2021

A Blockchain-based prototype for cybersecurity threat intelligence sharing: a case of Kenyan banking and insurance financial institutions.

Kibuci, Wanjohi Stephen

Strathmore Institute of Computing and Engineering Sciences

Strathmore University

A Blockchain-Based Prototype for Cybersecurity Threat Intelligence Sharing: A Case of Kenyan Banking and Insurance Financial Institutions

By

Wanjohi Stephen Kibuci

124535

A Thesis Submitted to the School of Computing and Engineering Sciences in partial fulfillment of the requirements for the award of a Degree of Master of Science in Information Technology of Strathmore University

Master of Science in Information Technology

Strathmore University

May 2021

Abstract

Cybersecurity threats to financial institutions have become more sophisticated and challenging to deal with. The growing dependence of financial institutions on the cyberspace makes cybersecurity preparedness against threats important to achieve a financial institution's mission and vision. In this context, cybersecurity preparedness is the process in which a financial institution can protect against, prevent, mitigate, respond to and recover from cyber threats. Traditionally, most organizations share threat intelligence through ad hoc methods such as emails and phone calls but there is a need to automate threat intelligence sharing where possible to improve cybersecurity preparedness. To address this issue, enhance cybersecurity and trust, a blockchain-based approach can be employed to share threat intelligence. This study aims to leverage blockchain technology by developing a prototype to automate cybersecurity threat intelligence sharing in financial institutions. The study used a quantitative approach in data collection using structured online questionnaires with close-ended questions and open source datasets and data analysis using several analytic tools. The prototype has been developed using the Rapid Application Development software development methodology using open source Oracle Virtual Box that runs on Linux Operating System.

Acknowledgments

I am grateful to God for giving me the strength and wisdom to complete this study. I would like to express my gratitude and appreciation to my supervisor, Dr. Bernard Shibwabo for his timely guidance and constructive feedback from the start to the completion of this research. I would also like to acknowledge Dr. Vincent Omwenga for his input on the research through the thesis seminars. I would like to thank the respondents for their time and input to this study.

List of Figures

Definition of Terms

Cyberattack – Any malicious attempt by a person, a group of people or even an institution to trespass the information systems of another person or institution. The adversary or attacker usually benefits from disrupting the victim's system or network in a monetary manner (Cisco, 2020).

Cybersecurity – A best practice of the protection of information systems, networks and applications from cyberattacks that aimed at accessing, modifying or deleting sensitive information, interrupting normal business processes or extortion of money (Cisco, 2020).

Cybersecurity Preparedness - The process that an institution or government ensures has it has developed, tested and verified its own ability to prevent, mitigate and recover from cybersecurity incidents (Lukin, 2019).

Cyber resilience - The ability of how apt an organization or financial institution can manage cyberattacks despite hostile cyber events (Björck et al., 2015).

Threat Intelligence – The information of cyberattacks that have been received in computer systems and shared experiences in cyber security within organizations as a means to counter these threats (Wu et al., 2019).

issues. These financial institutions need establish cybersecurity best practices to protect their systems and infrastructure and redesign their information security approaches.

Numerous organizations invest heavily in technology controls and defenses to prevent cyber risk but fail in assessment, transferring risk, planning for proper cyber response and other risk management areas that strengthen cybersecurity preparedness (Marsh and Microsoft, 2019). According to the 2019 Global Cyber Risk Perception Survey (Marsh and Microsoft, 2019), it was found that there was a significant decrease in confidence of companies and organizations in three critical areas of cybersecurity resilience. Survey participants that stated they had 'no confidence' increased from 9% to 18% for cyber risk assessment, from 12% to 19% for cyber threat prevention and from 15% to 22% for cyber event response and recovery.

Using blockchain technology has been recently advocated by research communities and gained momentum in the financial services industry. Blockchain technology has the potential to bring technological breakthroughs in the financial industry in four areas in particular: infrastructure, platform, channel and scenario (Choi & Huang, 2021). Blockchain provides infrastructure for sharing information in a secure way, automating registration processes and detecting fraudulent facilities. The cross interoperability of blockchain is important for facilitating it as a medium for exchange in the financial sector (Choi & Huang, 2021). Sharing of threat intelligence within organizations is being encouraged to have a broad perspective of the current cybersecurity posture and this in turn, increases and improves the levels of cyber preparedness and situational awareness (Wu et al., 2019).

1.2 Problem Statement

Financial institutions are dependent on the internet for their services and this dependence exposes new vulnerabilities in financial systems and malicious attempts to exploit vulnerabilities from attackers (Healey et al., 2018). Healey's paper continues to state that cyber criminals, who target core financial infrastructure, can potentially spark a financial crisis if the financial systems are already fragile.

Traditionally, sharing of threat information occurred through ad hoc methods such as email exchange, instant messaging clients, ticketing systems and phone calls where employees use these

i. To investigate the challenges in sharing cybersecurity information by financial institutions.

ii. To analyze frameworks and approaches used for cybersecurity preparedness in financial institutions

iii. To review existing platforms used for threat intelligence sharing

iv. To develop a blockchain-based prototype for sharing threat intelligence in financial institutions

v. To test the functionality of the developed prototype

1.4 Research Questions

The research questions of the study are:

i. What are the challenges in sharing cybersecurity information in financial institutions?

ii. What are the frameworks and approaches used for cybersecurity preparedness in financial institutions?

iii. What are the existing platforms used for threat intelligence sharing?

iv. How can a blockchain-based prototype for sharing threat intelligence in financial institutions be developed?

v. How can the functionality of the prototype be tested?

1.5 Justification

Financial institutions are generally reluctant when it comes to information sharing and avert sharing any information that is beyond their compliance with regulations. A decentralized approach can provide solutions in addressing this issue with the use of blockchain technology to be specific. Blockchain technology enables these institutions with information sharing through a shared distributed ledger in a secure manner thus providing distributed trust. Where two or more financial institutions have a memorandum of understanding to share threat intelligence amongst themselves, anonymity property of blockchain can deployed where the sender and receiver identities are unknown.

Chapter 2: Literature Review

2.1 Overview

This chapter focuses on understanding the cyber threats that financial institutions face, how cybersecurity preparedness takes place and how threat intelligence works. It discusses different frameworks currently used for cybersecurity preparedness and how blockchain technology works. It focuses on identifying existing blockchain-based architectures and designs that will form basis to the development of a prototype for improving cybersecurity preparedness within a financial institution.

2.2 Empirical Framework

The Communication Authority of Kenya (CAK) is responsible for sharing the latest statistics on the national cyber threat landscape. According to the Sector Statistics Report for the Financial Year 2020/21 (April-June 2021), there were 38,776,699 cyber threat attempts that were detected by the Kenya Computer Incident Response Team (KE-CIRT/CC). The cyber threats that are focused on are system vulnerabilities, different malware events, phishing attacks, botnets and web application attacks (Communication Authority of Kenya, 2021).

There has been a 37.27% increase in the number of cyber threats detected from the previous period, January to March 2021 because cyber threats are continuously evolving at a faster speed than the development of cyber defenses. The KE-CIRT/CC has put in place initiatives and best practices that are aimed at ensuring financial institutions have enhanced cybersecurity preparedness and cyber resilience to ensure sustainability in the financial sector. Table 2.1 summarizes the detected cyber threats (Communication Authority of Kenya, 2021).

Table 2.1: KE-CIRT/CC Cyber Threats Detected in Financial Year of 2020/2021

Cyber Threat	Apr - Jun 21	Jan - Mar 21	Variation (%)
Malware	23053190	21559181	6.92
DDOS/Botnet	2564173	2890847	-11.30
Web App Attacks	11272402	3767588	199.19
System vulnerabilities	1886934	30203	6147.51
Total	38776699	28247819	37.27

understood before considering exposure of the system to cyber threats (Nweke & Wolthusen, 2020; Shostack, 2014; Stewart et al., 2018).

2.3.1.2 Threat Categorization and Classification

The STRIDE model, created by Microsoft, was developed with the aim of assisting information security engineers understand and classify all possible threats (Khan et al., 2017; Shevchenko et al., 2018; Stewart et al., 2018) STRIDE is an abbreviation for the following threats:

i. Spoofing – This is a cyberattack where successfully gaining access to a system is the main goal using false identity. It can be used against logical identification such as usernames, email addresses, IP and MAC addresses.
ii. Tampering – This is any action that results to data manipulation or unauthorized changes, whether data is in transit or at rest. Tampering can alter static information or manipulate communications. These attacks violate data integrity and data availability.
iii. Repudiation – This is a situation where a user denies that they have performed systems actions or activities. Attackers can use attacks in repudiation to avoid taking responsibility for their actions and the attacks affect innocent users of the system who are blamed for security violations.
iv. Information disclosure – This means distributing, revealing or disclosing of private/confidential data such as health information, employee identity information to external third parties or unauthorized entities. Information disclosure also includes privacy breaches and data leaks.
v. Denial of service (DoS) – A cyberattack that involves the attacker or perpetrator exploits a vulnerability of the system to disrupt the authorized access to a resource, such as a website, temporarily or indefinitely. This can be done through traffic flooding or connection overloading.
vi. Elevation of privilege – This is a cyberattack where an employee's account that has limited permissions and access rights becomes an account with a higher level of privilege and access. This can be achieved by exploiting or stealing the credentials of an account with more privileges such as an administrator account or application developer account.

Effective management of threat information had led to the creation and enhancement of threat intelligence platforms (TIPs). TIPs are cyber threat repositories that enable institutions to aggregate, assess and interpret intelligence from external sources. A TIP's ultimate objective is to disseminate threat intelligence that will be fixed into the organization for better decision making (ENISA, 2019).

2.3.4 Blockchain Technology

Blockchain technology is often referred to as a combination of technologies used in decentralized networks with the aim of achieving transparent, security and consistency by maintaining a digital ledger which consists of a series of transactions. Blockchain technology has a wide range of applications across different domains including information sharing (Ayoade et al., 2018).

