis (Central Bank of Kenya, 2018).

The detailed reports CTI exchange mechanism is normally required by governmental institutions and regulators. This mechanism of exchange however tends to be a monolog communication where intelligence is sent to the government bodies or regulators and very little is shared to the community.

Technology used for detailed report exchange mechanism is largely email.

2.3.3 Secure Online Portals

Secure online portals CTI exchange mechanisms have been adopted by Computer Incident Response Teams (CIRTS) in the form of providing a way for reporting an incident (Omer Eltayeb, 2024). However, private companies provide on-demand access to an always-current threat intelligence database and a range of analytical functions that could be as basic as from simple queries to more complex data mining (Courage Ojo et al., 2024).

As this exchange model has been adopted by most Computer Incident Response Teams (CIRTS), who are largely consumers of CTI, but are also producers of CTI from their internal sources to a certain extent. CIRTs may share CTI with the other parties in the community using the established CTI sharing infrastructure (Fransen et al., 2015).

In Kenya the Communication Authority established a national Computer Incident Response Team (KE-CIRT) (Communication Authority of Kenya, 2025) that allows the public to report incidents using an online portal. National CIRTs are mostly utilized for incidents that require diplomatic approaches and are tasked with providing incident prevention and/or interdiction, threat mitigation, and incident coordination and management at a national level (DHS, 2016).

The technology used for secure online portals are mostly web-based application languages with cloud infrastructure as the preferred hosting environment.

2.3.4 Machine-Readable CTI

The effectiveness of CTI depends on the ability to overcome challenges, such as the dynamic nature of cyber threats. This requires continuous improvement and adaptation of detection strategies, which complicates the distinction between real threats and false positives (Santos et al., 2025). Machine-readable CTI takes the form of a direct data feed from automated intrusion detection systems which contrasts with CTI that takes the default form of written or verbal narrative (Bank of England, 2016). Beside these traditional countermeasures already discussed, there is an observable trend to increasingly exchange CTI between trusted organisations to aid the management of threats and vulnerabilities to mitigate incidents. To support these efforts, several standards have been developed to enable the automated exchange of CTI (Sauerwein et al., 2017). (Salem et al., 2024) suggests the use of Artificial Intelligence (AI) in cybersecurity is increasingly critical due to its capacity to analyze vast amounts of data rapidly, detect patterns, and identify potential threats with high efficiency. Integrating cyber threat intelligence (CTI) into organizational security infrastructure has become essential as cyber threats evolve and increase in complexity (Santos et al., 2025).

a) **Managed Incident Lightweight Exchange (MILE)** – Focus is development of standards for exchanging incident data. The MILE work group has developed a format to define indicators and incidents and standards for exchanging CTI.
b) **Open Indicators of Compromise (OpenIOC)** – It was first implemented by Mandiant but was later released as an open standard. The initial intent for developing OpenIOC was for sharing CTI. Its definitions are written in extensible markup language (XML).
c) **Vocabulary for Event Recording and Incident Sharing (VERIS)** – It was first released by Verizon in March of 2010. VERIS is a standard for defining and sharing incident information. The collected CTI is then incorporated and used as a larger data set for analysis and reporting. Big data storage technology is used with intent to provide strategic information and an aggregate view of incidents.

d) **Mitre Standards** – There are three main standards for Mitre on CTI (Laszka et al., 2023).
    i. Cyber Observable eXpression (CybOX) is a standard for defining indicator details known as observables.
    ii. Structured threat Information Expression (STIX) is a standard to define patterns of observables.
    iii. Trusted Automated eXchange of Indicator Information (TAXII) is a standard to exchange CTI.

Other researchers suggest the combination of two or more framework to manage CTI. (Simonetto & Bosch, 2024)recommends mapping CVEs to MITRE standards. (Georgiadou et al., 2021) suggest MITRE ATT&CK for Enterprise and ICS (Industrial Control Systems) model as a broader and more holistic approach. What is common on machine readable implementation is the client/server architecture employed. Most of these implementations include a server component which collects data from various feeds and stores CTI data then access is granted to client devices who are given access based on each organisation selection criteria.

2.4 Smart Contract Approaches

Blockchain development can be compared to the early phases of the internet emergence with elaborate prospects of the impending disruption across all industries particularly the financial sector, should the technology be well adopted. Public blockchain could hypothetically be compared to the internet, where organisations could exchange information with anybody who has access to a service provider in the case of blockchain a wallet provider. While private blockchain can be compared to organisations intranet pages, where data and information is only exchanged internally with those who have been authorized to access the site and in the case of private blockchain an authorized node within the blockchain network (Piscini & Kehoe, 2018). Blockchain is a distributed digital ledger used to record and share information through a peer-to-peer network (Miguel et al., 2022)

2.4.1 Overview of Ethereum

Ethereum is the largest public blockchain by usage (Béres et al., 2020). Bitcoin is the original blockchain entity for providing decentralized system and allowing peer to peer exchange of value, there are many research articles that provide details on Bitcoin history. Ethereum came from the idea that blockchain could be used for many more functions other than the exchange of value or financial transactions (Pradhan & Biswas, 2025). Ethereum can be defined as a secure decentralised generalized transaction ledger (Miguel et al., 2022). To digest the above definition, Ethereum is an open-source, distributed computing platform, featuring smart contract functionality to build decentralized applications on top of this platform and a smart contact is a computerised transaction protocol that executes the terms of a contract (Caston et al., 2016). Ethereum is currently the most popular technology that implements smart contract transaction protocol. Ethereum has evolved into a decentralized realm for crafting smart contracts and decentralized applications (Dapps) occupying the space of decentralized finance (DeFi) (Cosimo Lan et al., 2023).To answer the question why Ethereum was developed while Bitcoin already existed, below is a table that highlights the differences.

Table 2.1: Differences between Bitcoin and Ethereum

	Bitcoin	**Ethereum**
Concept	Digital money	World computer
Cryptocurrency Token	Bitcoin cash	Ether
Scripting Language	Turing incomplete – can solve limited computational problems by design.	Turing complete – can solve any computational problem by itself, given enough resources.
Consensus Algorithm	SHA256	Ethash
Coin Release Method	Early mining	Through initial coin offering
Average Block Time	~10 minutes	~12-15 seconds

A common contract-oriented high-level language that implements smart contracts on Ethereum Virtual Machine (EVM) is known as Solidity. The Solidity syntax is very similar to JavaScript.

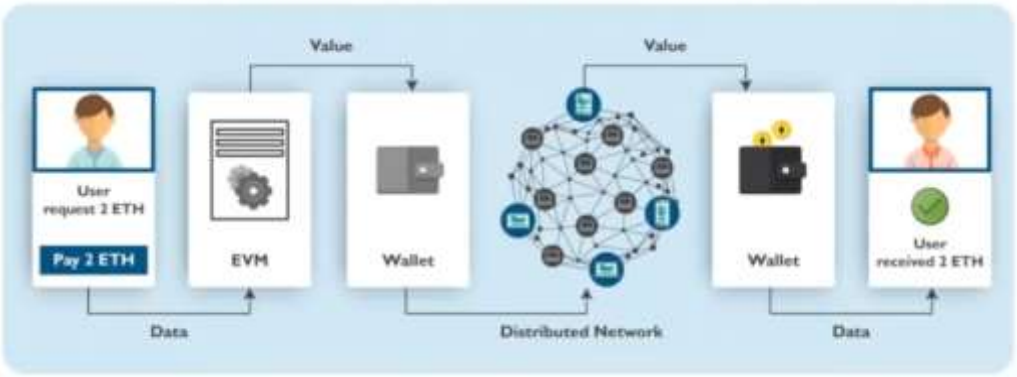
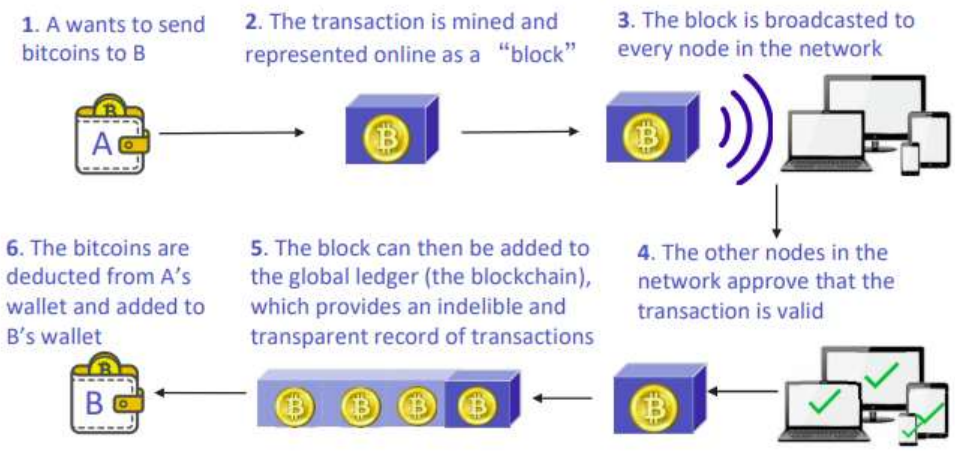


Figure 2.4: Execution at EVM

Source: (Cosimo Lan et al., 2023)

Contracts written in a high-level programming language like Solidity are compiled into immutable byte code to allow the EVM to read and execute.

Each node in the network has EVM to execute the codes and maintain the blockchain, a paradigm called consensus computing where all network nodes deterministic execute the contract using their copy of EVM to reach the same final state (McCorry et al., 2017). To prevent a piece of code from running for eternity or continuous loop, users pay an execution fee called gas as a reward for the miners/ owners of the nodes in the network for running EVM and maintaining chronological order of transactions in the blockchain network.



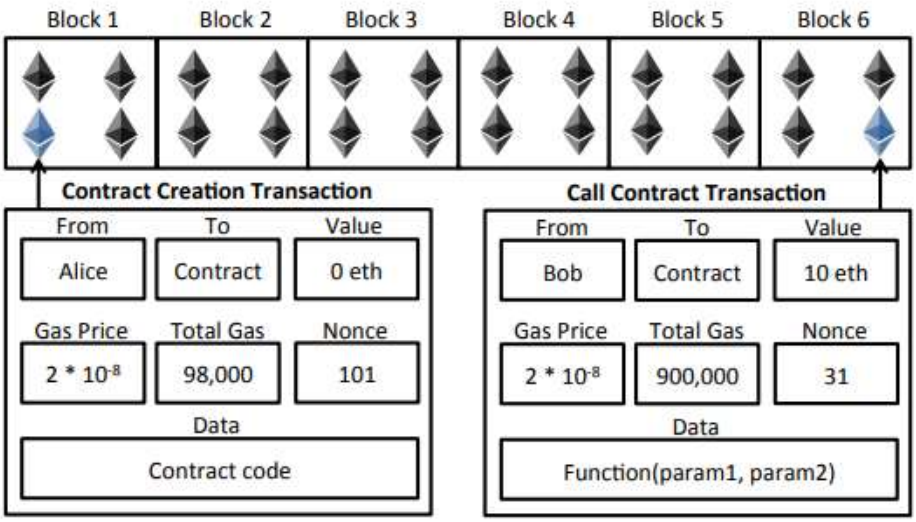


Figure 2.5: Example of a Smart Contract Execution

Source: (McCorry et al., 2017)

On contract creation transaction example, Alice creates a transaction in the blockchain, which includes Alice's address, address of the recipient, the value is the amount of Ether to be sent, if there is no exchange of value the input is 0. It also includes the execution fee in form of gas and the smart contract code (McCorry et al., 2017).

The Eth2 upgrade endeavors to augment scalability, security, and energy efficiency, thereby amplifying its prowess as a robust blockchain platform (Cosimo Lan et al., 2023). Ethereum characteristics have been highlighted by (David Friday Isie, 2023)

a) **Immutability and Transparency:** After creating and confirming a block it cannot be reversed (David Friday Isie, 2023).
b) **Auditability and data integrity:** Any transaction in the Blockchain network is traceable to its previous transaction (Miguel et al., 2022).
c) **Smart Contract**: Blockchain fulfills the terms of a contract (Miguel et al., 2022).
d) **Security:** The implementation of the blockchain network uses a private or public key to access or make transactions (Miguel et al., 2022).

2.4.2 Blockchain Architectures

a) **Public Permission-less Blockchain**, commonly implemented in crypto currencies, where anyone can read, write or participate in the blockchain. The transactions are transparent but with participants using pseudo-anonymity (David Friday Isie, 2023).
b) **Public Permissioned Blockchain**, a concept introduced by the Sovrin Foundation (Tobin & Reed, 2017), as an architecture of blockchain that only permits an elected group of participants to write in the ledger and perform consensus, while remains open for the public to read.
c) **Private Permissioned Blockchain**, where the participating nodes must be granted access to the network, via an invitation or registration, in order to perform various operations over the distributed ledger or participate in consensus. This architecture calls for specific agreements to be in place (David Friday Isie, 2023). Contents of the agreement usually include specification of the access control mechanism, an entry regulatory authority and a dispute resolution consortium (Felix Albrektson & Max Bergstrom, 2022).

Our research will focus on private permissioned blockchain architecture where participating nodes are already known.

2.4.3 Emerging Concerns around Smart Contract Technology

Zhang et al. (2019), noted very few efforts have been made to provide an in-depth analysis of the security and privacy properties of blockchain and different blockchain implementation techniques

a) Regulations (Privacy Concern) – With the emergence of international and national regulations around confidentiality and privacy of data smart contract implementations should take these laws into consideration (David Friday Isie, 2023). For instance the General Data Protection Regulation (GDPR) requires that the processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level

of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data, and the security of the related services offered by, or accessible via, those networks and systems, by public authorities, by computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), by providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the data controller concerned. This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communication systems (Kaiafas, 2020).

b) **Privacy Issues –** There has been raised privacy concerns around user anonymity, confidentiality and privacy control in their transactions on the ledger. These privacy issues rise concerns in citizens and companies that are still a bit wary to adopt blockchain in their processes and businesses, as it might imply sharing (even if encrypted and/or anonymised) in a public accessible database their data and transactions. Although the usage of pseudonyms avoids linking transactions to the real identity, users are not totally anonymous in their movements, since all usages behind these pseudonyms might be traceable and linkable, especially when handling multiple-entries transactions with several addresses from various accounts belonging to the same user (Felix Albrektson & Max Bergstrom, 2022).

2.5 Anonymity in Blockchain

We have reviewed that the emerging concern around blockchain is maintaining anonymity of participating users. We have also noted the current implementation provides public keys as pseudo-identities as Ethereum accounts. However, previous work has shown that it is difficult to maintain anonymity in the context of online services and networked data.

Crandall et al. (2010) did a research on Flickr users and came to the conclusion that individuals who choose to reveal some details of their public information on locations and time of their activities may be inadvertently exposing their social ties. (Narayanan & Shmatikov, 2009) developed a generic re-identification and successfully used to de-anonymize several thousand Twitter users using Flickr as the source of auxiliary information with 30.8% accuracy, at a time when the relationship of the two was relatively minor. Their research pointed to the important role of auxiliary information in de-anonymizing identities. Auxiliary information relating to personally identifiable information (PII). According to (Reid & Harrigan, 2011), the dependence on public key for anonymity can be illustrated by WikiLeaks providing an online mechanism for anonymous donations through one-time public-key. Reid & Harrigan, (2011), came to the conclusion that it is difficult to maintain anonymity on networked devices as publicly announced addresses, can be used to link identities and organizations to some transactions and recommended the use of Tor browser for anonymity.

In a university simulation of Bitcoin for daily transactions, (Androulaki et al., 2012) found out that measures adopted by Bitcoin are not sufficient to protect the identity of users. The experiment was able to positively identity 40%, a population of 200 Bitcoin users who took part in the simulation and made recommendation for Bitcoin to allow multi-input and multi-output transactions transparently. However, the identity of participating parties in the transaction will be known.

In a research done by (Biryukov & Pustogarov, 2015), they noted the increase of usage of Tor as an anonymizer in blockchain transactions. Their research was able to show an attacker through man-in-the-middle attack can figure-print users and learn their IP addresses. The researchers also proposed a technique for uniquely identifying Bitcoin users by targeting the nodes that they connect to, also known as entry nodes. By pairing connections to entry nodes, the researchers were able to disclose IP address information of clients located behind address translation with an accuracy of 11 – 60%, pairing an otherwise anonymous Bitcoin address with an internal IP address.

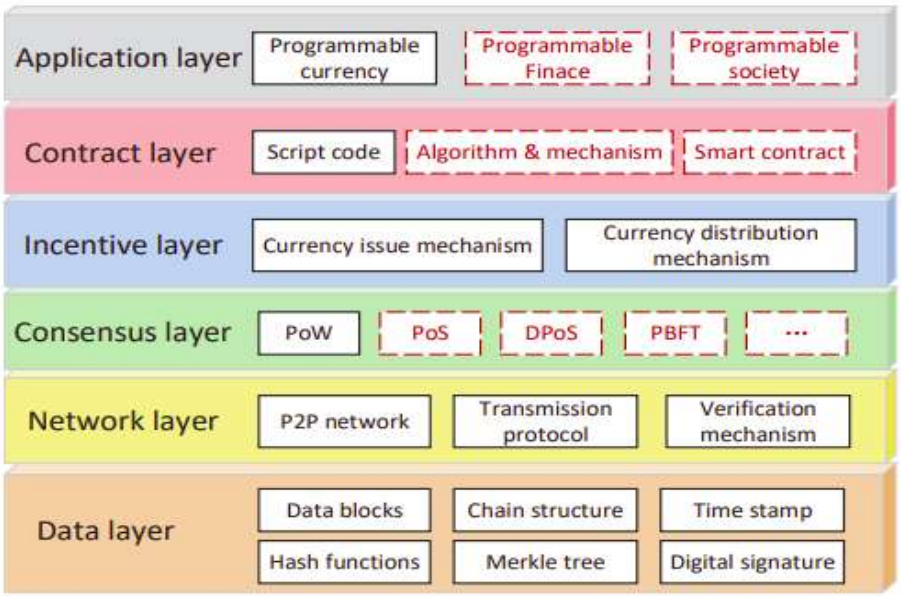


Figure 2.6: Blockchain Architecture

Source: (Zhang et al., 2019)

The figure 2.6. shows the architecture of Blockchain, where the contents of the dotted were developed by Blockchain 2.0. The network layer where the transmission protocol resides contains some auxiliary information including IP addresses. Further, digital currency wallet and other end user node service providers required users to register, thereby collecting datasets that can be used to uniquely identify individual or institution.

(Zhang et al., 2019), discussed unlinkability as the inability of stating the relation between two observed entities of the system with high confidence. Anonymity refers to the state of being unidentified. The research further stated that though the general Blockchain offers pseudonymity if fails to offer unlinkability. Further although multiple blockchain implementations encourage users to use multiple addresses during transactions, users can be linked by simple statistical analysis of the addresses used in transactions on the blockchain. Alternatively, one can link multiple addresses that originate from a single IP address. (Zhang et al., 2019) research concludes that blockchain technologies should be enhanced.

(Allouche et al., 2021) proposed Trusted Anonymous Data Exchange that requires the role of registrars, a trusted third party responsible for anonymizing the identity of the organisations on the network, among other actions. Trust focus on scalability of the network with a bottom-up network structure utilising existing threat intelligence exchange protocols such as structured threat information expression (STIX). However, a trusted third party for anonymizing intelligence shared in the network will create bottlenecks and additional costs of watching the watchers.

(Chatziamanetoglou & Rantos, 2024), suggest the use of access control protocols to protect access to a blockchain environment. The access control feature allows for controlled exchange of specific CTI, corresponding to the need for granular control over information dissemination. However, the various users will know who has shared a specific intelligence.

Most of the available solutions only touch on the application layer like the coin mixing approach, a user wishing to enhance her privacy sends her "initial" crypto coins to a trusted party, who in turn will send back "clean" coins after some time. A study on Ethereum peer to peer network revealed that full nodes and wallet providers can de-anonymise regular users and light clients already on the network layer (Béres et al., 2020). While there exist challenges in anonymizing IP addresses, there exists a gap on anonymizing portable device's identity. Example International Mobile Equipment Identity (IMEI) is a unique mobile device identifier that can uniquely identity a mobile device and ultimately the owner of that mobile device.

2.6 Blockchain for IoT in Finance

The Internet of Things (IoT) refers to the interconnection of smart devices to collect data and make intelligent decisions. The question if blockchain has other uses other than exchange of currency resulted to the development of Ethereum. More recently there has been deliberate efforts to decentralize and improve security around the use of IoT. (Conoscenti et al., 2016), explored the uses of blockchain for IoT and highlights a number of uses revolving around data storage including tamper-proof log of events and management of access control to data and registry of assets and inventory.

In a research done by (Khanboubi et al., 2019) and (Suseendran et al., 2020) on uses of IoT in banks, they documented some uses as highlighted below:

- RFID tags can be installed on debit and credit cards, with RFID readers installed on mobile devices, when a transaction is initiated with the RFID reader out of site, an alert is generated.
- Account management on things allows users to access banking account from any digital surface.
- Real time monitoring of collaterals and assets.
- Wallet of Things - a device that can store money without the need for a bank account and make payments directly to any payment terminals.
- Assets and inventory can be tagged with RFID tags, and activate alerts when tampered with.
- Intrusion detection can be configured with IoT infrastructure to generate alert if intrusion is detected.

In a research done by (Panarello et al., 2018), the paper categorized IoT usage into seven main categories. These include generic application, smart homes, smart cities, smart property, smart energy, smart manufacturing and data market place to illustrate the wide usage of IoT. (El Jaouhari et al., 2024) further noted any sensor that has the ability to transmit data and has an easy way to get regular data readings (e.g. through an API) can be used in a data marketplace. Device ID being the mandatory field and others are optional depending on usage.

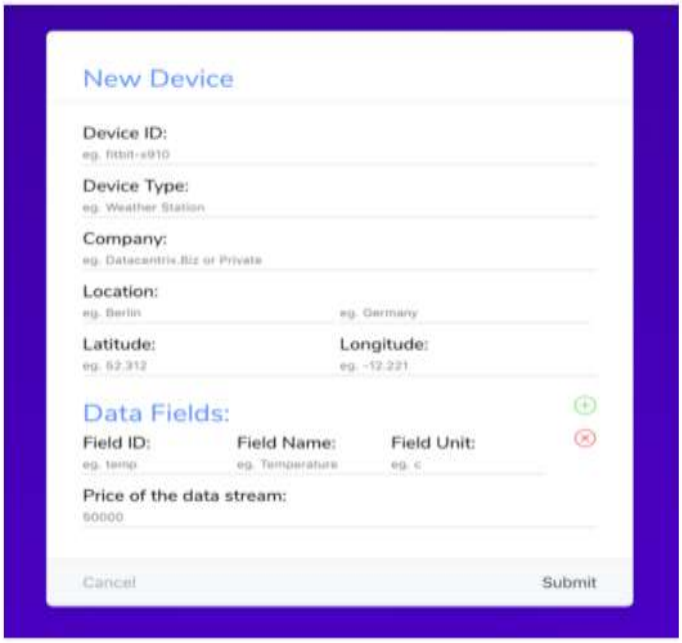


Figure 2.7: Sample Data Form Transmitted by an IoT Device

El Jaouhari et al. (2024) proposed Cyber Threat Intelligence for IoT (CTIoT), which aims to automate the collection, analysis and representation of CTI data related to an IoT system. The proposed solution also allows active monitoring of publicly available CTI information related the IoT devices present in each smart space. However, the issue of anonymity has not been tackled. (El Jaouhari et al., 2024) suggests that Common Vulnerabilities and Exposures (CVEs) are an important source of CTI. (Jin et al., 2024), suggests CVEs should be used together with Structured Threat

Information eXpression (STIX), a a de facto standard CTI format. While CVE will identify a vulnerability, STIX will elaborate how that vulnerability is being exploited in a real-world attack. When identifying vulnerabilities on CVEs: Name, Status, Description, References, Report Phase and Comments parameters should be included.

2.7 Strengths and Weaknesses of CTI Mechanisms of Exchange

Table 2.2: Strengths and Weaknesses of CTI Mechanisms of Exchange

CTI Exchange Mechanism	Weaknesses/ Critical review
Simple Alerts	• Simple alerts methods are informal and heavily reliant of personal (Omer Eltayeb, 2024). • The results are inconsistent and un-scalable (CREST, 2022).
Detailed Reports	• Detailed reports require many manual tasks make the user the bottleneck. As these reports usually include graphs and detailed information, it is highly dependent on employee morale (Courage Ojo et al., 2024). • Detailed reports are subject to misinterpretation because of lack of a standard defines the semantics for information elements (ENISA, 2014).
Secure Online Portals	• Secure online platforms focus on data collection instead of analysis and tend to be monologue. While numerous reporting is done, intelligence dissemination may require extra effort (Omer Eltayeb, 2024).
Machine-readable Cyber Threat Intelligence	• The major challenge in machine-readable CTI exchange approaches is that there is no common definition of threat intelligence sharing platforms (Santos et al., 2025). • The majority of machine-readable CTI exchange platforms is closed source. There are numerous vendors and each with their own standards (Sauerwein et al., 2017). • Trust issues between users and platform providers are mostly neglected. Since organizations may share private or sensitive information it is necessary to establish a trust-bond between organizations and the provider of said threat intelligence sharing platform (Salem et al., 2024).
Smart Contracts	• In private smart contract implementations, the participating nodes addresses (IP address/device identifiers) are already known and this limits anonymous cyber threat intelligence sharing (Miguel et al., 2022).

2.8 Existing Gaps

From the literature reviewed, it was noted that there exist limited studies on the implementation of smart contract technology for use of cyber threat intelligence sharing with scanty information provided for enhancing anonymity of participating nodes. Gaps are also identified in providing a mechanism for anonymity where participating nodes are IoT or mobile devices. Furthermore, it was noted that most of the studies focused on developing standards appropriate to the sharing of cyber threat intelligence.

2.9 Summary

El Jaouhari et al. (2024), research proposed CTIoT a solution that aggregates CTI for IOT from different security feeds for prediction purposes. The work of (El Jaouhari et al., 2024) was considered in this research in utilizing the Common Vulnerability and Exposures (CVE) structure.

Zhang et al. (2019) research was considered, as the paper suggested pseudonymity is not unlinkability, as pseudo identities can be linked together, pseudonymity if fails to offer unlinkability. This research builds on (Zhang et al., 2019) to create a model that ensures anonymity.

The works of (Allouche et al., 2021), suggesting the use of a mechanism to anonymize users sharing intelligence was considered in this research. Our research improved on this research by eliminating the role of registers to avoid the introduction of bottlenecks in the network.

(Chatziamanetoglou & Rantos, 2024), suggesting the use of access was considered. This research built on access control and introduced anonymity during intelligence sharing.

The proposed model will utilize Remix as the integrated development environment for smart contracts. The model will utilize off chain oracle to ensure device identities are hidden.

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Introduction

This chapter provides a discussion and illustration of specific areas that depict the research methodology used in this study. It emphasizes on the steps that were followed during the actual research. These include what data that was be collected, how it was collected, the experiments that were conducted, tools used for the experiment, and how data was extracted and analysed. The chapter includes the following areas: Research design, data collection methods, reliability and validity, research procedure, testing and validation, and finally data analysis.

3.2 Research Design

This was applied research and used quantitative methods to examine the relationships between variables. In this study the researcher also adopted a descriptive survey design. This research design provided a general blueprint for the collection, measurement and analysis of data, with the pivotal goal of solving the research problem (Creswell, 2012). This research has specifically deployed cross-sectional survey to gather information from cyber security specialists from financial institutions in Kenya. These relationships were analyzed and represented mathematically by using statistical analysis. The defining advantages of this design are that it takes place at a single point in time, it does not involve manipulating variables, it allows researchers to look at numerous variables at once (cost, anonymity, time) and is often used to look at the prevalence of phenomenon in each population (Creswell, 2012). This includes the research plan, from the comprehensive research questions to the final operational application and analysis of discovered data. The methodology prescriptively attempts to provide a solution to the problem of cyber threat intelligence sharing between trusted parties in a secure and anonymous approach. This research proposed to address the knowledge gaps identified during literature review and implement a smart contract transaction protocol for cyber threat intelligence exchange. This research implemented an architecture of smart contract technology and proposes upgrades to ensure anonymity of

participating IoT and mobile nodes while writing to the smart contract to address the privacy concerns.

3.3 Target Population and Sampling Procedure

All the items under consideration in any field of inquiry constitute a population. An enumeration of all the items in the population is also called a census inquiry (Kothari, 2004). As at the time of conducting this research there were 43 licensed commercial banks and mortgage finance institutions with 39 being operational (Central Bank of Kenya, 2020).

An unbiased sample is one in which the under-estimators offset the over-estimators. Increasing the sample size can reduce systematic variance as a cause of error. However, even the large size won't reduce error if the list from which you draw your participants is biased (Cooper & Schindler, 2014). Researchers accept that no sample will fully represent its population in all respects. However, to interpret the findings of research, we need a measure of how closely the sample represents the population. According to (Glenn D. Israel, 2003), the level of precision sometimes called sampling error, is the range in which the true value of the population is estimated to be. This value is expressed in percentage points. The confidence level is encompassed in the central limit theorem, when a population is repeatedly sampled, the average value of the attributes obtained by those samples is equal to the true population value. Equation (1) demonstrates computation of desired sample size. N represents population and e represents precision.

$$n = \frac{N}{1 + N(e)^2} \quad \text{..... (1)}$$

For this research we used 5% precision or error rate and a 95% confidence level. 36 samples were collected from the population from the 39 licensed banks.

3.4 Data Collection Methods

The type of data used in the research study was from two main sources: primary data collected through a questionnaire and interviews; and secondary sources, mainly, from published reports and available regulator records. Review of such works was useful in cross-checking and authenticating the primary data. To ensure dependability of data collected a pilot study was done to determine whether the respondents understood the questions correctly and where the questions did not seem clear enough, the necessary adjustments were made. 10 pre-test questionnaires were used in this research. This was applied research and used quantitative methods to examine the relationships between variables. The questionnaire was distributed to different members of financial institutions in the cyber security area of expertise. The questionnaire contains both open ended questions as well as close ended questions. These relationships were analysed and represented scientifically by using statistical analysis. The findings gathered from this research approach formed the basis to develop the smart cyber threat intelligence exchange prototype.

3.4.1 Questionnaires and Interviews

The questionnaires were administered before developing the prototype to understand the user perspective of the current problem under research. The researcher preferred the online questionnaires due to their convenience.

The individual conducting the interview needs a fuller understanding of the dilemma and how the insights will be used (Cooper & Schindler, 2014). The interviewed offered a better way of understanding the current process and different perspectives of what needs to be done to solve the current problem of cyber threat intelligence exchange which were taken into consideration in the prototype.

3.4.2 Instrumentation

The data collection instrument employed captured quantitative data. Primary data was collected using multiple choice questions employing a five-point Likert, specifically agreement scale type of rating with choices into two nominal categories (agree and

disagree). This instrument was quite relevant in this study as it sought to assess attitudes and perceptions of the cybersecurity experts towards exchanging cyber threat intelligence. The numerical scale helps to minimize the subjectivity and make it possible to use quantitative analyses. The questionnaire contained two sections: The first section required background information of the cybersecurity professionals while the second section addressed technical questions related to medium of exchange for cyber threat intelligence sharing.

3.4.3 Simulation Data Collection Methods

The input data for the simulation environment was extracted from an open-source library the Common Vulnerabilities and Exposures (CVE) by Mitre institute.

The research used the kill chain approach where the modus operandi of the today's sophisticated advanced persistent threat (APT) was used.