According to Ayoade's study (2018), the following are blockchain characteristics:

i. Immutability: This is the ability of the digital ledger to remain unchangeable because the ledger records every transaction and subsequent blocks protect the transactions due to the nature of hash algorithms.
ii. Decentralization: Blockchain has consistent public digital ledger that replaces the central server. Blockchain uses distributed consensus algorithms and mechanisms to deliver a consensus view of the digital ledger among the users.
iii. Anonymity: Users remain anonymous using generated addresses as they interact with the blockchain. The advantages of these addresses is that they are indirectly connected to identities of the real world and users can avoid exposing their identities by possessing many different generated addresses.
iv. Transparency: Each transaction on the ledger is traceable to prior transactions thus the high level of transparency as the ledger becomes tamper proof during data storage.

The first blockchain technology implementation that captured people's attention was Bitcoin (Nakamoto, 2008). Examples of popular blockchain technologies are Ethereum, which is a blockchain platform that allows creation of smart contracts on blockchain (Buterin, 2013), and Hyperledger (2018) created to advance cross-industry blockchain technologies.

All clients receive updated threat intelligence from the TAXII server as long as they are subscribed to the server. These clients shift into servers, delivering their threat information to the TAXII server for threat intelligence sharing. This mechanism runs on the cloud.

2.3.5 Laws and Regulations around Cybersecurity and Information Sharing in Kenya

2.3.5.1 Cyber Security and Protection Bill of 2016

The Cyber Security and Protection Bill was published in July 2016. The bill proposes to reinforce the law on cybercrimes and to establish the National Cyber Security Response Unit, a Kenyan governmental agency that has the authority to investigate cyberattack incidents and prosecute cyber criminals. There are specific cybercrime acts such as such as phishing and cybersquatting that the Bill legislates. In addition, the Bill creates an obligation on all computer and information system users to report all incidents of cyberattacks and intrusions to the Unit (Kenyan Gazette, 2016).

2.3.5.2 Computer Misuse and Cybercrimes Act of 2018

The Computer Misuse and Cybercrimes Act was enacted in May 2018 and aims to protect the confidentiality, integrity and availability of computer systems, applications and data as well as facilitate the prevention, detection, investigation, prosecution and punishment of cybercrimes. Some of the cybercrimes that the Act has established including unauthorized interference or interception of computer systems, cybersquatting, identity theft, computer forgery, fraud and unauthorized disclosure of passwords (Kenya Gazette, 2018).

2.3.5.3 Kenya Information and Communication Act (Amendment) Bill of 2019

The Kenya Information and Communication Act (KICA) is a law that was first passed in 1998, amended in 2013 and amended again in 2019. The Communications Authority of Kenya (CAK) is responsible for licensing and regulation of information and communication services in accordance to the provisions of KICA. According to the Act, some of the functions of CAK are to develop frameworks for investing and prosecuting cybercrimes, facilitate and promote cybersecurity practices in electronic transactions by ensuring reliability in those electronic records (Kenya Gazette, 2019).

2.4 Frameworks and Models

2.4.1 Cyber Prep Framework

Bodeau et al. (2010) developed a cybersecurity preparedness framework called Cyber Prep that uses a structured approach that addresses an organization's threats by facilitating cyber security strategic planning and determining the cyber preparedness levels necessary to ensure the success of the organization.

The five levels in the framework for organizational preparedness that are labelled as per the cyberattack's nature and rigidity or as per the attacker, plus possible strategies for cyber preparedness that can counter against such threats. Cyber Prep levels are categorized in terms of the organization's view to the cyber threats it faces, the strategy of the organization for countering the cyber threats and how the organization approaches governance of information security. Table 2.1 summarizes the cyber threats and their preparedness levels (Bodeau et al., 2010)

Table 2.2: Cyber Threat and Preparedness Levels (Bodeau et al., 2010)

Level	**Cyber Threat Level**	**Cyber Preparedness Level**
1	Cyber Vandalism	Perimeter Defense
2	Cyber Theft or Cyber Crime	Critical Information Protection
3	Cyber Incursion or Cyber Surveillance	Responsive Awareness
4	Cyber Sabotage or Espionage	Architectural Resilience
5	Cyber Conflict or Warfare	Pervasive Agility

Each Cyber Prep level has its own descriptions and its characteristics that it is associated with such as adversaries or attackers, defensive schemes and the techniques as summarized in Table 2.2. It is very crucial for senior management and the board of directors to understand the issues of cybersecurity preparedness and they need to be committed to improving the posture of cybersecurity of the organization because the progress from one level of Cyber Prep framework to the next will be inconsistent and incomplete.

2.4.2 FFIEC Cybersecurity Assessment Tool

The Federal Financial Institutions Examination Council (FFIEC) is a United States of America governmental body that consists of five banking regulators. FFIEC promote uniformity in principles and standards in the supervision of financial institutions. The FFIEC developed a diagnostic Cybersecurity Assessment Tool (CAT) that assists companies and financial institutions to identify their risk levels using risk profiles and assess the levels of their cybersecurity maturity (FFIEC, 2017).

The FFIEC's tool uses practices and processes to measure risk levels across several categories that include factors such as the institution's characteristics. The FFIEC tool allows senior management to make strategic decisions that are risk driven by using standard and selected risk assessment criteria through regular cybersecurity assessments (FFIEC, 2017).

The FFIEC's Cybersecurity Assessment Tool (2017) has two parts:

i. Inherent Risk Profile - Performed to determine an organization's current cybersecurity risk posture by identifying activities and services of the organization.
ii. Cybersecurity Maturity Assessment Level – After the inherent risk profile, the maturity level identifies the cybersecurity preparedness level of an organization by reviewing each domain and their assessment factors. The five domains are explained below and illustrated on Figure 2.2:
    a) Cyber Risk Management and Oversight: This domain addresses oversight on the board of directors in reference to strategies, policies and procedures, organization culture and training.
    b) Threat Intelligence and Collaboration: This domain involves the management team grading the institution in reference to threat intelligence, analysis and relevant stakeholders that promote the sharing of cyber threat information.
    c) Cybersecurity Controls: This domain involves the assessment of detective, preventive and corrective controls.
    d) External Dependency Management: This domain delves into establishing programs to oversee and manage third parties and other external connections that have organizational access to technology assets and information.

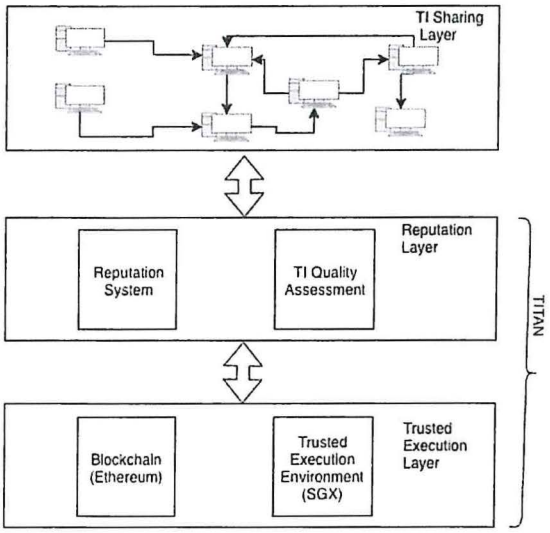


Figure 2.3: TITAN Architecture (Wu et al., 2019)

According to Wu et al. (2019), the TITAN system architecture has three layers:

i. Threat Information (TI) Sharing Layer: In this layer, the threat intelligence is shared within a community. The layer lies outside the TITAN framework but uses the TITAN services.

ii. Reputation Layer: This layer is the core layer of the system and handles the core functions that comprise of two parts, the reputation system that uses algorithms such as EigenTrust and the TI Quality Assessment that does the calculation of score data.

iii. Trusted Execution Layer: This layer consists of two components, the Trusted Execution Environment (TEE) and the blockchain. The functions of the blockchain are to store trust score data, provide security and to maintain integrity by preventing unauthorized modification of the scores. The functions of the TEE component are nearly similar to the blockchain in that it provides cybersecurity and maintains integrity for the TI algorithm for quality scoring by preventing tampering of the data or unauthorized modification.

branch of the institution. The peer maintains a ledger copy physically and is an interface to the client.

iii. Certificate Authority (CA): The Hyperledger Fabric Certificate Authority server will run an instance by each financial institution. The CA will circulate certificates to participants in the blockchain network for authentication. However, in the real world deployment of the model, real life certificate authorities such as DigiCert and Let's Encrypt issue the certificates.

iv. Chaincode: The chaincode is installed on selected peers and consists of hosted components that must be installed depending on the chaincode count and those deployed per channel component. The chaincode is idle and only activated by an 'INVOKE' event.

v. Application Programming Interface (API): The API handles interactions from the client between the peer nodes.

vi. Client: The client is a container that hosts an application instance.

vii. Command Line Interface (CLI): The CLI is the interface where commands are run during implementation and testing.

2.6 Existing Threat Intelligence Solutions

2.6.1 Open Source Threat Intelligence Platforms

2.6.1.1 Collaborative Research into Threats (CRITs)

CRITs is a free and open source threat repository that capitalizes other open source software to create a unified tool. Security analysts and experts who engage in cyber threat defense use the tool. Its ultimate goal is to provide an open platform to the information security community for analyzing and collaborating on threat information. CRITs is web-based written in Python and combines an analytic engine with a cyber threat database that serves both as a repository for cyberattack data and as a platform for conducting malware analysis. The CRITs API is accessible through a simple REST API (CRITs, 2020).

2.6.2.3 EclecticIQ

EclecticIQ Platform allows security analysts and experts to perform investigations while disseminating intelligence. The EclecticIQ Platform Workflow supports a wide range of use cases for security analysts and experts working within high-risk industries. The platform provides a core set of workflows and are designed for the real-world analysis of cyber threat intelligence (EclecticIQ, 2020).

2.6.3 Community-Based Threat Intelligence Platforms

2.6.3.1 Alienvault Open Threat Exchange (OTX)

Alienvault Open Threat Exchange (OTX) is the "neighborhood watch" of the global intelligence community. OTX enables private institutions, independent security experts and government agencies to collaborate, share the latest information about emerging threats and promote security across the entire community (AlienVault, 2020).