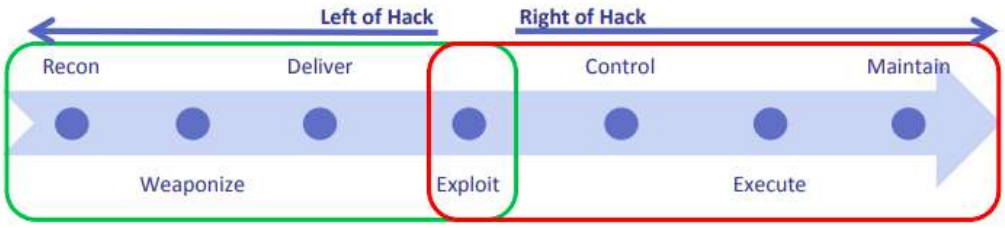


Figure 3.1: Kill Chain Simulation

Source: (Barnum, 2014)

Where the CTI will focus on attack prevention and early detection. Responding to incidents after the exploit has already occurred is very costly, both in the effective impact and in the level of effort necessary to root out the adversary's established foothold. Thus the data source to be valid must provide intelligence that can be utilized prior to the control phase of the kill chain life cycle. The choice of using the CVE structure was advised by the framework of CVE being modular and scalable architecture to ensure comprehensive vulnerability management and seamless integration with existing security infrastructures (Reddy Vaka, 2025). The importance of CVE extends beyond vulnerability identification; it serves as an integral part of

vulnerability management programs, threat intelligence sharing, and security automation CVE extends beyond mere identification; it serves as a cornerstone for vulnerability management programs, threat intelligence sharing, and security automation.

3.5 Pilot Study

To standardize the instrument, it was subjected to validity and reliability checks by pilot testing it among 10 financial institutions, drawn proportionately from the various categories. This sample is above the 10% of the actual sample size as recommended by (Tiberious et al., 2016).

3.6 Reliability and Validity

The proposed research solution checked for reliability and validity of the outcome. Reliability is the degree to which a research instrument and method yields consistent results after repeated trials (Cooper et al., 2011). It refers to the consistency of the research and the extent to which the study can be replicated. Therefore, prototype was done in different environments in terms of operating systems and devices. Further the prototype was evaluated by the interviewees and one of the questionnaire questions confirmed reliability from their perspective. 61% strongly agreed that they would use the system to exchange intelligence. 29% agreed the system is reliable to cyber threat intelligence exchange. 5% remained neutral and 5% disagreed on the reliability of the prototype.

3.7 System Development Methodology

The system development methodology involved an experimental process that includes smart contract modelling and simulation of anonymous message passing in a peer-peer environment.

For the development of the prototype the various stages of development will have a corresponding test plan that were simultaneously be created (Mudassar & Khan, 2023).

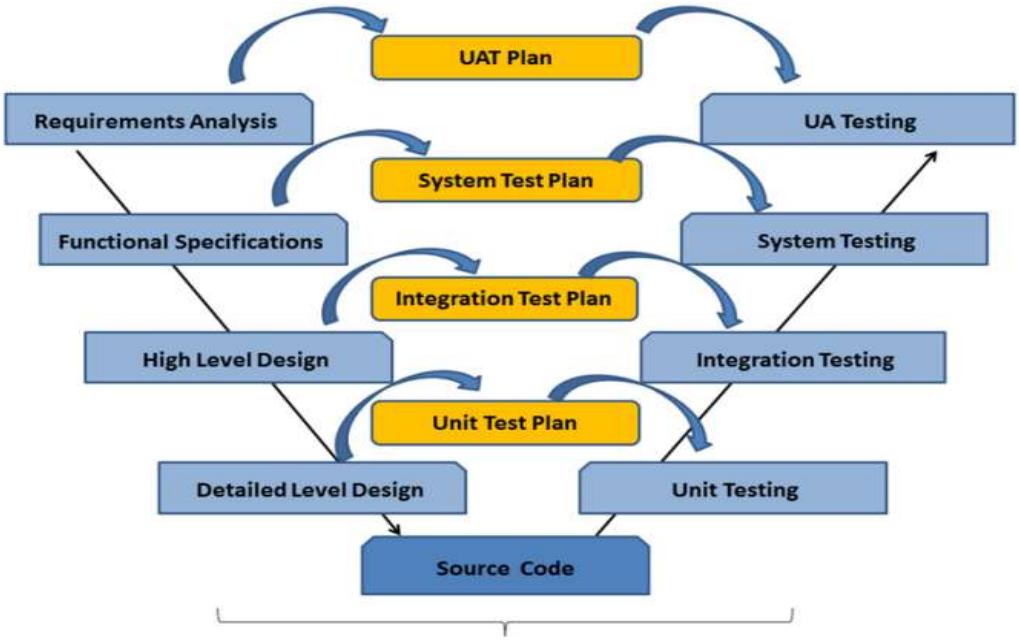


Figure 3.2: V-Process Model Approach

Source: (Mudassar & Khan, 2023)

Specific procedure that will be followed in the research as follows:

a) Business Requirements

This phase concentrations are on understanding the objective and what is needed to form a business perspective, then applying the knowledge to develop a solution that meets the objective of the research

b) The High-level Design

The high-level design provided an overview of the solution, platform, system, product and process. The high-level design guided the research to create an integration test plan that would aim to test the different component's ability to work together.

c) The Low-level Design

At the low-level design phase, actual software components are designed. The actual logic for each component of the system was defined. In this phase, the class diagram

was created detailing all the methods and relation between the classes comes. Simultaneously, the component tests were performed.

d) Coding and Implementation

At the coding and implementation phase, the system build, and coding was done.

The development of the smart contract based cyber threat intelligence sharing system contain the following features:

i. Formulation of data to be passed to the blockchain based on CVE standard.
ii. Write the data to the blockchain.
iii. Recording and logging the reaction of the blockchain.
iv. Confirming the output of the testing regime.

Described below are the tools and programming languages that will be utilised to develop the smart contract CTI system:

1. Solidity programming language – contract oriented, high-level language for implementing smart contracts on Ethereum Virtual Machine (EVM).
2. Solidity compilers and an Integrated Development Environment (IDE)
3. Blockchain hosting environments

3.8 Testing and Validation

3.8.1 Functional Testing

Functional testing is a software testing methodology used within software development where the software is tested to ensure that it conforms to all the required functionality that is specified within its functional requirements of the project.

Described below are the tests that will be undertaken in functionality testing:

1. Installation and deployment the smart contacts
2. Test the logic of the smart contract by compilation
3. Check the monitoring and logging functions of the smart contract

4. Test the logic of the solidity code for adequacy
5. Verify CTI is passed anonymously

3.8.2 Non-Functional Testing

Non-Functional testing checks the performance, reliability and other non-functional characteristics of the software system. Non-functional testing will be done after the functional testing.

1. Check the performance of the deployed blockchain smart contract
2. Check read write rights to the deployed smart contract
3. Confirm integrity of the smart contract

After the smart contract blockchain is developed, validate whether the blockchain solves the problem stated.

3.8.3 Data Analysis

Results analysis was done to evaluate the results of the research, the effectiveness of the data source selected and the efficiency and effectiveness of the developed prototype to share CTI anonymously, to ensure that this research meets the research objectives. This entailed organizing the collected data and further breaking them down into smaller, easily understood parts. The Quantitative data collected was analyzed using Microsoft Excel since it allows a useful number of statistical analysis functionalities. The findings/ information of this research was presented using these tools

I. Tables - Significant variables are summarized by Tables
II. Pie Charts – To present the results of the quantitative data in a visual format and facilitate correlations and comparisons within the data.

3.9 Ethical Considerations

High ethical standards were applied in the research. Permission was sought from both the university and the National Commission for Science Technology and Innovation (NACOSTI) to collect data from relevant experts. The welfare of the participants in

the studies and also the organizations to which they belong, their clients and their colleagues was taken into careful consideration. Permission was sought from the respondents to participate in the study and the data gathered was treated with a high degree of confidentiality. The received data was used for the sole purpose of this research.

3.10 Framework for CTI Sharing

The model is proposing an Internet of Things devices IoT implementation with a reader that connects to a blockchain. The model also consists of an Ethereum Virtual Machine (EVM) and Blockchain. The data source is the IoT's RFID reader, the EVM does the data processing where smart contracts written in solidity language get executed and stored in a blockchain. To best of my knowledge, this is the first solution proposing IoT and specifically RFID and device ID anonymization for cyber threat intelligence sharing

In a research done by (Khanboubi et al., 2019) and (Suseendran et al., 2020) some uses are highlighted below:

- Account management on things allows users to access banking accounts from any digital surface.
- Real time monitoring of collaterals via assets tagging.
- Intrusion detection can be configured with IoT infrastructure to generate alert if intrusion is detected.

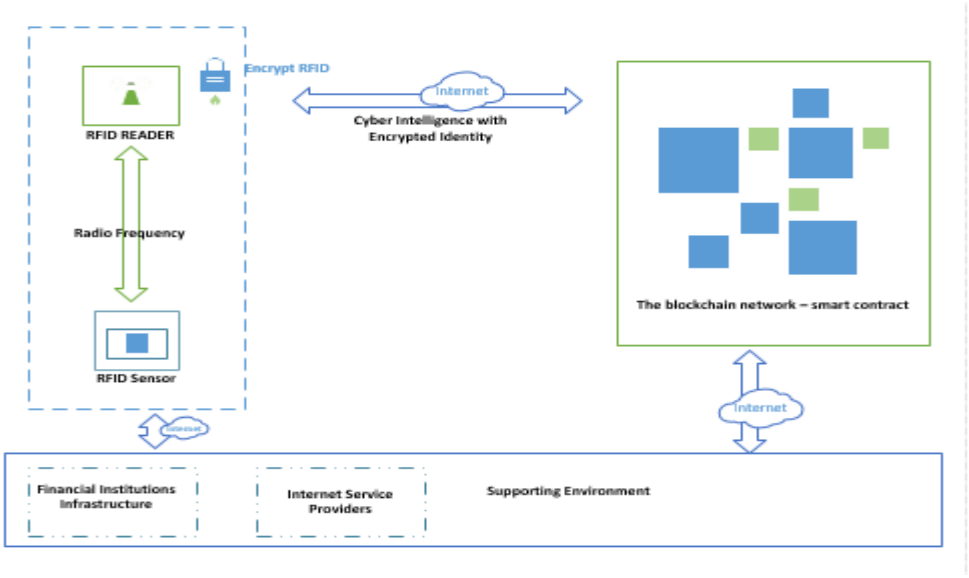


Figure 3.3: Smart Contract Framework for CTI Sharing

The smart contract architecture for cyber threat intelligence sharing over IoT devices as shown in figure 3.3 The model comprises of a decentralized application (DApp) as the front-end interface to be used by cyber security professionals. This will be hosted at the RFID reader. Model also includes external infrastructure for connectivity and the blockchain for data storage.

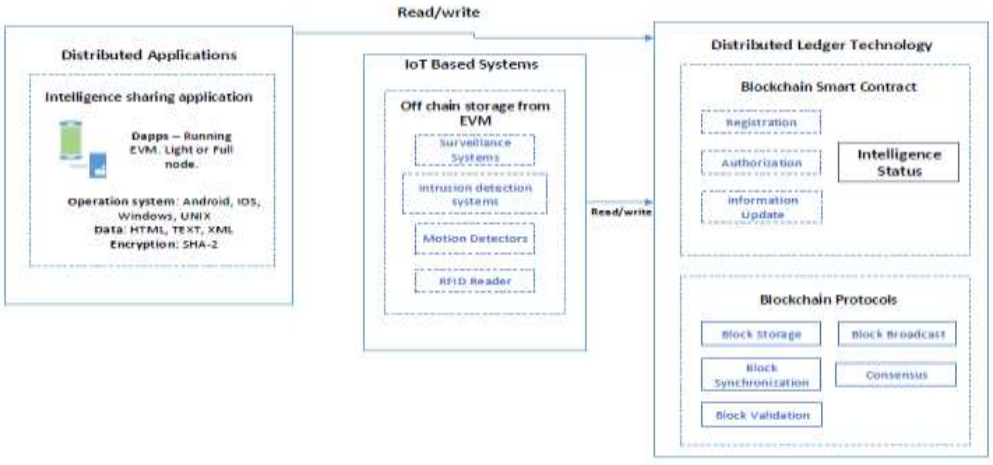


Figure 3.4: System Components and Protocols

Figure 3.4 highlights the different components and protocols in the model ecosystem. The distributed application was the interaction point with the model users; in our model this was the RFID reader. The model required storage of offline data that is application specific and blockchain storage which will utilize the blockchain protocols. The model hosted 3 smart contracts registration.sol, update.sol and notification.sol to achieve a cyber-intelligence awareness status.

3.11 Model Implementation

The smart contract approach to cyber intelligence utilizes a web interface, middleware and blockchain for storage.

The web interface was developed by ReactJS as they are most used to connect Ethereum through Web3.js was used to establish connection to the test network. ReactJS makes it painless to create interactive user interfaces. React syntax is similar to Javascript. Web3.js is a collection of libraries that allow you to interact with a local or remote ethereum node. Remix Integrated Development Environment bundles all these features together.

Solidity language was used for the development of smart contracts, which is the main language on Ethereum. Solidity is an object-oriented, high-level language for implementing smart contracts. Smart contracts are programs which govern the behaviour of accounts within the Ethereum state. Solidity is a curly-bracket language. It is influenced by C++, Python and JavaScript, and is designed to target the Ethereum Virtual Machine (EVM).

The model utilized Ropsten and Kovan Test Net, which are used for testing blockchain environment maintained by Ethereum. An important advantage on evaluating the solution in Ropsten and Kovan is that no financial investments are required, as both Ropsten and Kovan provide a faucet to request Ethers to this testing network.

The model was implemented on a high-performance laptop (intel core i7 vPro) using Remix IDE utilizing javascript and reactJS, Metamask for connecting to the blockchain test network utilizing web3js and Ropsten test network. The simulation

involved three node addresses on the same computer. Remix programing language was used to develop smart contracts.

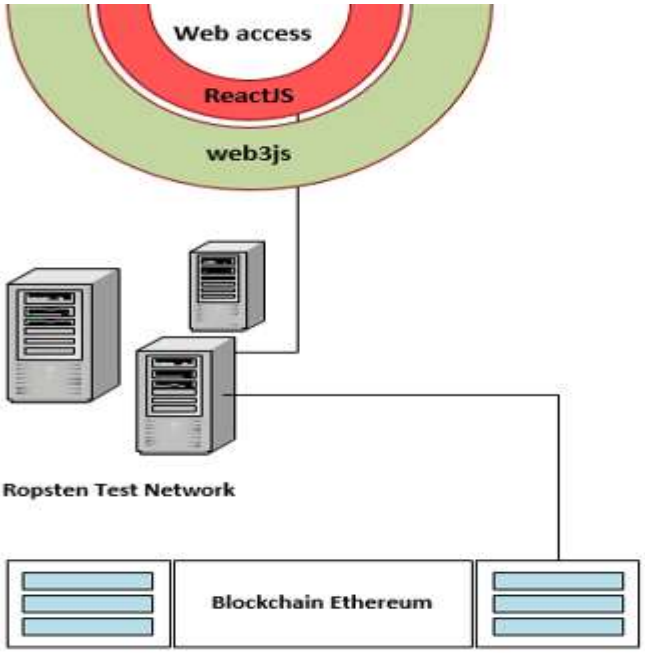


Figure 3.5: Test Environment Architecture

3.12 Smart Contracts Developed

a) Registration Smart Contract

At registration, no information will be collected except the generation of both public and private key pair by the application, which is done on the device.

b) Share Intelligence Smart Contract

The intel.sol smart contract pushes information onto the blockchain from the RFID receiver after initial registration. Includes code to mask the device ID for the RFID or the serial Number.

c) Notification Smart Contract

The notification.sol smart contract is the contract that will be configured on a device available to the participants that can mark if the intelligence was useful or not. This can also be called intelligence status.