In OTX platform, any individual or institution in the cyber security community can contribute, discuss research, verify and share threat information. An individual or institution can integrate threat information from OTX directly into AlienVault and other third-party security products so that the threat detection defenses are updated with the latest cyber threat intelligence. As of July 2020, OTX has over a hundred thousand users in 140 countries who share over 19 million threat indicators on a day-to-day basis (AlienVault, 2020).

2.6.3.2 Facebook Threat Exchange

Threat Exchange is a set of RESTful APIs on the Facebook Platform for querying, publishing, and sharing security threat information. It is a lightweight way for exchanging details on malware, phishing pages, and other threats with either specific members of the community or the Threat Exchange community at large. Facebook created Threat Exchange for participating individuals and institutions with the purpose of sharing threat information using a convenient and easy-to-use API that provides privacy controls to enable sharing. Threat Exchange has a graphical user interface you can use to quickly and interactively do things like upload descriptors, run queries, create and assign tags, view/edit privacy groups, and so on (Facebook for Developers, 2020).

blockchain consensus mechanism that provides fault tolerance. This will lead to the generation of an incident report that one of the users (CI1 - CIn) produces. This incident report is automatically handled using instructions that have been programmed and goes through the smart contracts (Graf & King, 2018).

2.7 Proposed Conceptual Framework

The conceptual framework will have the blockchain network administrator as the main actor who does the administration of the system including access control and user creation. Authorized users will be allowed to share threat intelligence amongst themselves over the blockchain network. All cyber threat information, user requests and access control policies will be stored on the database.

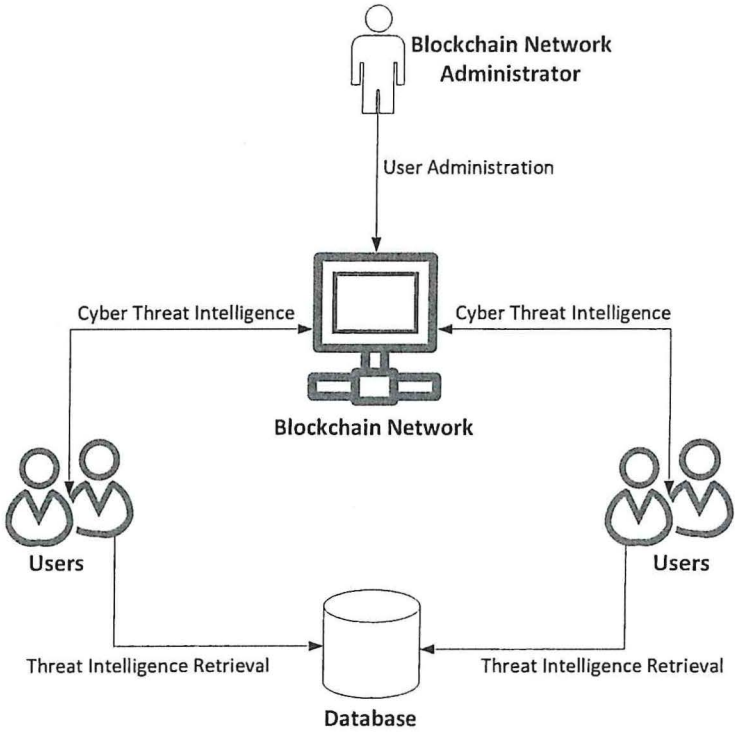


Figure 2.6: Proposed Conceptual Framework

This is turn results in greater efficiency of the project, faster prototype development and effective communication. RAD consists of four main phases as shown in Figure 3.1.

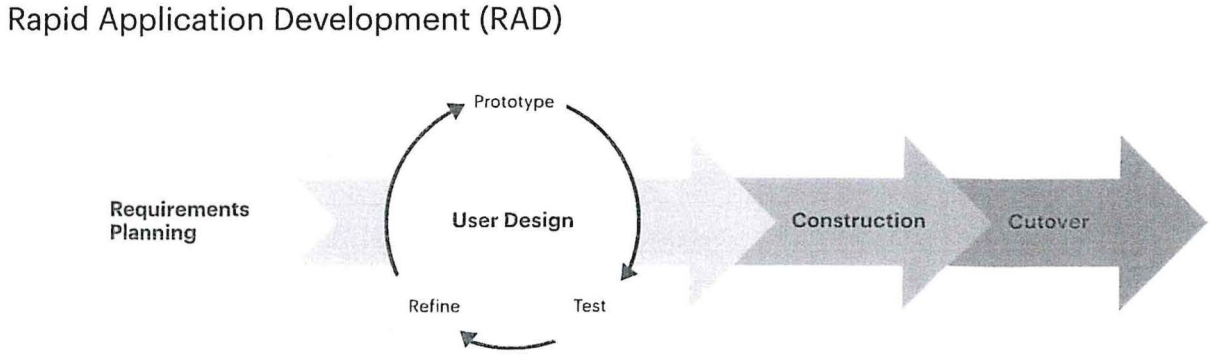


Figure 3.1: Rapid Application Development Methodology (Hamzah et al., 2019)

3.3.1 Requirements Planning Phase

During this stage, the researcher determines business needs, project scope, goals and expectations of the prototype to be built through data collection methods of questionnaires and datasets. The researcher needs to address current and potential problems that might occur during the construction of the prototype. At this stage, all planning in the construction of the prototype is determined (Hamzah et al., 2019).

3.3.2 User Design Phase

After completion of planning the system requirements, development began by building user designs through various prototype iterations. The process is similar to developing customizable software where users can test every product prototype, at every stage, to make sure it meets expectations. All bugs and errors were resolved in a repetitive process. The researcher designed the prototype, users tested it and they communicated on what works and what does not. This method gave the researcher the opportunity to change the model as they wished until they reach a satisfactory design. Unified Modeling Language (UML) software, Visual Paradigm and Lucid Chart, were used to design UML diagrams such as use case diagrams and class diagrams.

3.5 Sampling Population

The sampling population, also referred to as the study population, is a whole group such as citizens in a county, an organization's clients, community residents or in the case of this study, the number of financial institutions in a particular area (Kumar, 2019). According to the 2018 CBK Bank Supervision Annual Report (CBK, 2018), there are 43 banking institutions and the 2017 Insurance Industry Annual Report (Insurance Regulatory Authority, 2018) states there are 52 licensed insurance companies bring the total population for this research to 95 financial institutions.

3.6 Sampling

Sampling is the selection of a few respondents, a sample, from a larger group, the sampling population. The aim of sampling is to form the basis for estimating the frequency of specific information of the researcher's interest (Kumar, 2019). A convenience sampling approach, a type of non-probability sampling, was used in the research guided by the researcher's convenience with regard to selection of respondents such as accessing respondents easily, availability of the respondents, respondents within the researcher's vicinity (Kumar, 2019). Slovin or Yamane formula is used to determine sample size for general cases where there is unknown distribution (Adam, 2020). Denoting by n the sample size, Slovin or Yamane formula is given by:

$$n = \frac{N}{(1+N(d))^2}$$ where N is the total population size and d is the margin of error.

Given the population is 95 financial institutions with a confidence level of 95% and margin error is 0.05, the sample size becomes 77 financial institutions. Using a convenience sampling approach, ten financial institutions, both banking institutions and insurance companies, located in Upper Hill were selected which is 10% of the original total population and 13% of the sample size from the Slovin/Yamane formula.

3.7 Data Collection

The study used different approaches to get both primary and secondary data such as questionnaires as the primary data collection method.

3.10 Ethical Considerations

Due to the confidential nature of the data on cyber threats, the researcher obtained consent from the selected participants and the Strathmore University Institutional Ethics Review Committee (SU-IERC).A research permit was also awarded by the National Commission for Science, Technology and Innovation (NACOSTI). The online questionnaires required having disclaimers and thereby, permission was granted from the respondents to participate in the study through the questionnaires and follow up questions. The immutability of data was provided by the blockchain framework which allowed the prototype to be easily accessible to the users but must be kept confidential. Data gathered was protected and used for the sole purpose of this research.

3.11 Dissemination of Research Results

Disseminating the results was appropriate because it promotes higher quality research, instills trust between the researcher and the participant and allows the participants have a sense of ownership of the results (Purvis et al., 2017). The participants were able to view a summary of the results from the questionnaire but they were notified that it is for academic purposes. The summary of results was presented in form of graphs and charts in dashboards on Survey Monkey via a link but confidential information was not be shared. The thesis shall be accessible online via the Strathmore University Library for access by the general public.

3.12 Utilization of Research Results

The results of the research are exclusively for academic purpose only. The results were used to form the basis for the development of the cyber threat intelligence sharing prototype. This will assist financial institutions improve their cybersecurity preparedness, enhance their cyber resilience and promote best practices in their cyber threat landscape.

4.2.2 Financial Institution Context Results

From the questionnaire under the Financial Insitution Context section, 100% of respondents agreed that employee error posed the most significant threat to their financial institution as illustrated in Figure 4.2. Criminal organizations, hackvist groups and insider threats are tied at second with 85.71% as the most significant threats. Figure 4.3 shows that the primary cyber threat concern is the denial of service or business disruption with 85.71% of the responses. The second most selected cyber threat concerns were operational data integrity, system and communication availability and loss of reputation with 71.43% of the responses.