3.12.1 Sequence Diagram

Sequence diagram shows an elaborated flow for a specific use case or even just part of a specific use case. Tells how objects interact with each other i.e. how messages are being sent and receive between objects. A sequence diagram has two dimensions: The vertical axis shows time and the horizontal axis shows the objects.

Figure 3.5 shows the activities of a user initiating a smart contract transaction. The connections between two objects are shown by an arrow along with communication messages. The vertical line shows the lifeline of the object. The user sends a smart contract transaction request which gets executed at the EVM and written on the smart contract.

IoT nodes will send intelligence to the blockchain and notifications will be broadcasted to the registered financial institutions. Users will be able to view the blockchain for cyber intelligence.

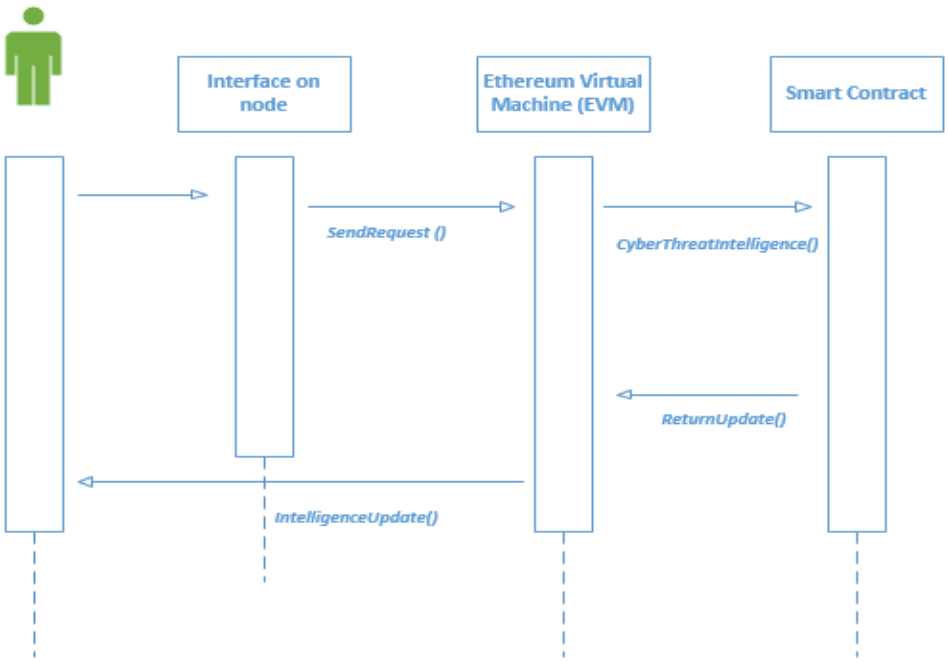


Figure 3.6: Sequence Diagram

CHAPTER FOUR

RESEARCH RESULTS AND DISCUSSION

4.1 Introduction

This chapter is organized into various parts including demographic information of the respondents; age, level of formal education, area of specialization and experience of the cybersecurity professionals in financial institutions, cross tabulations of the respondents' characteristics with the independent variables results and discussion. The research data was collected using both questionnaires and interview questions to broaden the scope and diversity of responses. The various themes and results are presented in the form of frequency tables and pie charts while analyses involving testing of research objectives are presented.

4.2 Response Rate

The study sampled 38 cybersecurity professionals drawn from financial institutions. Out of these 36 cybersecurity professionals responded to the survey. This this indicates 94.75% response rate. Among the main reasons that can be attributed to this high response rate is that most cybersecurity professionals have common social groupings, in social media platforms. In addition, the researcher is also a cybersecurity profession in a financial institution and is therefore quite familiar with the professionals in the cybersecurity field.

4.3 Pilot Study

The pilot study sort opinions and answers to the below 3 questions apart from having an interview session with the respondents, mapping to question 1, 2 and 6 of Appendix II:

1. Cyber security incidents and breaches are replicated across organizations when there are information sharing gaps or existing mechanisms are ineffective.
2. It is easy to establish if cyber threat intelligence sharing mechanisms are effective, provided they are in-place; and

3. If a proper system based cyber threat intelligence exchange is implemented, it would make the financial institutions more effective and efficient in addressing cyber threats.

4.3.1 Cyber Security Incidents Replication Across Organizations

As illustrated in Figure 4.1, 86% of the respondents (cybersecurity professionals in financial institutions) strongly agreed that cyber incidents are replicated across institutions when information sharing mechanisms are inadequate. 14% of the respondents strongly disagreed that inadequate mechanisms result to cyber incidents but other factors were the major cause.

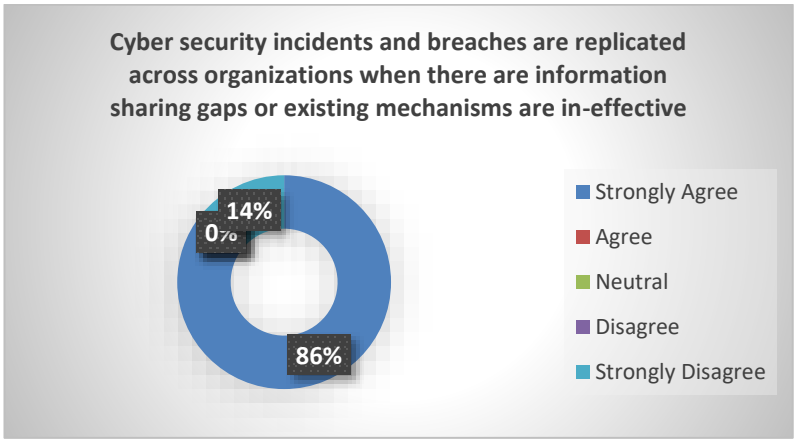


Figure 4.1: Cyber security Incidents and Breaches Replication

4.3.2 Measure of CTI Mechanisms Effectiveness

43% of the responded strongly agreed that it is easy to measure effectiveness of cyber threat intelligence mechanisms. Another 43% were also in agreement. 14% disagreed that it is not easy to measure the effectiveness of cyber threat intelligence sharing mechanisms.

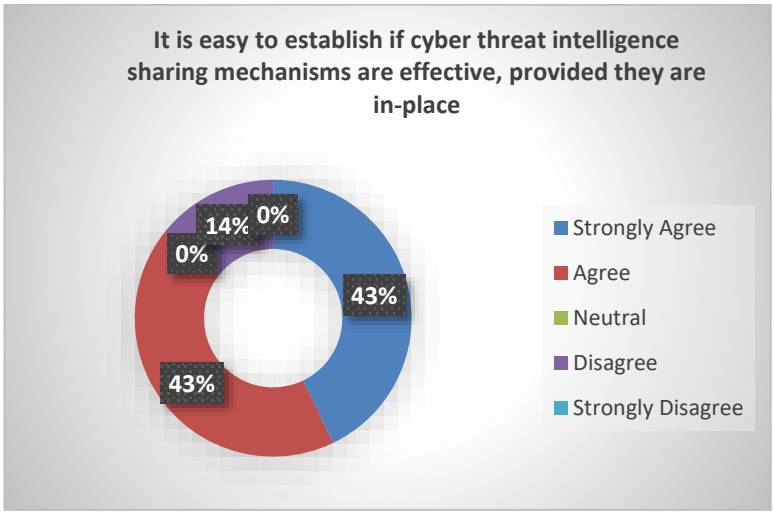


Figure 4.2: Measure of Cyber Threat Intelligence Effectiveness

4.3.3 Need for a New Mechanism or System for CTI Sharing

On the need of a new cyber threat intelligence sharing mechanism, 71% strongly agreed that a proper system based cyber intelligence exchange mechanism will result to efficient and effective approach of addressing cyber threats. 29% agreed to the need of a proper system-based mechanism for cyber threat intelligence sharing. This is shown in Figure 4.3

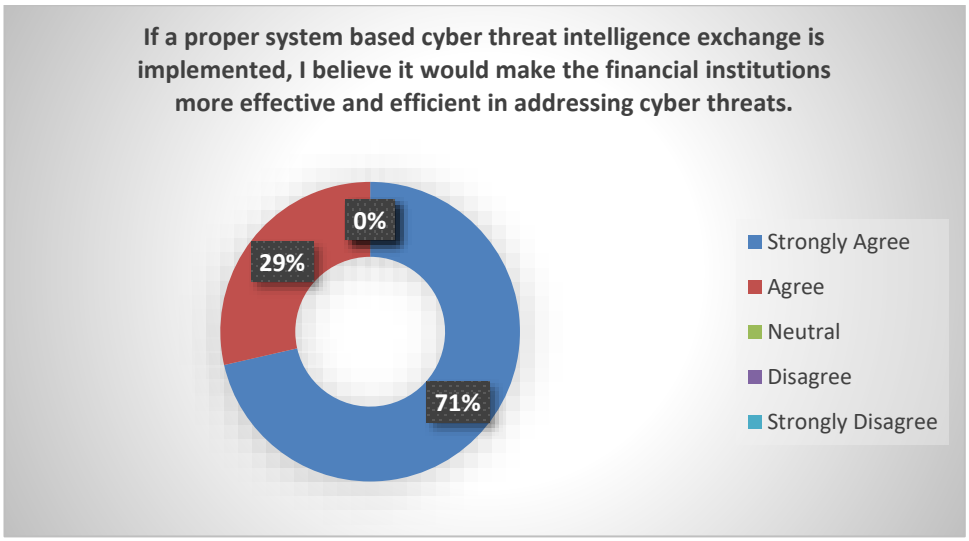


Figure 4.3: Need for a New Mechanism or System for CTI Sharing

4.4 Demographic Characteristics of the Respondents

This evaluates the background information of the respondents based on their gender, age, level of management, duration in the company, department of working as well as their respondents' highest level of education.

4.4.1 Gender Distribution

Table 4.1: Gender Distribution

Gender	Frequency	Percentage (%)
Male	27	75
Female	9	25
Total	36	**100**

The survey targeted 38 respondents in Kenya and out of these 36 or 94.75% responded. A notable phenomenon was that the cybersecurity sector is male dominated. The gender of the respondent was determined. Majority of the respondents were male (75%) while the rest 25% were female as shown in the Table 4.2 above. This is attributed to the technicality experienced in this sector. Since majority of the responses in this study relies on perceptual measures of the respondents, this gender distribution is expected to accommodate the views and opinions of both sides of the gender divide. Nevertheless, the balance in gender may be evidence of successful efforts by the various gender mainstreaming campaigns. In a research done by (Serianu, 2018) in 2018 estimated there are approximately 1,700 certified cyber professionals in the country based on numbers from various certification bodies including ISACA and (ISC)2. Research shows women make up to 20% of cybersecurity professionals, with Serianu Limited estimating a much lower figure of 10% in Africa. Various initiatives targeting women to the cyber security field have been promoted, the percentage is expected to change in the near future (ISACA, 2019) with various programs already taking root, like She Leads Tech by ISACA.

4.4.2 Age

Table 4.2: Age

Age	Frequency	Percentage (%)
Up to 24 years	2	5.6
25-34 years	18	50
35-44 years	15	41.6
45-54 years	1	2.8
Above 55 years	0	0
Total	**36**	**100**

The age category of the respondents was determined. Majority of the respondents were between 25-34 years of age at 50%, followed by others between 35-44 years of age at 41.6% while those below 24 years 5.6% and those between 45-54 years were 2.8% as shown in the Table 4.2 above. This implies that the financial institutions and majorly in the Information Technology and Risk and Compliance Departments most employees are between the ages of 25-44 years and this is a relatively young generation. This is attributed to the ever-changing dynamics in the technological advancements. The young are more flexible to accommodate change and as such, they are the ones charged with the responsibility of ensuring intelligence sharing to optimise on the benefits of accurate information sharing to reduce cyber threat. According to a survey conducted by International Information System Security Certification Consortium (ISC)2, a majority of cybersecurity professions fall within the millennials age group between the ages of 25 and 40 ((ISC)2, 2020).

4.4.3 Qualifications

Table 4.3: Qualifications

Level of Education	Frequency	Percentage (%)
KCSE	0	0
Certificate	0	0
Diploma	2	5.6
Bachelor's Degree	22	61.1
Postgraduate Degree	12	33.3
Total	**36**	**100**

The Level of Education of the respondents was determined. Majority of the respondents had a bachelor's degree at 61.1%, followed by those with Postgraduate Degree at 33.3% and Diploma holders came in at 5.6% as indicated in the Table 4.3 above. This implies that the financial institutions and majorly in the Information Technology and Risk and Compliance Departments most employees are well learned and trained to be able to handle the complex Cyber Threats which keep reappearing in diverse ways. They are knowledgeable and hence, well placed to share Intelligence where it is needed to ensure that all players in the financial industry are aware of the recent cyber-attacks and have put in place suitable measures to avoid future reoccurrence of such attacks. Also global survey by ((ISC)2, 2020), a majority of cybersecurity professions are either bachelor's or master's degree holders.

4.4.4 Job Group Level

Table 4.4: Job Group Level

Job Level	Frequency	Percentage (%)
Lower Management	11	30.5
Middle Management	20	55.6
Senior Management	5	13.9
Total	**36**	**100**

The Job Level of the respondents was determined. The Lower Management were at 30.5%, the Middle Management at 55.6% and the Senior Management at 13.9% as indicated in the Table 4.4 above. This infers that among the respondents who are in the Information Technology and Risk and Compliance Departments, most are in the Middle Level Management category; they are best suited to break down the strategies and measures placed on curbing cyber security to weekly, monthly, quarterly strategies. The senior management are responsible for developing these strategies while the Lower Management are responsible for implementation of the strategies and measures. This ensures that the whole organisation is actively involved in Intelligence sharing. In Kenya, (Serianu, 2018) observed a skill gap in high level management or the c-suite executives. Further (ISACA, 2019) observed a challenge among cyber security professionals in interpreting and communicating in line with business objectives.

4.4.5 Length of Stay in the Organisation

Table 4.5: Length of Stay in the Organisation

Length of stay in the firm	Frequency	Percentage (%)
Less than 5 years	22	61.1
6-10 years	7	19.4
11-15 years	7	19.4
More than 16 years	0	0
Total	**36**	**100**

The Length of stay of the respondents in their organisations was determined. Most of the respondents had stayed in their current firms for less than 5 years at 61.1%, others had been there for 6-10 years at 19.4% while those who had been there for 11-15 years accounted for 19.4% as evidenced in the Table 4.5 above. This infers that the ICT and Risk and Compliance Departments had relatively more employees who were new to the organisation. This finding may be attributed to the volatility of the market with new talent be sourced by the most competitive organisations. Most employees leave one financial institution to join another in the same industry either to allow them growth and develop themselves, for better pay or even for opportunities for mentoring and coaching. As they go form one firm to another, they also transfer cyber intelligence across the industry to minimise cyber threats. According to (ISACA, 2019), retaining cybersecurity professionals is exceptionally difficult. With better financial incentives, flexible working hours and lower stress levels as some of the factors that result to the high staff attrition rates in organisations.

4.4.6 Department

Table 4.6: Departments

Department	Frequency	Percentage (%)
Risk and Compliance	19	52.7
ICT Operations	12	33.3
Managed Security Services	3	8.3
Audit	2	5.6
Total	**36**	**100**

The Departments of the respondents was determined. Most of the respondents were in the Risk and Compliance Department at 52.7%, followed by those in the ICT operations Departments at 33.3%, Managed Security Services at 8.3% and Audit Department at 5.6% as shown in the Table 4.6 above. This suggests that Cyber Threat and Intelligence sharing is mainly performed by the Risk and Compliance Department who are expected to come up with mechanisms to create awareness and ensure that cyber threats are minimised in the organisation. The IT and Audit Departments too support this by ensuring safe and restricted access to the financial information through the use of password and compliance through verification of the access details respectively. This is to reduce any negative effects to the financial institutions.

4.5 Descriptive Analysis

Descriptive statistics are a set of brief descriptive coefficients that summarizes a given data set, which can either be a representation of the entire population or a sample. The measures used to describe the data set are calculated in percentage and tabulated as shown below.