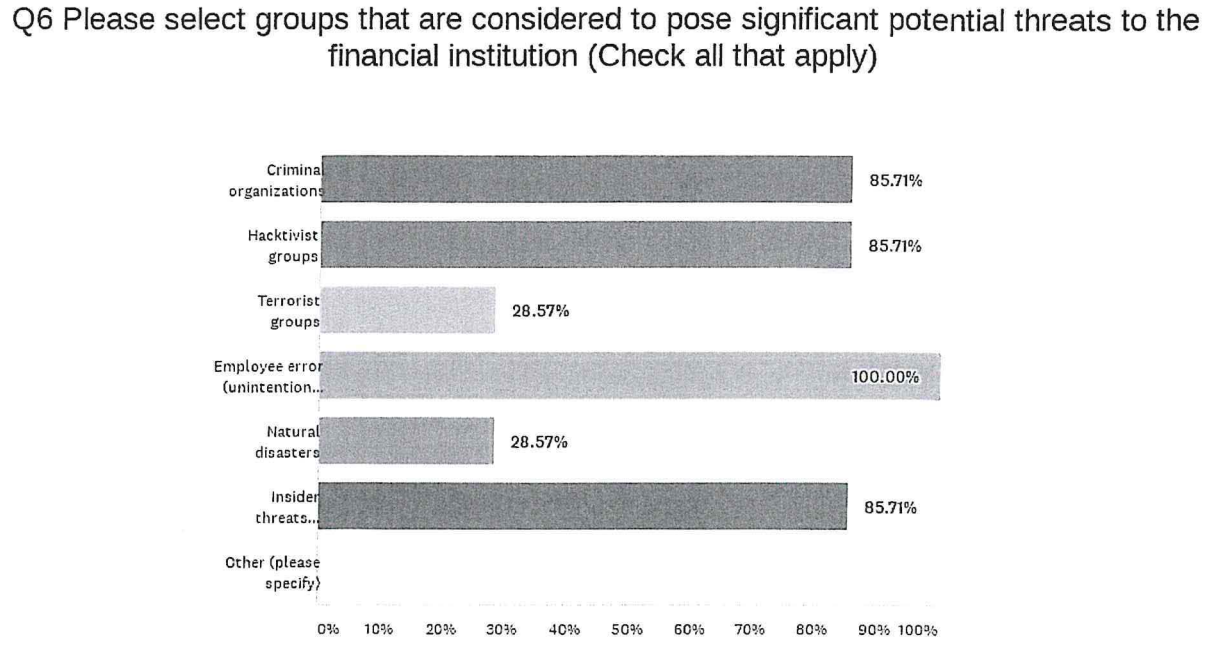


Figure 4.2: Groups That Pose Potential Threats

Q16 Most users are knowledgeable about detecting intrusion attempts.

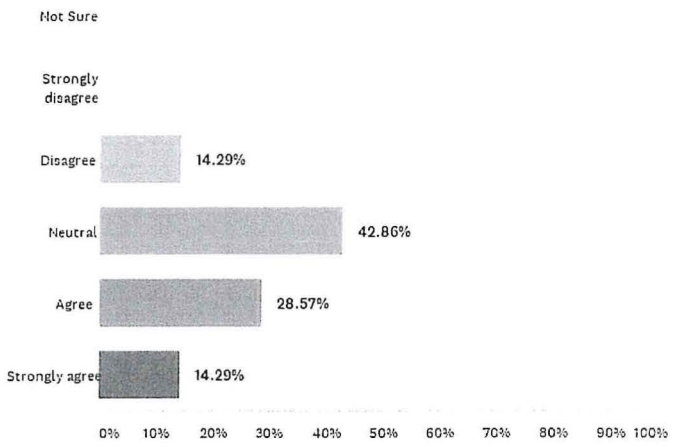


Figure 4.4: User Knowledge on Intrusion Attempts

Figure 4.5 shows that 42.86% of the respondents provide continuous and ongoing training on cybersecurity awareness while 28.57% provide training in response to specific cyber threats occurring. Another 28.57% of respondents offer training at least once annually.

Q17 How often does the financial institution provide any user training on cybersecurity awareness?

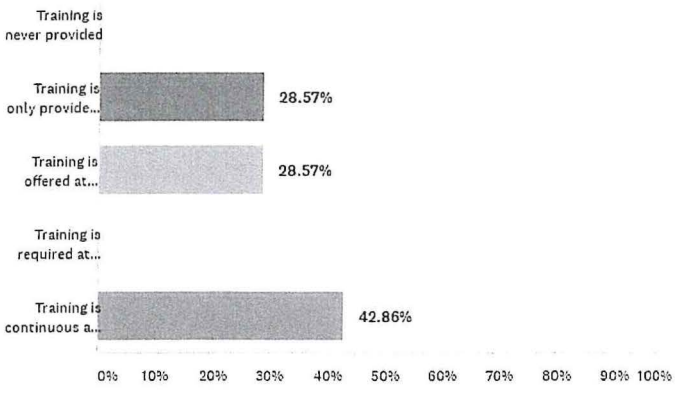


Figure 4.5: Frequency of User Training on Cybersecurity Awareness

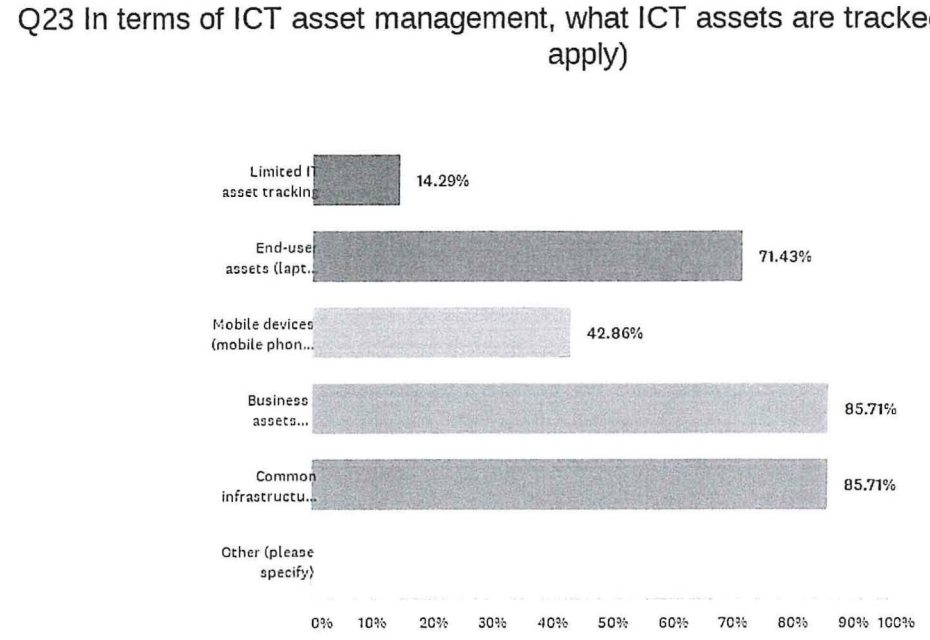


Figure 4.7: Tracked ICT Assets

4.2.5 Internal Process and Collaboration Results

Figure 4.8 illustrates that all the respondents stated that there is regular communication between the cybersecurity/ICT team and the senior management on cybersecurity while 85.71% of the respondents stated cybersecurity/ICT team have departmental communication. 57.14% of respondents stated that it takes 1 to 4 hours for the cybersecurity or ICT team to alert the financial institution to a significant threat.

In terms of level of communication and cooperation, 57.14% of the respondents stated that cyber threat intelligence and cyber tool tuning are well integrated in their institutions as illustrated in Figure 4.10.

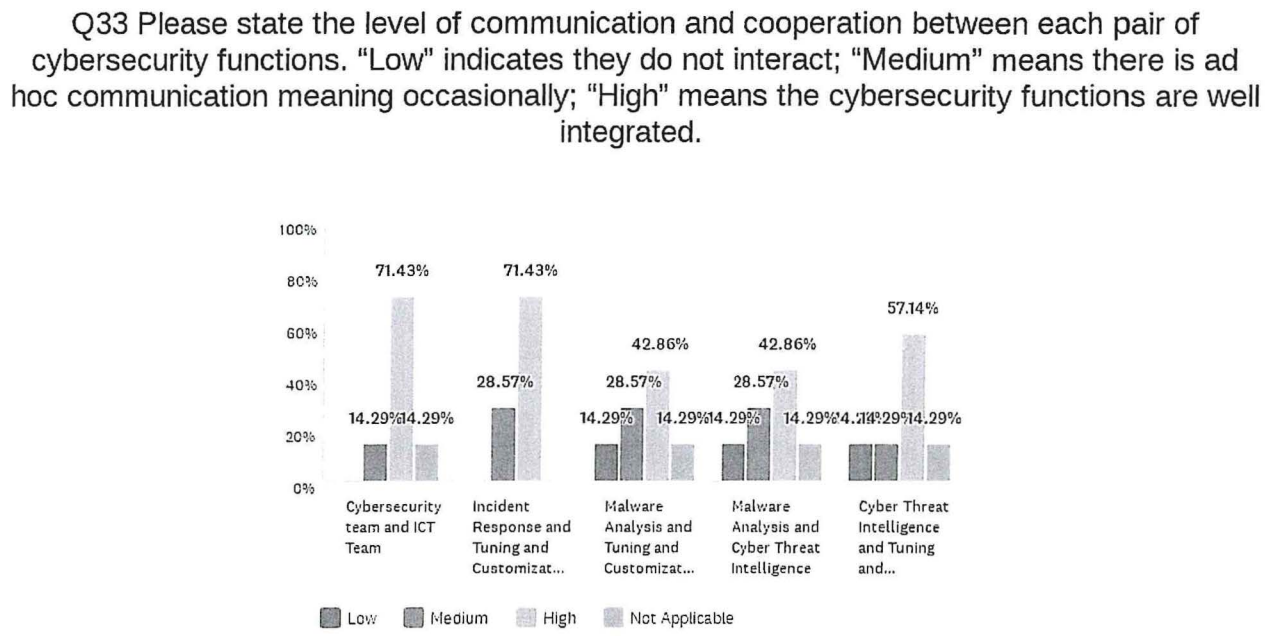


Figure 4.10: Level of Communication and Cooperation between Cybersecurity Functions

4.2.6 Tracking and Analysis Results

In tracking of the cyber threats, 57.14% of the respondents use databases to track their cyber threat indicators. Another 28.57% use spreadsheets and 14.17% use an internet portal as shown in Figure 4.11. The types of indicators collected include domain names which 100% of the respondents collect and email addresses and Uniform Resource Locators (URLs) which 85.71% of respondents collect. Figure 4.12 illustrates the incidental details that are collected by the indicators and 100% of respondents collect the date the cyber incident was added. Other cyber threat indicators include sources of the cyber threats and actions taken to those threats where 85.71% of respondents track them.