4.5.1 The Influence of Mechanisms of Exchange in CTI Sharing

Table 4.7: Perception on the Mechanisms of Exchange of CTI

Mechanism of Exchange	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Sustainability	40%	37%	20%	3%	0%
Scalability	29%	51%	11%	6%	3%
Cost Implication	34%	40%	17%	6%	3%
Support Availability	31%	37%	26%	6%	0%

From Table 4.7 above, it is clear that majority of the respondents strongly agree that Sustainability influences the choice of Mechanism of Exchange at 40%, 37% agree to a moderate extent, 20% are neutral, 3% disagree and 0% strongly disagree. This means that the Mechanisms of Exchange have to be sustainable to guarantee Intelligence sharing across the financial institutions.

When asked to what extent Scalability influenced Mechanisms of Exchange, 29% strongly agreed, 51% agreed, 11% were neutral, 6% disagreed and 3% strongly disagreed. This can be translated to mean that more than half of the respondents agree that scalability impacts Mechanisms of Exchange.

When asked to which extent Costs impacted the Mechanisms of Exchange, 34% strongly agreed, 40% agreed, 17% were neutral, 6% disagreed and 3% strongly disagreed. This means that costs do impact Mechanisms of Exchange to a high extent as it is very costly to purchase, implement and maintain these mediums such as software which will facilitate the Intelligence sharing.

When asked to which extent Availability of Support impacted Mechanisms of Exchange, 31% strongly agreed, 37% agreed, 26% were neutral, 6% disagreed and 0% strongly disagreed. This is seen to mean that for smooth sharing of cyber threats intelligence, there must be adequate system support available. This will greatly assist the financial institutions to know how to detect, treat and prevent against such cyber threats from attacking them in the future.

As recommended by (Lunardi et al., 2021), in their research titled "Performance and cost evaluation in smart contracts in health", private instances do not have financial cost on transactions. Only infrastructure costs will be required. The proposed model is designed as private instance for financial institutions in Kenya.

4.5.2 Adoption of Smart Contract Technology

Table 4.8: Perception on Adoption of Smart Contract Technology on CTI

Adoption of Smart Contract Technology	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Ethics and law	69%	28%	0%	3%	0%
Privacy	66%	22%	6%	3%	3%
Sensor Security	42%	46%	6%	3%	3%
Social Translucence	46%	37%	17%	0%	0%

From Table 4.8 above, it is clear that the majority of the respondents strongly agree that Ethical and Legal Consideration will significantly impact Intelligence sharing at 69%, 28% agree, 0% were neutral, 3% disagreed and 0% strongly disagreed.

This means that while sharing intelligence, the financial institutions must do it an ethical manner and at the same time, observe the legal requirements.

When asked to what extent Privacy impact Intelligence sharing, 66% strongly agreed, 22% agreed, 6% were neutral, 3% disagreed and 3% strongly disagreed. This advocates for enhanced privacy models to allow the financial institutions freely share the information they deem sensitive anonymously without fear of victimisation.

When asked to which extent Sensor Security impacts intelligence sharing, 42% strongly agreed, 46% agreed, 6% were neutral, 3% disagreed and 3% strongly disagreed. Sensor security and location privacy must be maintained confidential to ensure the safety of the entity sharing the intelligence.

When asked to which extent Social Translucence impacts intelligence sharing, 46% strongly agreed, 37% agreed, 17% were neutral, 0% disagreed and 0% strongly disagreed. Social translucence should be observed to see to it that the intelligence shared is reliable, accurate, timely and can be depended upon to make strategies and decisions to curb cyber threats.

As recommended by (Béres et al., 2020) and (Venčkauskas et al., 2024) the developed model ensured anonymity of participating users.

4.5.3 Impact of CTI Sources

Table 4.9: Perception on Sources of CTI to Quality of Intelligence

Sources of Cyber Threat Intelligence	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
External intelligence	40%	29%	8%	20%	3%
Internal Intelligence	40%	32%	11%	17%	0%
Fusing Internal & External	57%	37%	0%	6%	0%
Employee Capability	60%	31%	9%	0%	0%

From Table 4.10 above, it is evident that External Intelligence impacts quality of intelligence where 40% strongly agree, 29% agree, 8% were neutral, 20% disagreed while 3% strongly disagreed. External intelligence is key in reducing and preventing cyber-attacks since those who have been affected will inform the other industry players for all to be aware and read to tackle such when they arise.

When asked to what extent Internal Intelligence influences intelligence sharing, 40% argued that they strongly agreed, 32% agreed, 11% were neutral, 17% disagreed while 0% strongly disagreed. Sharing intelligence internally ensured that all relevant stakeholders were aware, alert and well trained to detect and reduce cyber-attacks instances. Information regarding cyber security has to be transmitted internally and thus, all employees need to be conversant with how to avoid being prey to cyber-attacks.

When asked to which extent the Risk Framework and Vulnerability Management influences intelligence sharing; 57% strongly agreed, 37% agreed,0% were neutral while 6% disagreed, 0% strongly disagreed. The financial institutions have to have a strong risk framework which will minimise, mitigate, avoid and sometimes even transfer risk to other parties. They must minimise their vulnerability by ensuring that they are very alert on any cyber-attacks claims and strengthen their systems to reduce any attempts of such.

When asked to which level employee capability affected intelligence sharing, 60% strongly agreed, 31% agreed, 9% were neutral,0% disagreed and 0% strongly disagreed. The IT and Risk and Compliance employees have to be well trained, experienced and qualified to be able to detect, control, monitor and prevent cyber-attacks from occurring. When they have received the intelligence, they must act promptly to guarantee that the intelligence received is optimised.

As recommended by European Union Agency for Cybersecurity, the model adopted Common Vulnerabilities and Exposures (CVE) by Mitre institute as a reference method (ENISA, 2014). It includes the below parameters: Name, Status, Description, References, Report Phase and Comments.

4.5.4 Effectiveness of Smart Contract Technology

Table 4.10: Perception on Effectiveness of Smart Contract Technology on CTI

Effectiveness of Smart Contract Technology	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Distributed Computing	40%	46%	8%	0%	6%
Availability of Technology	49%	37%	8%	0%	6%
Complexity	43%	28%	17%	6%	6%
Response Time	51%	37%	6%	3%	3%

From table 4.10 above, respondents support Distributed Computing strongly at 40%, agree by 46%, neutral were 8%, 0% disagreed while 3% strongly disagreed.

When asked to what extent the available technology supported intelligence sharing, 49% strongly agreed, 37% agreed, 8% were neutral, 0% disagreed and 3% strongly disagreed.

When asked to which extent the complexity of the technology impacted intelligence sharing, 43% strongly supported, 28% supported, 17% were neutral, 6% disagreed while 6% strongly disagreed.

The study sought to which level Security of technology influenced intelligence sharing, 51% strongly supported, 37% agreed, 6% were neutral, 3% disagreed and 3% strongly disagreed.

As recommended by (Lunardi et al., 2021), private instances should have execution time of less than 1 minute. Model to take recommendation into consideration.

4.6 Interview Summary

All the 36 participants took part in the written interview, a further 15 participants were willing to participate in the oral interview. The objective of the interview was to ask both closed and open-ended questions. This enabled the researcher gain a better understanding of the current state of Cyber Threat Intelligence sharing in the financial industry. Data was then coded to enable responses to be grouped into categories.

Coding involves assigning numbers so that the responses could be grouped into a number of classes or categories.

4.6.1 CTI Exchange Methodologies

The current methodology of cyber threat intelligence sharing is user friendly and convenient.

Table 4.11: User Friendly and Convenience

User Friendly and Convenient	Frequency	Percentage (%)
Strongly Agree	1	7
Agree	1	7
Neutral	4	26
Disagree	8	53
Strongly disagree	1	7
Total	**15**	**100**

From Table 4.11 above, 7% of the respondents strongly agreed, those who agreed came in at 7%, those who were neutral were 26%, those who disagreed were 53% while those who strongly disagreed were 7%. The proposed prototype to consider HCI during development stage. According to (Rozanski & Haake, 2017), the general principles of learnability, flexibility and robustness when applied successfully in the design of system, they enhance usability.

4.6.2 Objectivity of CTI in Relation to Current Methodologies

The current methodology of sharing cyber threat intelligence is institutional based and objective.

Table 4.12: Objectivity of CTI

Institutional Based Systems	Frequency	Percentage (%)
Strongly Agree	1	7
Agree	5	33
Neutral	3	20
Disagree	4	27
Strongly disagree	2	13
Total	**15**	**100**

Based on Table 4.12 above, 7% of the respondents strongly agreed, 33% agreed, 20% were neutral, 27% disagreed while 13% strongly disagreed. The proposed system to consider objectivity of cyber threat intelligence being shared by adopting a standard.

This research adopted from the existing standard by the Mitre Corporation the Common Vulnerabilities and Exposures (CVE) reference method to improve objectivity of intelligence shared. This standard is able to assist the users easily access the type of vulnerability detected, the risk factor, the systems affected by the vulnerability and a detailed overview of the risks posed by the vulnerability. The smart contract prototype through the update.sol smart contract provided the necessary fields to share CTI in that format.

(CREST, 2022) defines intelligence as information that has been enhanced further, analysed and standardised resulting to an output that is relevant, actionable and valuable. For intelligence to be objective it must be relevant, actionable and valuable.

4.6.3 Confidentiality of CTI in Relation to Current Methodologies

Cyber security threat intelligence exchange in my organization is confidential.

Table 4.13: Confidentiality of CTI

Confidentiality of CTI	Frequency	Percentage (%)
Strongly Agree	1	7
Agree	5	33
Neutral	5	33
Disagree	2	13
Strongly disagree	2	13
Total	**15**	**100**

The researcher set out to find if the Cyber Threat Intelligence was Confidential in the institutions of the respondents. According to Table 4.13 above, 7% of the respondents strongly agreed, 33% agreed, 33% were neutral, 13% disagreed and 13% strongly disagreed. Cyber threat intelligence may be productive when used for the right reasons and also counterproductive if the intelligence get to the wrong hands. Proposed system should consider confidentiality in the design.

4.6.4 Assessment on Methodology of CTI Exchange

Some of the current methodology used includes peer forums, word of mouth as well as social media. There is also the IT Security Team in Kenya Bankers Association (KBA) which houses a fusion unit that deals with cyber intelligence. Further, intelligence is shared through networking and other channels of communication such as emails. Weekly review meetings also help to brainstorm on such intelligence in good time.

4.6.5 Assessment on Challenges in the Current CTI Mechanisms

Reports are not sustainable, verified nor tested. The intelligence may also be subjective. There may be information leakage or even no intelligence. Moreover, the intelligence shared may not be accorded the attention it deserves.

4.6.6 Assessment on CTI Disseminating Approaches

There is centralised dissemination of information where a team of experts work on a system and present their findings as a single report. Continuous sensitization of awareness to helps to keep employees on the lookout. Presence of a process document (Standard Operating Procedure) which is approved to provide guidance on intelligence sharing. Formal reporting helps to know the trends. Frequent (preferably monthly) summary of the threats faced to assist in forecasting and knowing the trends.

4.6.7 Assessment on Determining what CTI to Disseminate

Lack of anonymity or confidentiality. The cyber threat intelligence shared also cannot be authenticated. High staff turnover that reduces efficiency and effectiveness of the policies set as the employees leave too soon before the policy are well implemented. Lack of intelligence sharing that makes it hard for industry players to act simultaneously to intelligence shared.

4.6.8 Assessment on Required Improvement on CTI Exchange

A centralised intelligence collection and dissemination point to allow for anonymity. A documented process/ methodology to govern the process. Regular trainings and awareness creation, making resources available and increased collaboration by the industry players. A regulatory framework/ legislation regulating intelligence sharing. According to intelligence sharing proper attention and formalisation of the mechanisms to share intelligence in good time.

4.7 Summary of Data Analysis

From the analysis results, there are four main considerations that should be considered in the development of the model:

4.7.1 Cost Consideration

From the survey results, 74% agree that cost impacts choice of mechanism of exchange.

Take home: As recommended by (Lunardi et al., 2021) in their research titled performance and cost evaluation in smart contracts, private instances do not have financial cost on transactions. Only infrastructure costs will be required. The proposed model is designed as private instance for financial institutions in Kenya.

4.7.2 User Privacy

From the survey results 88% agree that user privacy consideration will affect the adoption of smart contract technology.

Take home: As recommended by (Béres et al., 2020) and (Rozanski & Haake, 2017) the proposed model to ensure anonymity of participating users.

4.7.3 Response Time

From the survey 88% system response time will affect the effectiveness of the smart contract technology.

Take home: As recommended by (Lunardi et al., 2021), private instances should have execution time of less than 1 minute. Model to take recommendation into consideration.

4.7.4 Intelligence Source

From the survey participants agree that the intelligence source impacts the quality of the intelligence.

Take home: As recommended by European Union Agency for Cybersecurity, the model to adopt Common Vulnerabilities and Exposures (CVE) by Mitre institute as a reference method (ENISA, 2014) and (CREST, 2022). It includes the below parameters: Name, Status, Description, References, Report Phase and Comments as compared to a non-structure intelligence sharing via social media.

4.8 Smart Contract Algorithms

4.8.1 Registration Smart Contract

- At registration, no information is collected except the generation of both public and private key pair by the application, which is done on the device. One key is registered as the public key on the blockchain through events for accessing the smart contracts, the private key is stored on the registered device.
- Function captureDeviceID() explicitly captures and encrypts (secure hash algorithm 3) the DeviceID of the RFID device at the time of calling the contract.
- Function enroll() is called when users want to enroll and participate in this blockchain.

Input: Serial number of tag ‘‘serial_id’’; S = {s1,s2, . . . ,sn}

Output: The hash of RFID serial, ‘‘encrypt_id’’ and the Timestamp (E, T); E = {e1, e2, . . . , en}, T = {t1, t2, . . . , tn}

This smart contract is generated by either a user with an application or an RFID reader on behalf of a passive RFID tag.

4.8.2 Update Smart Contract

- The update.sol smart contract pushes information onto the blockchain from the RFID receiver after initial registration
- Function log_serial() allows for encrypted logging of either deviceID or serialNo of the RFID receiver calling the smart contract.
- Function shareIntel() allows participants to pass cyber threat intelligence to the blockchain. Data type is string.

Input: Serial_id of tag S and the Message (S, M) S = {s1,s2, . . . ,sn}, M= {m1,m2, . . . ,mn}

Output: The hash of serial and the timestamp (T, E); E = {e1, e2,…, en}, T = {t1, t2,. . ., tn}

Participants will be using the common vulnerability and exposures (CVE) format for Name, Status, Description, References, Phase and Comments.

4.8.3 Notification Smart Contract

- The notification.sol smart contract will be available to the participants or configured on a device available to an authority or neutral participant.
- The user will be able to mark an intelligence shared on the blockchain either useful or not useful.

Input: Cyber threat intelligence status

Output: The timestamp and the hash of serial, and intel status (T, H, IS);

T = {t1, t2, . . . , tn}, E = {e1, e2, . . . , en},IS = {is1, is2, . . . , isn}

The useful status is initialized at 0 not useful, participants will be able to respond to useful cyber threat intelligence as marked by an assigned financial authority.

4.8.4 Execution at Ethereum Test Net

Sample transaction deployed on Ropsten Testnet. The transaction contains the below details:

- Block Number
- Time: 12 Seconds
- Date: 18th Aug 2025
- From: Public Key Address
- To: Contract Address
- Value: $0 no monetary exchange
- Fee in Eth: 0.0001

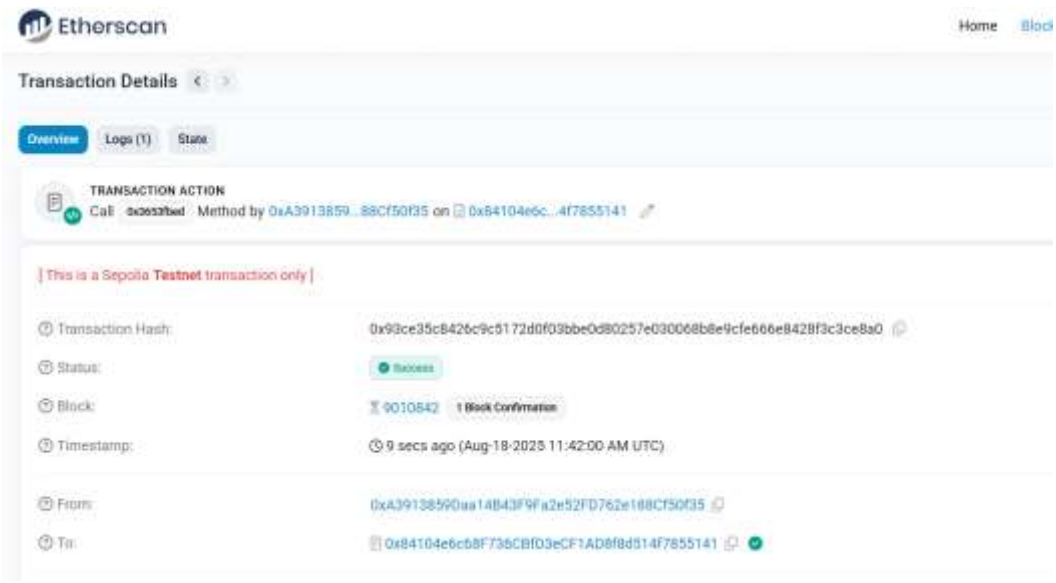


Figure 4.4: Sample Executed Transaction on Sepolia Testnet

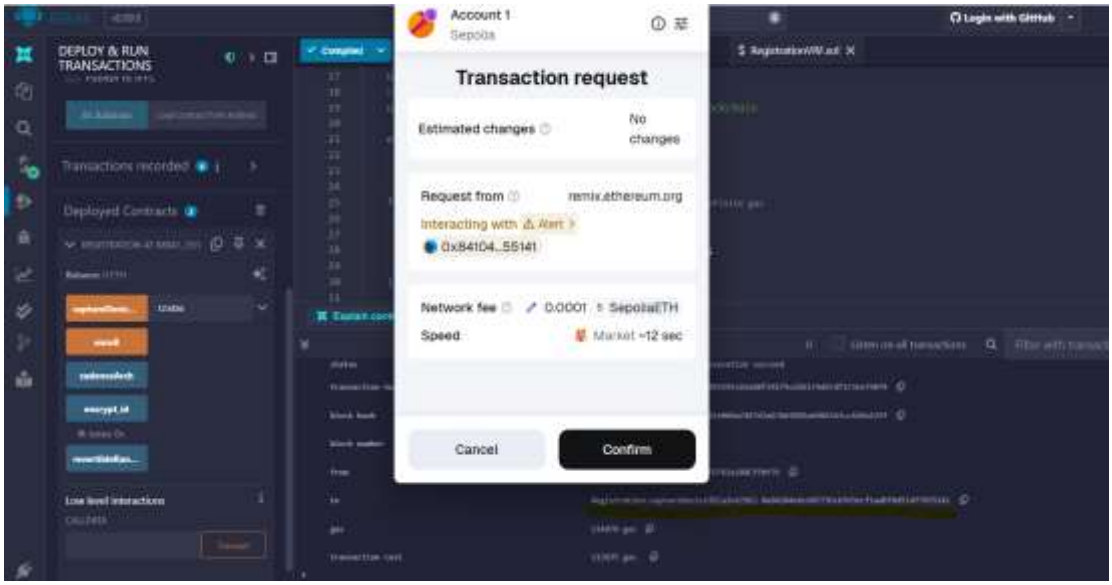


Figure 4.5: Device ID Masked at Execution successfully (Registration.sol)

Results in Figure 4.5 showing encrypted deviceID '123456' to an MD5 value '0xa3913859daa14b43f9fa2e52fd762e188cf50f35'

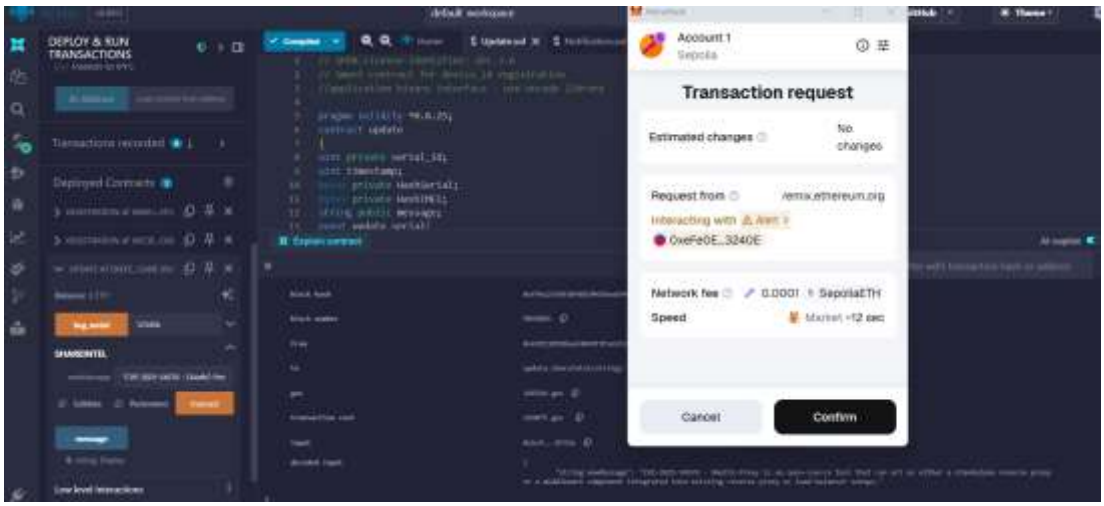


Figure 4.6: CTI shared within the Blockchain Network (Update.sol)

Figure 4.6 shows intelligence can reach the entire network within 12 seconds. Results show the model can adapt to Common Vulnerabilities and Exposures (CVE) standards to share intelligence.

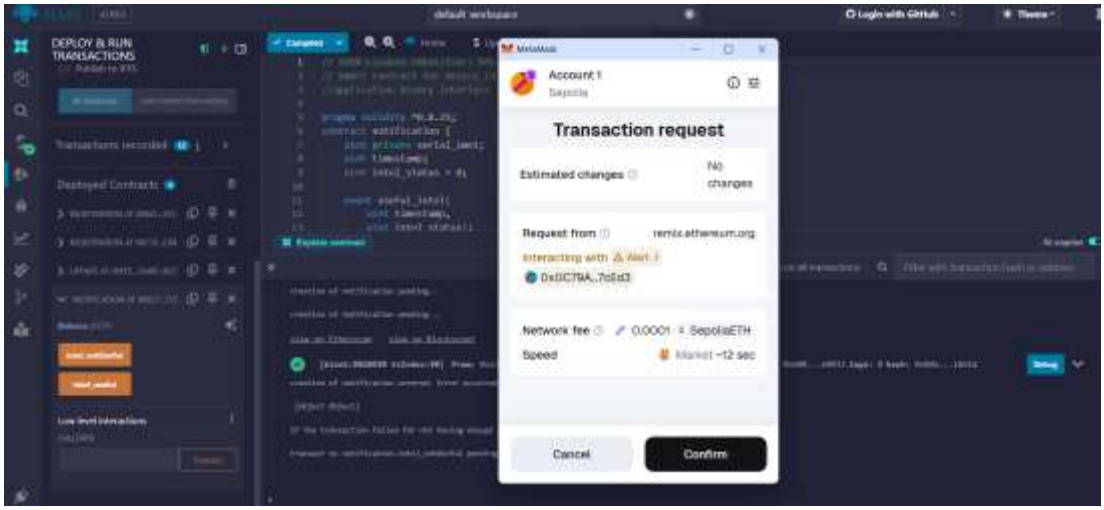


Figure 4.7: Participants Can Rate Intelligence (Notification.sol).

Results in figure 4.7 show participants can be able to rate intelligence shared either as useful or not useful. This is a mechanism to encourage participants to share intelligence that can be utilized within the network.

This model set out to achieve confidentiality of users by protecting personal data against unauthorized accesses, keeping personal data protected, anonymised and therefore private regarding the public. To achieve this objective, we collected device ID of an RFID device and encrypted the id prior to being written on the blockchain.

4.9 Simulation Results Conclusion

4.9.1 Simulation Results Table

Table 4.14: Simulation Results in Terms of Execution Time and Costs

Contract	Activity	Gas Used	Transaction Fee ETH	Transaction Fee FIAT	Mining Time
Registration	Deploying contract	159199	0.0001633	$ 0.38	27 Sec
	Calling captureDeviceID function	89563	0.0000919	$ 0.22	59 Sec
	Calling enroll function	32938	0.000034	$ 0.08	49 Sec
Update	Deploying contract	284208	0.000292	$ 0.68	48 Sec
	Calling shareIntel function	44627	0.000046	$ 0.11	41 Sec
Authorize	Deploying contract	118993	0.000122	$ 0.29	29 Sec
	Calling intel_useful function	47081	0.000048	$ 0.11	50 Sec
	Calling intel_notUseful function	49859	0.000051	$ 0.12	54 Sec

1. **Response Time**

Simulation results show that it will take less than a second to complete on Remix, on the public Ethereum test network, it will take an average of 45 seconds. The actual project is recommended to run on a private network at the beginning since the research population involves once sector the financial sector in Kenya. Response time is projected to have faster turnaround time.

2. Cost Consideration

Simulation results shows that it costs an average of $0.45 equivalent to Kes. 50 to deploy the three smart contracts and almost $0.13 equivalent to Kes. 14 to call and update functions in those smart contracts. Deployment is done once when the smart contract is set up. The cost is much lower than existing transaction costs of various channels.

3. User privacy

This model set out to achieve confidentiality of users by protecting personal data against unauthorized accesses, keeping personal data protected, anonymized and therefore private with regard to the general public. To achieve this objective we collected device ID of an RFID device and encrypted the id prior to being written on the blockchain.

4. Intelligence sources

The prototype is open for the two broad categories of intelligence sources, that is internal within an organization and from external sources. For intelligence usability, we have put in a control, via the notification smart contract where an administrator can be able to mark whether an intelligence shared is useful or not useful facilitated by notification.sol. The other control is users incurring a small fee to share intelligence of approximately Kes. 14.

CHAPTER FIVE

SUMMARY, CONCLUSIONS & RECOMMENDATIONS

5.1 Introduction

The research aimed to evaluate the mechanisms of exchange of cyber threat intelligence as the first objective. The researcher reviewed the existing and baseline approaches that financial institutions employ to exchange intelligence. In this comparative study with other mechanisms of cyber threat intelligence exchange, the researcher was able to model these approaches to ascertain the gaps that would form the base of the prototype. The other objective was to develop a smart contract-based architecture for cyber threat intelligence sharing. Once the prototype was developed, the same targeted group who provided user requirements were approached as end users. The end users were given an opportunity to provide feedback on how they felt about the prototype on different elements of user experience. The respondents were trained and provided with reference materials for their use. Feedback was collected in the form of a questionnaire and results documented and summarized in pie charts format.

5.2 Findings

The specific objectives of this research are:

i. To evaluate the existing mechanisms of exchange of cyber threat intelligence including their strengths and weaknesses.
ii. To develop a smart contract model that masks the identity of participating mobile devices and internet of things (IoT) devices when passing information on the block chain.
iii. To evaluate the effectiveness of the developed model in anonymizing participants in the model.

Objective one was answered by both literature review and the questionnaires answered by the interviewees, who noted the current CTI mechanisms of exchange are largely informal and based on unstructured social media exchanges.

Objective two: To develop a smart contract model that masks the identity of participating mobile devices and internet of things (IoT) devices when passing information on the block chain. The model was able to exchange CTI synonymously with excellent results as highlighted in table 4:14.

Objective Three: To evaluate the effectiveness of the developed model (ability to anonymise participating devices. From the simulation results, the prototype is able to anonymize participating devices by hiding the device ids. Evidence has been provided as shown in figure 4.5.

The model was developed and accessed by the interviewees, and they gave their feedback as noted in section 5.2.

5.2.1 User Experience Findings

Compared to other mechanisms of cyber threat intelligence sharing a survey on end user experience was performed. 57% strongly agreed that they needed minimal training on using the interface. 15% agreed to require minimal training. 14% remained neutral on their training needs and a further 14% strongly disagreed and indicated they required adequate training. This is shown in Figure 5.2.1

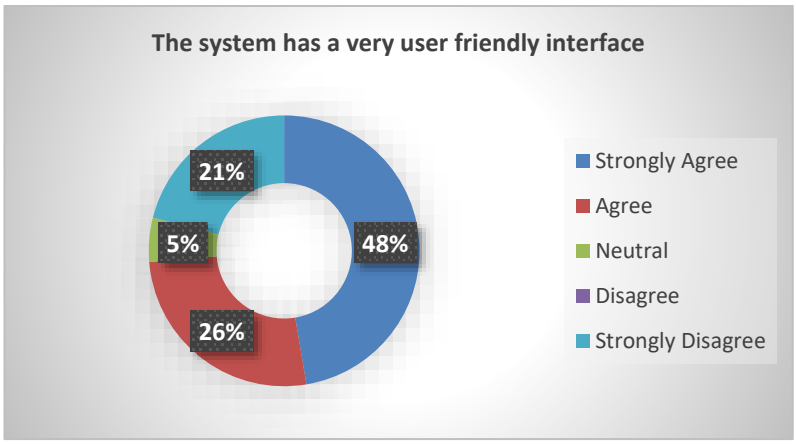


Figure 5.1: Mechanism of CTI Sharing User Friendliness

5.2.2 Prototype Performance

Though mechanisms of cyber threat intelligence exchange of intelligence tend to consume time and resources within a work group. 61% strongly agreed that they would use the system to exchange intelligence. 29% agreed the system is reliable to cyber threat intelligence exchange. 5% remained neutral and 5% disagreed on the reliability of the prototype. This is shown in Figure 5.2.2

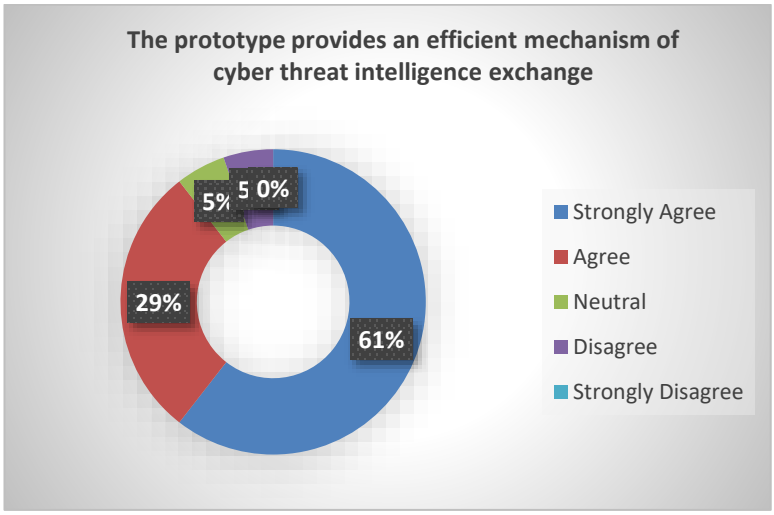


Figure 5.2: Mechanism of CTI Sharing Efficiency

5.2.3 Ability of the Model to Anonymize CTI sharing Devices

28% strongly agreed the model can anonymize smart contract based cyber threat intelligence exchange devices. 54% agreed to the model was able to anonymize sharing devices. 8% remained neutral and 10% disagreed on anonymizing CTI sharing devices. This is shown in Figure 5.2.2

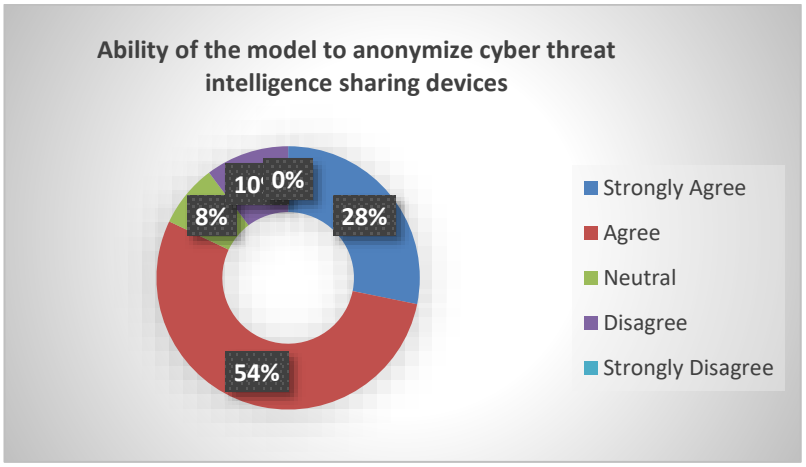


Figure 5.3: Ability to Anonymize CTI

5.3 Limitations of this Prototype

During the research it was noted users had challenges in the classification of cyber threat intelligence. To mitigate this, the prototype categorized intelligence by providing a mechanism of participation institutions to rate the intelligence as either useful or not useful. Future we recommend the model to include artificial intelligence to rate cyber threat intelligence exchanged.