Figure 4.13 shows the cyberattack or incident data that is collected. The most collected data are affected assets and how the attack was stopped if it was prevented. Data also collected was number of cyber threat incidents.

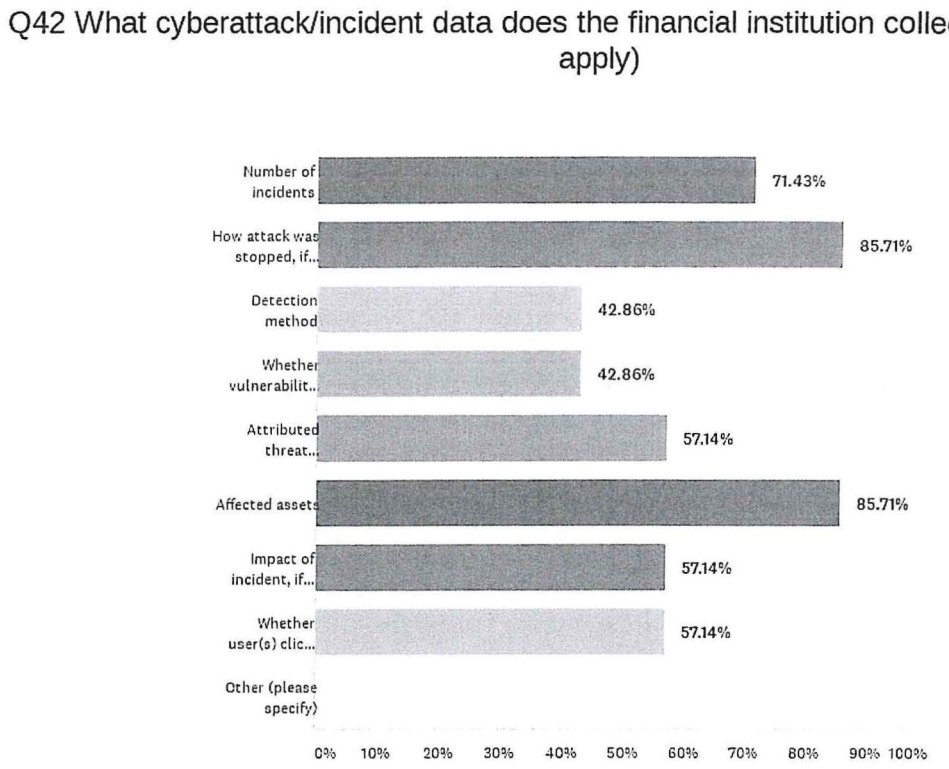


Figure 4.13: Cyber Incident Data Collected by Financial Institution

4.2.7 External Engagement Results

The main sources of potential cyber threats are the internet and the users who report on suspicious activity with 100% of respondents selecting them as seen in Figure 4.14. Other sources of information on cyber threats include social media with 85.71%, government and law enforcement, vendor reports and threat sharing peers with 71.43%. Only 57.14% of the respondents stated that the information comes from the regulator, either CBK or IRA. Figure 4.15 shows the mechanisms used to share threat intelligence. All the respondents use private communications to share threats and 71.43% of the respondents also use email distribution lists and face-to-face meetings.

Figure 4.16 shows the reasons why these financial institutions participate in threat sharing. The main reason was to protect their customers with 100% of the respondents stating so. Other reasons include improving the institution's cybersecurity posture and learn the best cybersecurity practices with 85.71% of the respondents of the selection.

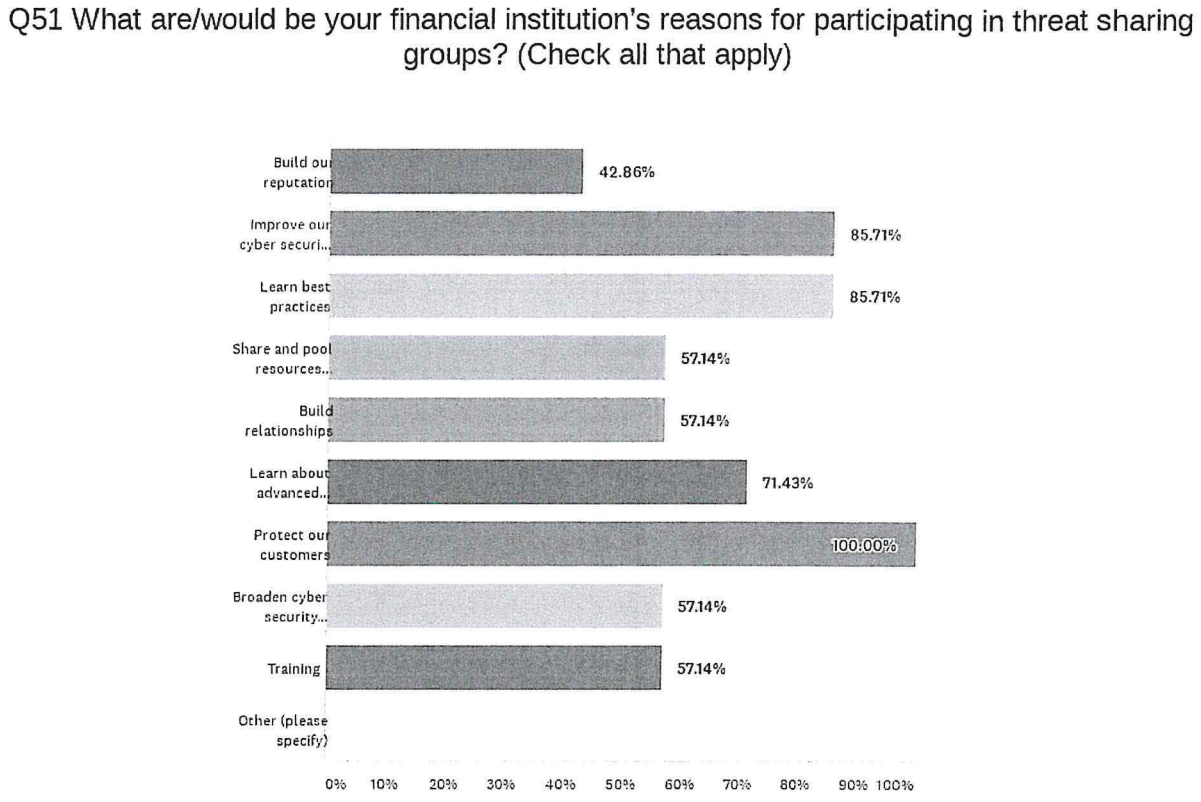


Figure 4.16: Reasons for Participating in Cyber Threat Sharing

When asked what factors limit the respondents from sharing threat intelligence with other institutions, 85.71% of them stated level of trust while 71.43% stated competition and lack of sharing agreements as illustrated in Figure 4.17.

4.3.2 Functional Requirements

Functional requirements are those that the prototype must be able to accomplish in terms of input fed to it (Cossentino et al., 2014). The functional requirements for blockchain prototype include:

i. Allow the blockchain network administrator to register, edit and delete users of the prototype.
ii. Allow the blockchain network administrator to grant, deny or revoke user access and permissions to the prototype.
iii. Registered users should be able to log into the prototype.
iv. The prototype should allow users to input cyber threat data from the user interface after a cyber threat incident.
v. Allow authorized users to share threat intelligence to the other authorized users.
vi. The prototype should be able to send alerts on cyber threats via email.
vii. Allow authorized users to view all cyber threat intelligence in the system.

4.3.3 Non-Functional Requirements

Non-functional requirements are those global constraints offered by a system and do not directly affect how the system works successfully (Cossentino et al., 2014). The non-functional requirements for blockchain prototype include:

i. Performance - The prototype should have a fast response time that is desirable to the users
ii. Reliability - The prototype should be available to users and maintain zero to minimal downtime
iii. Security - Due to the nature of threat information being shared by the financial institution, only authorized users should have access to maintain confidentiality and integrity
iv. Usability – The prototype should be easy to use for users
v. Scalability - The prototype should be designed that more modules can be added easily
vi. Compatibility - The prototype should be accessed through many different operating systems

b. **Peers**: Two peers, one of them anchor, are deployed for each organization in the network. Anchor peers are discoverable by Orderer and peers in different organizations through gossip data dissemination protocol. They receive updates and broadcast them to the other peers in their organization. In the setup, anchor peers are also endorsing peers which execute transaction proposals.

c. **Certificate Authorities (CA)**: They carry out the task of distributing the certificates to network participants. Then these certificates are used to authenticate members. A Fabric CA server instance is being run by each organization in the blockchain network. Each CA server issue certificates with previously generated cryptographic materials. Fabric has also the ability to interoperate with real certificate authorities in real-world deployments.

d. **CouchDBs:** In order to store ledger state, there are two options: LevelDB and CouchDB. In the blockchain network, the CouchDB is used as state database and a CouchDB instance is running for every peer.

e. **Chaincode:** After the instantiation of installed chaincodes, these components are activated and chaincode runs in this isolated environment.

f. **API**: Available Fabric SDKs allow client applications to connect with the blockchain network. SDK developed for Node.js is used in the prototype.

g. **Channel**: The channel maintains the confidentiality and privacy of the chaincode and the ledger by giving authorization only to the authentic channel participants. A peer connected to one channel cannot access to the ledger and the chaincode of another channel of which peer is not a participant.

v. **Client:** The client application is utilized to interact with the blockchain network by using RESTful APIs which provide the CTI sharing service to the organizational user.

vi. **HTTP Server:** HTTP server receives request from organizational entities. As a first step, the HTTP server needs to be connected to the CA server for admin identity enrollment and for user registration using the admin identity. Second, the registered user specifies the unique channel name and smart contract name using Fabric Node.js SDK and initiates the particular smart contract on the desired channel.