5.4 Conclusion and Recommendations

This research provides a novel approach to curbing the issue of income leakages among financial institutions in Kenya particularly because of threat replication among different financial institutions.

The research has proved that we are able to encrypt and randomize device IDs including RFIDs to protect the identity of users. Smart contract technology one of the best technologies to be adopted for cyber threat intelligence sharing thereby taming the issue of cyber threat replication among financial institutions in Kenya.

We suggest future work on the analytical capabilities of CTI exchange mechanisms

REFERENCES

Aayush, T., Rashi, G., & Krishnappa, J. (2024). Cyber Threat Intelligence Research Paper. *Research Paper on Cyber Threat Intelligence (CTI)*, *1*(1), 1–24. https://doi.org/10.13140

Abu, M. S., Selamat, S. R., Ariffin, A., & Yusof, R. (2018). Cyber threat intelligence – Issue and challenges. *Indonesian Journal of Electrical Engineering and Computer Science*, *10*(1), 371–379. https://doi.org/10.11591/ijeecs.v10.i1.pp371-379

Aljuhami, A. M., & Bamasoud, D. M. (2021). Cyber Threat Intelligence in Risk Management A Survey of the Impact of Cyber Threat Intelligence on Saudi Higher Education Risk Management. In *IJACSA) International Journal of Advanced Computer Science and Applications* (Vol. 12, Issue 10). www.ijacsa.thesai.org

Allouche, Y., Tapas, N., Longo, F., Shabtai, A., & Wolfsthal, Y. (2021). *TRADE: TRusted Anonymous Data Exchange: Threat Sharing Using Blockchain Technology*. http://arxiv.org/abs/2103.13158

Androulaki, E., Karame, G. O., Roeschlin, M., Scherer, T., & Capkun, S. (2012). *Evaluating User Privacy in Bitcoin*.

Bank of England. (2016). Understanding Cyber Threat Intelligence Operations. *Cbest*.

Baraniuk, K., & Marszałek, P. (2024). The potential of Cyber Threat Intelligence analytical frameworks in research on information operations and influence operations. *Przegląd Bezpieczeństwa Wewnętrznego*, *16*(31), 279–320. https://doi.org/10.4467/20801335pbw.24.027.20804

Basheer, R., & Alkhatib, B. (2021). Threats from the Dark: A Review over Dark Web Investigation Research for Cyber Threat Intelligence. In *Journal of*

Computer Networks and Communications (Vol. 2021). Hindawi Limited. https://doi.org/10.1155/2021/1302999

Béres, F., Seres, I. A., Benczúr, A. A., & Quintyne-Collins, M. (2020). *Blockchain is Watching You: Profiling and Deanonymizing Ethereum Users*.

Biryukov, A., & Pustogarov, I. (2015). *Bitcoin over Tor isn ' t a good idea*.

Caston, A., Cavoukian, A., Ticoll, D., Lowy, A., Ticoll, D., Williams, A. D., & Williams, A. D. (2016). *Blockchain Revolution* (1st ed.). Penguin.

Central Bank of Kenya. (2018). *GUIDELINES ON CYBERSECURITY FOR PAYMENT SERVICE PROVIDERS* (Issue August).

Central Bank of Kenya. (2020). *ANNUAL REPORT & FINANCIAL STATEMENTS 2019/20*.

Chatziamanetoglou, D., & Rantos, K. (2024). Cyber Threat Intelligence on Blockchain: A Systematic Literature Review. In *Computers* (Vol. 13, Issue 3). Multidisciplinary Digital Publishing Institute (MDPI). https://doi.org/10.3390/computers13030060

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). NIST Special Publication 800-61 Revision 2: Computer Security Incident Handling Guide Recommendations. *NIST Special Publication*. https://doi.org/10.6028/NIST.SP.800-61r2

(Communication Authority of Kenya, 2025). (2025). *Cybersecurity Report*. www.ke-cirt.go.ke

Conoscenti, M., Vetro, A., & De Martin, J. C. (2016). Blockchain for the Internet of Things: A systematic literature review. *Proceedings of IEEE/ACS International Conference on Computer Systems and Applications, AICCSA*, *0*. https://doi.org/10.1109/AICCSA.2016.7945805

Cooper, D. R., & Schindler, P. S. (2014). Business Research Methods 12th Edition. In *Business Research Methods*.

Cosimo Lan, Adele Veschetti, & Sergio Solmonte. (2023). *SCUOLA DI SCIENZE Corso di Laurea Magistrale in Informatica*.

Courage Ojo, Emmanuel Ayodeji Osoko, Joy Nnenna Okolo, & Mamudat Jaji. (2024). Incident response: A structured model from detection to containment and recovery. *World Journal of Advanced Research and Reviews*, *24*(1), 1401–1407. https://doi.org/10.30574/wjarr.2024.24.1.3148

Crandall, D. J., Backstrom, L., Cosley, D., Suri, S., Huttenlocher, D., & Kleinberg, J. (2010). Inferring social ties from geographic coincidences. *Proceedings of the National Academy of Sciences of the United States of America*, *107*(52), 22436–22441. https://doi.org/10.1073/pnas.1006155107

CREST. (2022). *What Is Cyber Threat Intelligence and How Is It Used? CREST Guide*. http://www.crest-approved.org

Creswell, J. W. (2012). *Educational research : planning, conducting, and evaluating quantitative and qualitative research* (Pearson Education, Ed.; 4th ed.). Pearson Education.

Cybersecurity Report. (n.d.). www.ke-cirt.go.ke

David Friday Isie. (2023). *Application of Blockchain Technology and Integration of Differential Privacy: Issues in E-Health Domains*. https://commons.und.edu/theses/5676

DHS. (2016). *Critical infrastructure threat information sharing framework: A reference guide for the critical infrastructure community*. *October*, 110.

El Jaouhari, S., Ahmed, S., & Jaouhari, S. EL. (2024). *CTIoT: A Cyber Threat Intelligence Tool for IoT*. 1483–1489. https://doi.org/10.1109/IWCMC61514.2024.10592406ï

ENISA. (2014). *Standards and tools for exchange and processing of actionable information* (Issue November).

Felix Albrektson, & Max Bergstrom. (2022). *Blockchain technology, an enabling force: Getting access to a new spectrum of international markets Bachelor Thesis*.

Fransen, F., Smulders, A., & Kerkdijk, R. (2015). Cyber Security-Informationsaustausch zur Erkennung von Cyber-Bedrohungen und -Vorfällen. *Elektrotechnik Und Informationstechnik*, *132*(2), 106–112. https://doi.org/10.1007/s00502-015-0289-2

Georgiadou, A., Mouzakitis, S., & Askounis, D. (2021). Assessing mitre att&ck risk using a cyber-security culture framework. *Sensors*, *21*(9). https://doi.org/10.3390/s21093267

Glenn D. Israel. (2003). Using Published Tables Using Formulas To Calculate A Sample Size Using A Census For Small Populations. *University of Florida*, *2*(1).

Goodwin, C., Nicholas, J. P., Bryant, J., Ciglic, K., Kleiner, A., Kutterer, C., Massagli, A., Mckay, A., Mckitrick, P., Neutze, J., Storch, T., & Sullivan, K. (2015). *A framework for cybersecurity information sharing and risk reduction*. 1–24.

gorodenkoff. (2024). *Cyber Threat Trends Report From Trojan Takeovers to Ransomware Roulette Cyber Threat Trends Report*.

IBM. (2025). *IBM X-Force 2025 Threat Intelligence Index*.

IBM XForce Security. (2021). *IBM Security - XForce Threat Intelligence Index*.

Interpol. (2025). *INTERPOL AFRICA CYBERTHREAT ASSESSMENT REPORT 2025*.

ISACA. (2019). *State of Cybersecurity 2019*. *November 2018*, 1–21.

(ISC)2. (2020). *Cybersecurity Professionals Stand Up to a Pandemic*. *2020*, 1–43.

Javaheri, D., Fahmideh, M., Chizari, H., Lalbakhsh, P., & Hur, J. (2024). Cybersecurity threats in FinTech: A systematic review. In *Expert Systems with Applications* (Vol. 241). Elsevier Ltd. https://doi.org/10.1016/j.eswa.2023.122697

Jin, B., Kim, E., Lee, H., Bertino, E., Kim, D., & Kim, H. (2024, February 10). *Sharing cyber threat intelligence: Does it really help?* https://doi.org/10.14722/ndss.2024.24228

Johnson, C., Johnson, C., & Snyder, J. (2016a). Guide to Cyber Threat Information Sharing. *Special Publication - Council for Agricultural Science and Technology*. https://doi.org/10.6028/nist.sp.800-150

Johnson, C., Johnson, C., & Snyder, J. (2016b). Guide to Cyber Threat Information Sharing. *Special Publication - Council for Agricultural Science and Technology*. https://doi.org/10.6028/nist.sp.800-150

Johnson, C. S., Badger, M. L., Waltermire, D. A., Snyder, J., & Skorupka, C. (2016). *Guide to Cyber Threat Information Sharing*. https://doi.org/10.6028/NIST.SP.800-150

Kaiafas, G. (2020). *D5 . 1 Threat Intelligence Sharing : State of the Art and Requirements*. *700071*, 1–56.

Khanboubi, F., Boulmakoul, A., & Tabaa, M. (2019). Impact of digital trends using IoT on banking processes. *Procedia Computer Science*, *151*(May), 77–84. https://doi.org/10.1016/j.procs.2019.04.014

Kothari, C. R. (2004). Research Methodology Methods and Technigues. In *Journal of Materials Processing Technology* (Vol. 1, Issue 2).

KPMG. (2016). *Bangladesh hack illustrates rising sophistication of attacks*. 1–3.

Kral, P. (2020). *Information Security Reading Room Incident Handler ’ s Handbook*.

Laszka, A., Loukas, G., Roy, S., Panaousis, E., Noakes, C., & Panda, S. (2023). *SoK: The MITRE ATT&CK Framework in Research and Practice*. https://doi.org/10.48550/arXiv.2304.07411

Lunardi, R. C., Nunes, H. C., Branco, V. da S., Lippert, B. H., Neu, C. V., & Zorzo, A. F. (2021). *Performance and Cost Evaluation of Smart Contracts in Collaborative Health Care Environment*. 49–54. https://doi.org/10.20533/icitst.worldcis.wcst.wcicss.2019.0007

McCorry, P., Shahandashti, S. F., & Hao, F. (2017). A smart contract for boardroom voting with maximum voter privacy. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *10322 LNCS*, 357–375. https://doi.org/10.1007/978-3-319-70972-7_20

Miguel, L., León, C., Tuffaha, A., & Wen, W. (2022). *Title: Application of Blockchain Technology in the Financial Services Industry. The Big Four perspective. Course: BUSN79 Degree Project in Accounting and Finance*.

Mohammed, M., Adnan, Y., Uddin, I., & Ahmed, O. (2023). *Cyber Threat Intelligence and Information Sharing*. www.ijsdr.org

Mucheru, J. (2016). *Ministry of Information Communications and Technology National Information & Communications Technology (Ict) Policy*. *June*, 1–50.

Mudassar, S., & Khan, A. (2023). *V-Model Used in Software Development*. https://www.researchgate.net/publication/371902849

Müller, M. (2019). Cyber Security Report 2019. *Die Aktiengesellschaft*, *64*(19), r283–r284. https://doi.org/10.9785/ag-2019-641919

Nakamoto, S. (2017). Bitcoin: A Peer-to-Peer Electronic Cash System. *Artificial Life*, *23*(4), 552–557. https://doi.org/10.1162/ARTL_a_00247

Narayanan, A., & Shmatikov, V. (2009). *Shmat_Oak09*.

Nelson, A., Rekhi, S., Souppaya, M., & Scarfone, K. (2025). *Incident response recommendations and considerations for cybersecurity risk management :* https://doi.org/10.6028/NIST.SP.800-61r3

Ogunrinde, V., & Peter, K. (2024). *Cybersecurity Challenges and Opportunities in Kenya Amidst the Fourth Industrial Revolution*. https://www.researchgate.net/publication/386824120

Omer Eltayeb, O. E. (2024). The Crucial Significance of Cyber Threat Intelligence in Mitigating Cyber Attacks. *Journal of Ecohumanism*, *3*(4), 2422–2434. https://doi.org/10.62754/joe.v3i4.3767

Panarello, A., Tapas, N., Merlino, G., Longo, F., & Puliafito, A. (2018). Blockchain and iot integration: A systematic survey. In *Sensors (Switzerland)* (Vol. 18, Issue 8). https://doi.org/10.3390/s18082575

Piscini, E., & Kehoe, L. (2018). Blockchain & Cyber Security. Let's discuss for more information please contact : *Deloitte*, 14.

Pradhan, S., & Biswas, D. (2025). A Conceptual Framework for Cybersecurity Threat Intelligence Sharing Using Blockchain-Based Systems. *International Journal for Research in Applied Science and Engineering Technology*, *13*(5), 939–945. https://doi.org/10.22214/ijraset.2025.70340

Reddy Vaka, P. (2025). Common Vulnerabilities and Exposures: What You Should Know. *International Research Journal of Engineering and Technology*. www.irjet.net

Reid, F., & Harrigan, M. (2011). An analysis of anonymity in the Bitcoin system. *Proceedings - 2011 IEEE International Conference on Privacy, Security,*

Risk and Trust and IEEE International Conference on Social Computing, PASSAT/SocialCom 2011, July 2011, 1318–1326. https://doi.org/10.1109/PASSAT/SocialCom.2011.79

Rozanski, E. P., & Haake, A. R. (2017). Human–computer interaction. In *Systems, Controls, Embedded Systems, Energy, and Machines*. https://doi.org/10.1201/9781420037043

Sailio, M., Latvala, O. M., & Szanto, A. (2020). Cyber threat actors for the factory of the future. *Applied Sciences (Switzerland)*, *10*(12). https://doi.org/10.3390/app10124334

Salem, A. H., Azzam, S. M., Emam, O. E., & Abohany, A. A. (2024). Advancing cybersecurity: a comprehensive review of AI-driven detection techniques. *Journal of Big Data*, *11*(1). https://doi.org/10.1186/s40537-024-00957-y

Santos, P., Abreu, R., Reis, M. J. C. S., Serôdio, C., & Branco, F. (2025a). A Systematic Review of Cyber Threat Intelligence: The Effectiveness of Technologies, Strategies, and Collaborations in Combating Modern Threats. *Sensors*, *25*(14), 4272. https://doi.org/10.3390/s25144272

Santos, P., Abreu, R., Reis, M. J. C. S., Serôdio, C., & Branco, F. (2025b). A Systematic Review of Cyber Threat Intelligence: The Effectiveness of Technologies, Strategies, and Collaborations in Combating Modern Threats. *Sensors*, *25*(14), 4272. https://doi.org/10.3390/s25144272

Sauerwein, C., Sillaber, C., Mussmann, A., & Breu, R. (2017). Threat Intelligence Sharing Platforms: An Exploratory Study of Software Vendors and Research Perspectives. *13th International Conference on Wirtschaftsinformatik*, 837–851.

Serianu. (2018). *Cyber Security Skills Gap*.

Simonetto, S., & Bosch, P. (2024). *Comprehensive threat analysis and systematic mapping of CVEs to MITRE framework*. https://cwe.mitre.org/

Suseendran, G., Chandrasekaran, E., Akila, D., & Sasi Kumar, A. (2020a). Banking and FinTech (Financial Technology) Embraced with IoT Device. *Advances in Intelligent Systems and Computing*, *1042*(January), 197–211. https://doi.org/10.1007/978-981-32-9949-8_15

Suseendran, G., Chandrasekaran, E., Akila, D., & Sasi Kumar, A. (2020b). Banking and FinTech (Financial Technology) Embraced with IoT Device. *Advances in Intelligent Systems and Computing*, *1042*(February), 197–211. https://doi.org/10.1007/978-981-32-9949-8_15

The Republic of Kenya. (2018). *Laws of Kenya: Computer Misuse and Cybercrimes Act*. *5*.

Tiberious, Murithi., Mwania, J. M., & Mwinzi, J. (2016). The Influence of Financial Resources on the integration of the National Goals of Education. *International Journal of Education and Research*, *4*(9), 51–62.

Tobin, A., & Reed, D. (2017). The Inevitable Rise of Self-Sovereign Identity. *White Paper*, *29*(September 2016), 10.

TransUnion. (2025). *DIGITAL FRAUD TRENDS IN AFRICA Strategies and Trends for Protecting Organisations and Consumers*.

Venčkauskas, A., Jusas, V., Barisas, D., & Misnevs, B. (2024). Blockchain-Based Model for Incentivized Cyber Threat Intelligence Sharing. *Applied Sciences (Switzerland)*, *14*(16). https://doi.org/10.3390/app14166872

Vergara Cobos, E., Cakir, S., Straub, S., Qiang, C. Z., & Torgusson, C. (n.d.-a). *A Review of the Economic Costs of Cyber Incidents*.

Vergara Cobos, E., Cakir, S., Straub, S., Qiang, C. Z., & Torgusson, C. (n.d.-b). *A Review of the Economic Costs of Cyber Incidents*.

Wood, G. (2014). Ethereum: a secure decentralised generalised transaction ledger. *Ethereum Project Yellow Paper*, 1–32. https://doi.org/10.1017/CBO9781107415324.004

Zhang, R., Xue, R., & Liu, L. (2019). Security and privacy on blockchain. *ACM Computing Surveys*, *52*(3). https://doi.org/10.1145/3316481

Zhang, S., Chen, P., Bai, G., Wang, S., Zhang, M., Li, S., & Zhao, C. (2022). An Automatic Assessment Method of Cyber Threat Intelligence Combined with ATT&CK Matrix. *Wireless Communications and Mobile Computing*, *2022*. https://doi.org/10.1155/2022/7875910

APPENDICES

Appendix I: Questionnaire

Academic Researcher: Wilson Muigai Maina

MSc. IT, JKUAT University

This research is exclusively for academic purpose only. The main objective of the research is to solicit the user requirements that will be used to develop a prototype for passing cyber threat intelligence privately and securely in financial institutions in Kenya. Kindly provide your honest answers to ensure that the researcher accurately captures the facts. Kindly note that this research will be treated with high confidentiality and your responses will be private and confidential.

Interviewee: ……..……. Organization: ……..……..

Interview channel: …… Date: ……

PART A: GENERAL INFORMATION

1. Gender of respondent Male [ ] Female [ ]
2. Age category of respondent

Up to 24 years **[ ]** 25 -35 years **[ ]** 35 to 45 years **[ ]** 45 to 55 years **[ ]**
Over 55 years **[ ]**

3. Highest level of education

KCSE **[ ]** Certificate **[ ]** Diploma **[ ]** Bachelor's degree **[ ]** Postgraduate degree **[ ]**

4. What is your job level?

Lower management [ ] Middle Management [ ] Top Management [ ]

5. How long have you worked with the organization?

Less than 5 years [ ] 6-10 years [ ] 11-15 years [ ] 16-20 years [ ]
More than 20 years [ ]

6. Kindly indicate your department……..……

PART B: INFLUENCE OF THE MECHANISMS OF EXCHANGE OF CYBER THREAT INTELLIGENCE ON INTELLIGENCE SHARING

To what extent do you agree with the following statements on the influence of the Mechanisms of Exchange of Cyber Threat Intelligence on Intelligence Sharing?

KEY: 5 = Strongly Agree 4= Agree 3= Neutral 2= Disagree 1= Strongly Disagree

INFLUENCE OF MECHANISMS OF EXCHANGE ON CYBER THREAT INTELLIGENCE	**5**	**4**	**3**	**2**	**1**
1. Sustainability impacts choice of mechanism of exchange					
2. Scalability impacts choice of mechanism of exchange					
3. Cost impacts choice of mechanism of exchange					
4. Non-repudiation impacts choice of mechanism of exchange					

What are the other Mechanisms of Exchange of Cyber Threat Intelligence that influence Intelligence Sharing in your Organization?

……

……

PART C: THE IMPACT OF FORMULATING A SMART CONTRACT LOGIC THAT MASKS THE IDENTITY OF PARTICIPATING MOBILE DEVICES DURING INTELLIGENCE SHARING.

To what extent do you agree with the following statements on the influence of formulating a smart contract logic that masks the identity of participating mobile devices during Intelligence Sharing?

KEY: 5 = Strongly Agree 4= Agree 3= Neutral 2= Disagree 1= Strongly Disagree

INFLUENCE OF ADOPTION OF SMART CONTRACT TECHNOLOGY	5	4	3	2	1
1. Ethical and legal considerations impact on Intelligence Sharing.					
2. Privacy of Users' Identity					
3. Sensor security and location privacy impact on Intelligence Sharing.					
4. Social translucence impacts Intelligence Sharing					

What are the other smart contract logic that masks the identity of participating mobile devices during Intelligence Sharing in your Organization?

……

……

PART D: THE IMPACT OF THREAT INTELLIGENCE SOURCES ON INTELLIGENCE SHARING.

To what extent do you agree with the following statements on the impact of Fusing Internal and External Intelligence on Intelligence sharing?

KEY: 5 = Strongly Agree 4= Agree 3= Neutral 2= Disagree 1= Strongly Disagree

IMPACT OF THREAT INTELLIGENCE SOURCES	5	4	3	2	1
1. Use of external Intelligence only impacts Intelligence Sharing.					
2. Use of Internal Intelligence only impacts Intelligence Sharing.					
3. Fusing External and Internal Intelligence impacts Intelligence Sharing					
4. Employee capability and management support impacts on Intelligence Sharing.					

What are the other Internal and External Intelligence Factors which influence Intelligence Sharing in your Organization?

……

……

PART E: THE EFFECTIVENESS OF SMART CONTRACT TECHNOLOGY ON INTELLIGENCE SHARING.

To what extent do you agree with the following statements on the effect of exchange medium on Intelligence Sharing?

KEY: 5 = Strongly Agree 4= Agree 3= Neutral 2= Disagree 1= Strongly Disagree

IMPACT OF EXCHANGE MEDIUM OR UNDERLYING TECHNOLOGY	**5**	**4**	**3**	**2**	**1**
1. Distributed computing impacts on Intelligence Sharing.					
2. Availability of underlying technology impacts on Intelligence Sharing.					
3. Complexity of underlying technology affects Intelligence Sharing.					
4. Response Time affects Intelligence Sharing					

What are the other intelligence exchange media which influence Intelligence Sharing in your Organization?

……

……

THANK YOU.

Appendix II: Interview Questions

1. Cyber security incidents and breaches are replicated across organizations when there are information sharing gaps or existing mechanisms are in-effective

□ Strongly Agree

□ Agree

□ Neutral

□ Disagree

□ Strongly Disagree

2. It is easy to establish if cyber threat intelligence sharing mechanisms are effective, provided they are in-place

□ Strongly Agree

□ Agree

□ Neutral

□ Disagree

□ Strongly Disagree

3. The current process of sharing cyber threat intelligence among financial institutions is efficient.

□ Strongly Agree

□ Agree

□ Neutral

□ Disagree

□ Strongly Disagree

4. The current methodology of cyber threat intelligence sharing is time saving and user friendly.

□ Strongly Agree

□ Agree

□ Neutral

□ Disagree

□ Strongly Disagree

5. I believe that the current methodology of sharing cyber threat intelligence is institutional based and not subjective

□ Strongly Agree

□ Agree

□ Neutral

□ Disagree

□ Strongly Disagree

6. If a proper system based cyber threat intelligence exchange is implemented, I believe it would make the financial institutions more effective and efficient in addressing cyber threats.

□ Strongly Agree

□ Agree

□ Neutral

□ Disagree

□ Strongly Disagree

7. Cyber threat intelligence exchange is confidential in your organization?

□ Strongly Agree

□ Agree

□ Neutral

□ Disagree

□ Strongly Disagree

8. When a cyber-threat intelligence exchange mechanism is ineffective, what should be the approach to remediate it?

_____

_____

9. What is the current methodology of cyber threat intelligence exchange?

_____

_____

10. What are the challenges in the current cyber threat intelligence exchange mechanism?

_____

_____

11. What approach has your organization taken to ensure cyber threat intelligence is disseminated to all concerned parties as per the incident response plan?

_____

_____

12. What challenges has your organization faced when determining the cyber threat intelligence

_____

_____

13. In your opinion, what needs to be improved in the current cyber threat intelligence mechanisms?_____

_____

Appendix III: Research License

REPUBLIC OF KENYA

NATIONAL COMMISSION FOR SCIENCE,TECHNOLOGY & INNOVATION

Ref No: 222034

Date of Issue: 24/February/2021

RESEARCH LICENSE

This is to Certify that Mr.. Wilson Muigai Maina of Jomo Kenyatta University of Agriculture and Technology, has been licensed to conduct research in Nairobi on the topic: A SMART CONTRACT APPROACH FOR CYBER THREAT INTELLIGENCE SHARING for the period ending : 24/February/2022.

License No: NACOSTI/P/21/9070

222034

Applicant Identification Number

Director General
NATIONAL COMMISSION FOR SCIENCE,TECHNOLOGY & INNOVATION

Verification QR Code

NOTE: This is a computer generated License. To verify the authenticity of this document, Scan the QR Code using QR scanner application.

Appendix IV: Code Used for Smart Contract Intelligence Exchange

```
pragma solidity ^0.8.25;

contract registration {

    uint private device_id;

    bytes public encrypt_id; //

    uint timestamp;  //as at the time of calling the bloc   blockchain

    event register(

        uint timestamp,

        bytes encrypt_id    );

    function captureDeviceID(uint d_i) public{

        timestamp = block.timestamp;

        device_id = d_i;

        encrypt_id = bytes(abi.encodePacked(device_id));

        emit register(timestamp, encrypt_id);    }

    function enroll() public {

        timestamp = block.timestamp;

        encrypt_id = bytes(abi.encodePacked(msg.sender));

        emit register(timestamp, encrypt_id); }}
```

```
pragma solidity ^0.8.7;

import {VRFCoordinatorV2Interface} from
"@chainlink/contracts@1.1.1/src/v0.8/vrf/interfaces/VRFCoordinatorV2Interface.s
ol";

import {VRFConsumerBaseV2} from
"@chainlink/contracts@1.1.1/src/v0.8/vrf/VRFConsumerBaseV2.sol";
```

```
import {ConfirmedOwner} from
"@chainlink/contracts@1.1.1/src/v0.8/shared/access/ConfirmedOwner.sol";

contract VRFv2Consumer is VRFConsumerBaseV2, ConfirmedOwner {
    event RequestSent(uint256 requestId, uint32 numWords);
    event RequestFulfilled(uint256 requestId, uint256[] randomWords);
    struct RequestStatus {
        bool fulfilled; // whether the request has been successfully fulfilled
        bool exists; // whether a requestId exists
        uint256[] randomWords;
    }
    mapping(uint256 => RequestStatus)
        public s_requests; /* requestId --> requestStatus */
    VRFCoordinatorV2Interface COORDINATOR;
    uint64 s_subscriptionId;
    uint256[] public requestIds;
    uint256 public lastRequestId;
    bytes32 keyHash =
        0x474e34a077df58807dbe9c96d3c009b23b3c6d0cce433e59bbf5b34f823bc56
c;
    uint32 callbackGasLimit = 100000;
    uint16 requestConfirmations = 3;
    uint32 numWords = 2;
    /**
```

```
     * COORDINATOR: 0x8103B0A8A00be2DDC778e6e7eaa21791Cd364625
     */
    constructor(
        uint64 subscriptionId
    )
        VRFConsumerBaseV2(0x8103B0A8A00be2DDC778e6e7eaa21791Cd364625
)
        ConfirmedOwner(msg.sender)
    {
        COORDINATOR = VRFCoordinatorV2Interface(
            0x8103B0A8A00be2DDC778e6e7eaa21791Cd364625 );
        s_subscriptionId = subscriptionId;
    }
    function requestRandomWords()
        external
        onlyOwner
        returns (uint256 requestId)
    {
        requestId = COORDINATOR.requestRandomWords(
            keyHash,
            s_subscriptionId,
            requestConfirmations,
            callbackGasLimit,
```

```
            numWords
        );
        s_requests[requestId] = RequestStatus({
            randomWords: new uint256[](0),
            exists: true,
            fulfilled: false
        });
        requestIds.push(requestId);
        lastRequestId = requestId;
        emit RequestSent(requestId, numWords);
        return requestId;
    }
    function fulfillRandomWords(
        uint256 _requestId,
        uint256[] memory _randomWords
    ) internal override {
        require(s_requests[_requestId].exists, "request not found");
        s_requests[_requestId].fulfilled = true;
        s_requests[_requestId].randomWords = _randomWords;
        emit RequestFulfilled(_requestId, _randomWords);
}
    function getRequestStatus(
        uint256 _requestId
```

```
    ) external view returns (bool fulfilled, uint256[] memory randomWords) {
        require(s_requests[_requestId].exists, "request not found");
        RequestStatus memory request = s_requests[_requestId];
        return (request.fulfilled, request.randomWords); }
uint  serial_id;
uint timestamp;
bytes  HashSerial;
bytes  HashIMEI;
string  message;
event update_serial(
uint timestamp,
bytes HashIMEI,
bytes HashSerial  );
function log_serial(uint dev_id, uint serial_No)
public {  serial_id = dev_id;
HashSerial = bytes(abi.encodePacked(serial_No));
HashIMEI = bytes (abi.encodePacked(serial_id));
timestamp = block.timestamp;
emit update_serial(timestamp,HashSerial, HashIMEI);
}
function shareIntel(string memory newMessage) public {
message = newMessage; } }
```

pragma solidity ^0.8.25;

```
contract notification {
    uint private serial_imei;
    uint timestamp;
    uint intel_status = 0;
    event useful_intel(
        uint timestamp,
        uint intel_status);
    event notUseful_intel(
        uint timestamp,
        uint intel_status);
    function intel_useful ()
    public{
        intel_status = 1;
        timestamp = block.timestamp;
        emit useful_intel (timestamp, intel_status);}
    function intel_notUseful()
    public{
        intel_status = 0;
        timestamp = block.timestamp;
        emit notUseful_intel (timestamp, intel_status);
    }
}
```

Appendix V: Publications from Thesis

Publication One:

https://ieeexplore.ieee.org/document/9845603

A Smart Contract Approach to Cyber Threat Intelligence Sharing in Kenya

Wilson Maina; Lawrence Nderu; Tobias Mwalili

Conferences >2022 (IST-Africa Conference (IST-Africa)

A Smart Contract Approach to Cyber Threat Intelligence Sharing in Kenya

Publisher: IEEE

Wilson Maina; Lawrence Nderu; Tobias Mwalili