4.5.1 Use Case Diagram

Use case diagrams are created during early phases of software development. They are important for validating and documenting the system behavior and act as a contract between the developer and the system users (Sabharwal et al., 2017). The use case diagram is shown on Figure 4.19.

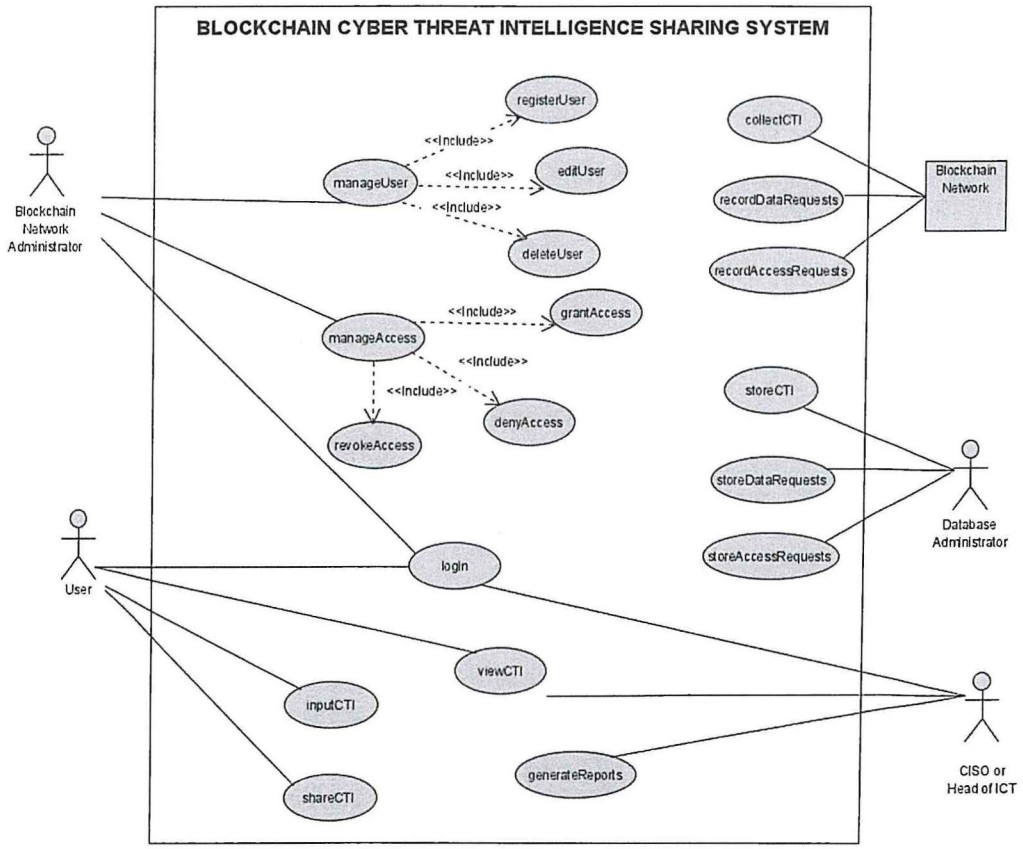


Figure 4.19: Use Case Diagram

The descriptions of the main use cases are summarized and explained in Table 4.1.

Table 4.1: Prototype Use Case Descriptions

Use Case Name	**login**
Description	The actors log into the system

Post condition	Access is granted to the users to input, view or share cyber threat intelligence
Main Success Scenario	For granting user access i. Blockchain Network Administrator views access request from user ii. Blockchain Network Administrator grants the user access to view or share the cyber threat intelligence iii. System sends user a message that access has been successfully granted
Use Case Name	**inputCTI**
Description	Users input cyber threat intelligence into the system
Primary Actor	User
Precondition	The user has to be granted permission to input the data
Post condition	Data has been posted successfully in the system
Main Success Scenario	Data has been recorded and stored in the database
Use Case Name	**shareCTI**
Description	User shares cyber threat intelligence with other users
Primary Actor	User
Precondition	The user must be granted permission to share cyber threat intelligence with other users by the Blockchain Network Administrator
Post condition	Authorized users receive the cyber threat intelligence
Main Success Scenario	Cyber threat intelligence is shared to users
Use Case Name	**viewCTI**

Use Case Name	**recordDataRequests**
Description	The Blockchain Network records all data requests in the prototype
Primary Actor	Blockchain Network
Precondition	None
Post condition	All data requests from the users will be recorded by the Blockchain Network
Main Success Scenario	The Blockchain Network will automatically record all data requests in a ledger
Use Case Name	**recordAccessRequests**
Description	The Blockchain Network records all access requests in the system
Primary Actor	Blockchain Network
Precondition	None
Post condition	All access requests from the users will be recorded by the Blockchain Network
Main Success Scenario	The Blockchain Network will automatically record all data requests in a ledger
Use Case Name	**storeCTI**
Description	The database stores all previously shared cyber threat intelligence in the prototype
Primary Actor	Database Administrator
Precondition	None

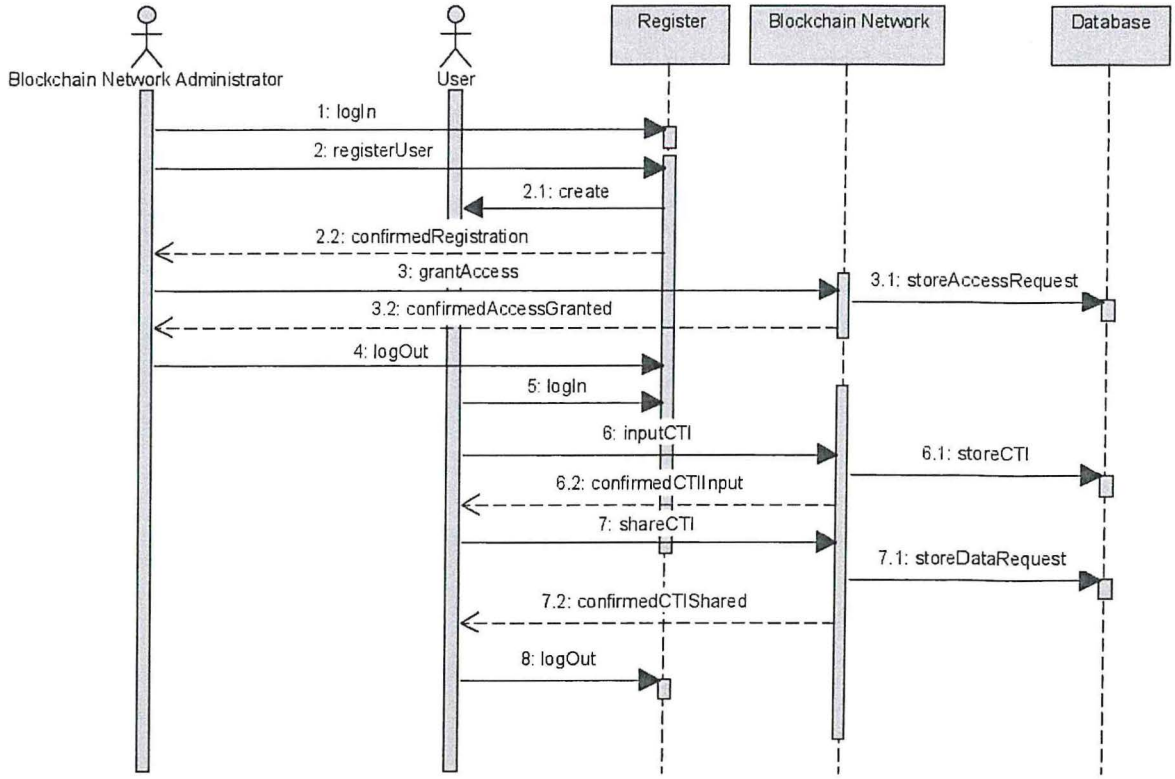


Figure 4.20: Sequence Diagram

4.5.3 Entity Relationship Diagram

An entity relationship diagram (ERD) is a high-level conceptual model that outlines information as entities, attributes and relationships. It is usually used to design the database of the system. It involves collecting the requirements, identifying entities, attributes and the relationship between the entities (Kashmira & Sumathipala, 2018). The ERD of the prototype is shown in Figure 4.21.

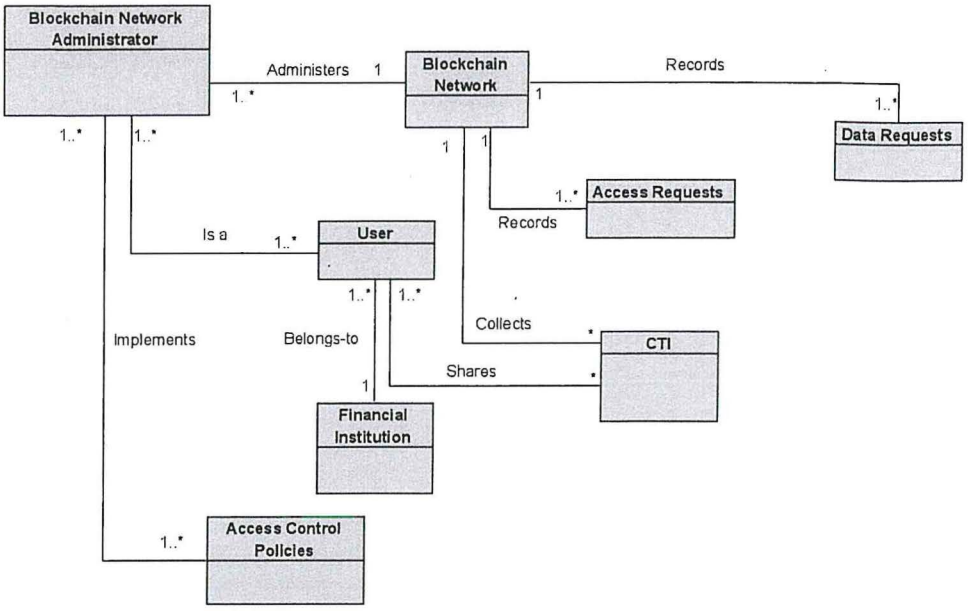


Figure 4.22: Class Diagram

4.5.5 Wireframes of System

Wireframes are cognitive diagrams that are important in system design and help create ideas early in the website or application planning process. They are used to organize content and show the basic visual appearance to create a common understanding of what a website, application or prototype will look like. The benefit of wire framing is that they lessen the chance of errors occurring during the actual system development process (Adams, 2020). Figure 4.23 shows the wireframe of the login page of the prototype, Figure 4.24 shows the home page wireframe and Figure 4.25 shows CTI sharing page wireframe.

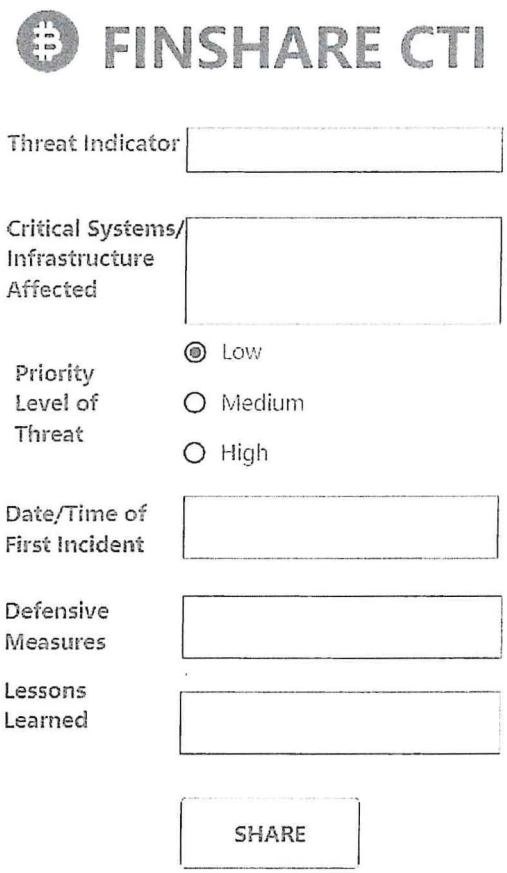


Figure 4.25: CTI Input Page Wireframe

	Docker Compose	Tool for defining and running multi-container Docker applications	Docker Compose 1.8
	Node.js	Backend programming language and runtime environment	Node.js 13.6.0
	Angular	Frontend web application framework	Angular 13
	Go	Docker base language	Go 1.13.15
	Database	State database that can store any binary data that is modeled in chaincode in JSON format	CouchDB 0.4.10
	Development Framework	Open development toolset and framework to make developing blockchain applications easier	Hyperledger Composer 20
Network Environment	Laptop Wi-Fi Adapter	Laptop Wi-Fi Adapter	Realtek RTL8822BE 802.11ac PCIe Adapter
	Virtual Machine Network Adapter	Network connection for the virtual machine	PCnet-FAST III (Am79C973)
	Internet connection	Internet Connection	Safaricom Home Fibre 10MBps

5.2.1 Starting the Blockchain-Based Prototype

For the prototype to run, Hyperledger Fabric has to be running on the operating system. This is done by executing './startFabric.sh'on the Fabric folder via the terminal as seen on Figure 5.1.

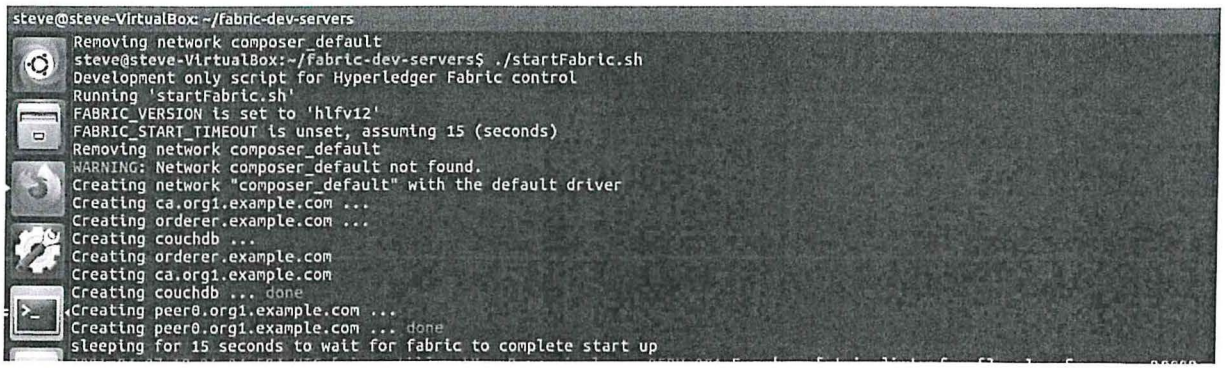


Figure 5.1: Screenshot of Hyperledger Fabric start

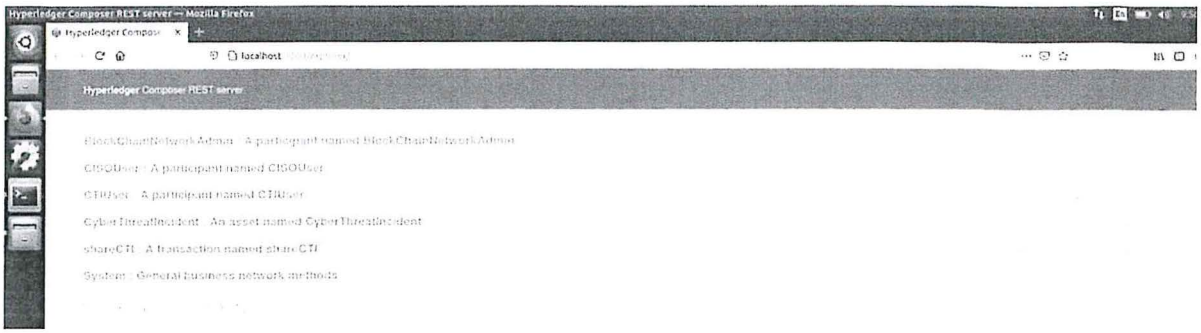


Figure 5.4: Hyperledger Composer REST Server

After the APIs are generated, the blockchain prototype is generated and launched on the URL http://localhost:4200 as seen on Figure 5.5.

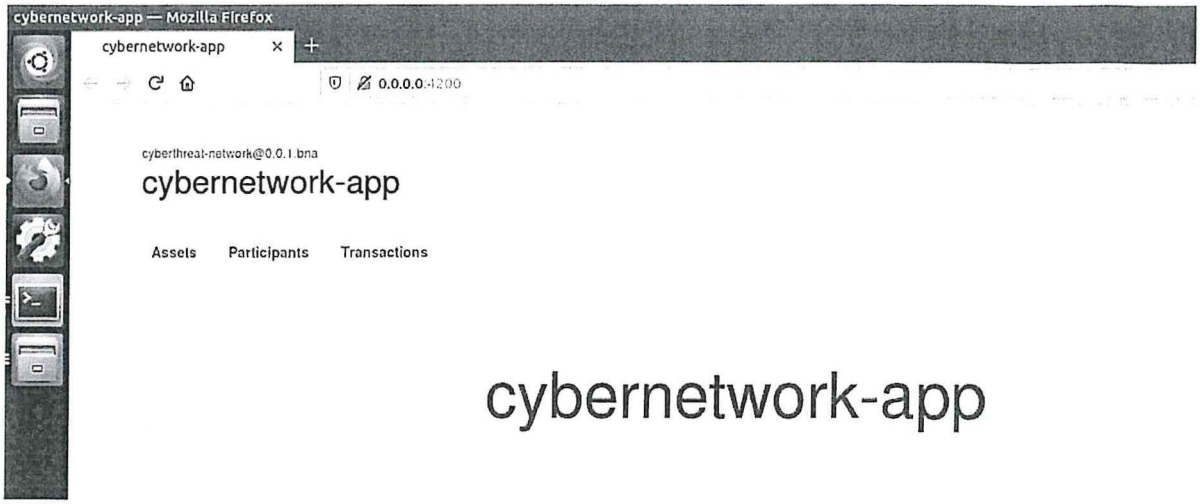


Figure 5.5: Blockchain Application

5.3 System Testing

System testing is the process of evaluating software at the system level and it is conducted by integrating all the modules of a system together based on the functional and non-functional requirements (Desai & Srivastava, 2016).

5.3.1 Functional Testing

Functional testing is the process of validating a system against specified functional requirements that have been gathered (Lewis, 2017; Nayyar, 2019). The purpose of functional testing is to ensure

5.3.1.2 Input Cyber Threat Intelligence

Registered users can input the cyber threat details on the application as seen on Figure 5.8. The details include the description of the cyber threat, infrastructure affected, level of threat, date of the incident, defensive measures and lessons learned.

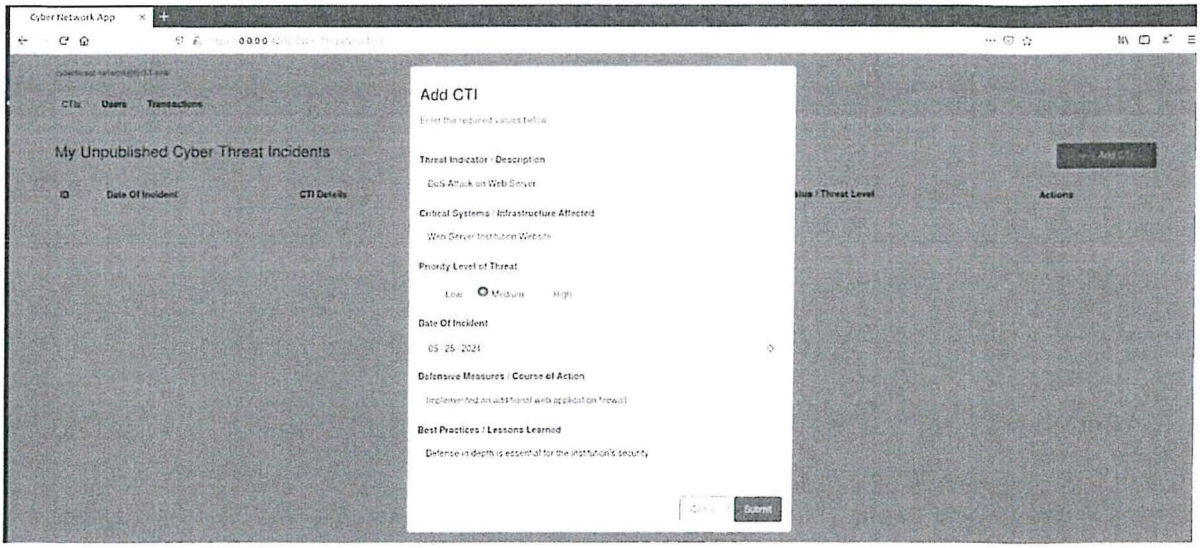


Figure 5.8: Input CTI Details

Once the CTI User inputs the CTI, the incident remains unpublished on Figure 5.9. During this time, the CTI Users can edit and confirm that the details are correct because once the CTI has been published, they cannot edit the details on the ledger.

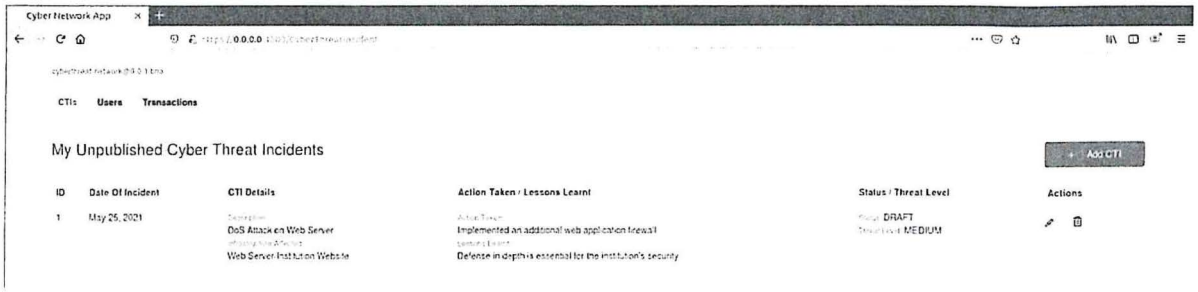
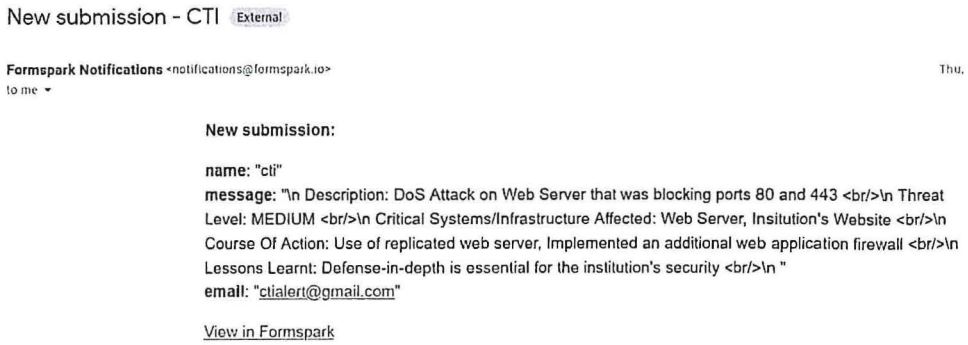


Figure 5.9: Created and unpublished CTI


New submission - CTI External

Formspark Notifications <notifications@formspark.io> Thu,
to me

New submission:

name: "cti"
message: "\n Description: DoS Attack on Web Server that was blocking ports 80 and 443
\n Threat Level: MEDIUM
\n Critical Systems/Infrastructure Affected: Web Server, Insitution's Website
\n Course Of Action: Use of replicated web server, Implemented an additional web application firewall
\n Lessons Learnt: Defense-in-depth is essential for the institution's securily
\n "
email: "ctialert@gmail.com"

View in Formspark

Figure 5.12: Email Alert

5.3.1.4 View Cyber Threat Intelligence

CTI Users can view their published and unpublished cyber incidents by selecting the dropdown menu on the CTI Tab as demonstrated on Figures 5.13 and 5.14.

Figure 5.13: Published Cyber Threat Incidents

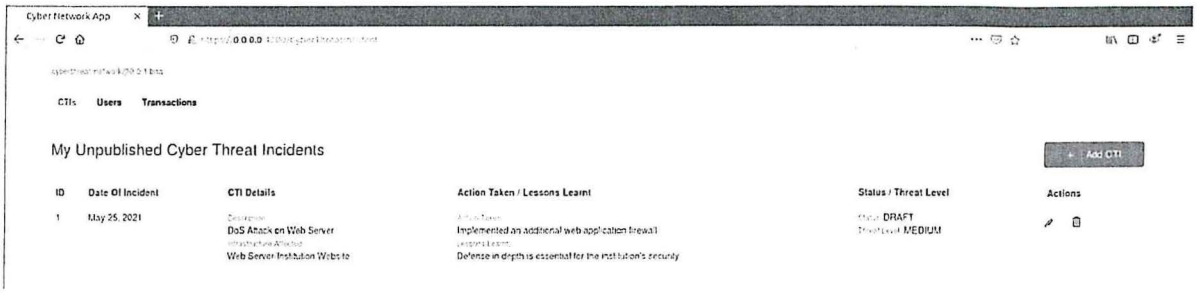


Figure 5.14: Unpublished Cyber Threat Incidents

On the Hyperledger Playground page, the interactive testing can be done on the created business network which in this case is the 'cyberthreat-network'. Figure 5.16 shows the Test page for the 'cyberthreat-network' where tests where done on creating a user, creating an asset and submitting a transaction. Table 5.3 summarizes the interactive test scenarios.

Table 5.3: Interactive Test Scenarios

Test ID	Interactive Test	Expected Outcome	Comment
1	Creating a user	CTIUser created successfully	Pass
2	Creating an asset	CyberThreatIncident created successfully	Pass
3	Submitting a transaction	shareCTI was successful	Pass

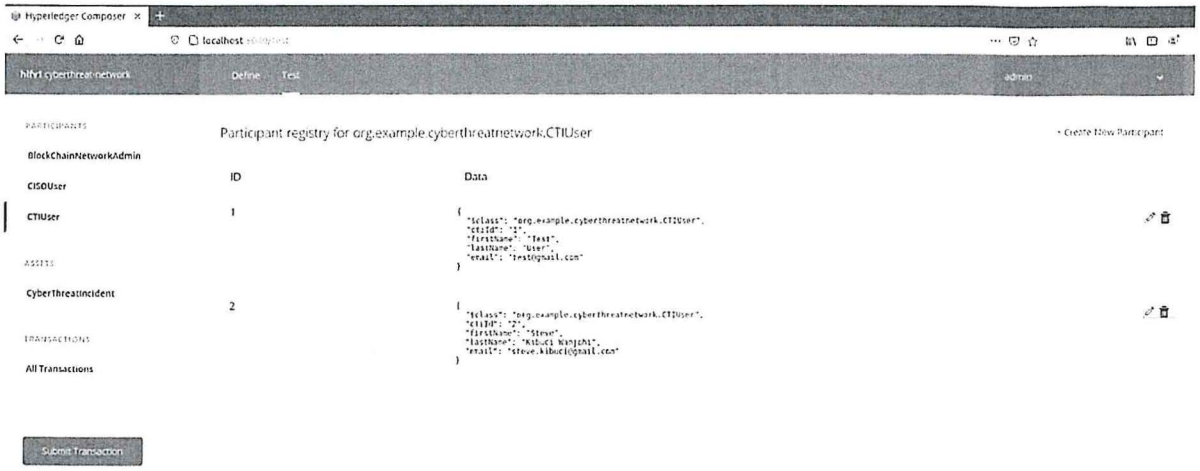


Figure 5.16: Interactive Test Page

The third objective was to review existing platforms used for threat intelligence sharing. The existing platforms were divided into three: open source platforms that are free for download including CRITs and MISP, commercial platforms that are off-the-shell solutions such as ThreatStream, ThreatConnect and EclecticIQ and community-based platforms that are online spaces where groups of individuals interact with each other on cyber threats such as Alienvault and Facebook Threat Exchange.

The fourth objective was to develop a blockchain-based prototype for sharing threat intelligence in financial institutions. This was achieved through actual design, implementation and testing of the blockchain solution. Use cases, sequence diagrams and data flow diagrams aided in the design phase of the application.

The fifth objective was to test the prototype. The functional and non-functional requirements of the system were tested. The compatibility testing was done on different browsers and the responsiveness of the prototype was tested. Interactive testing was done using Hyperledger Playground to test creating participants, assets and submitting transactions.

6.3 System Assessment

The prototype was developed and required a user to be in the same wireless network as the host virtual machine to access. The following section briefly describes the advantages and disadvantages presented by the prototype.

6.3.1 Advantages of the Prototype

i. The time and cost of implementing the prototype were relatively economical as the development tools and operating system were open source.
ii. The blockchain prototype provides immutability and trust amongst financial institutions by sharing cyber threat intelligence that cannot be altered on the ledger.
iii. System compatibility of the prototype aims to give quality user experience where users can access using different operating systems.
iv. The prototype enhances privacy and security mechanisms of Hyperledger Fabric including asymmetric cryptography and zero-knowledge proof.

Chapter 7: Conclusion, Recommendations and Future Work

7.1 Conclusion

The study was aimed at developing a prototype for sharing cyber threat intelligence between financial institutions using blockchain technology. This was achieved by investigating the challenges in sharing cybersecurity information by financial institutions. Several sources of literature were reviewed to analyze frameworks and approaches used for cybersecurity preparedness in financial institutions. Existing platforms were also reviewed that are used for cyber threat intelligence sharing.

A blockchain-based prototype that shares cyber threat intelligence in financial institutions was developed using system design and the functionality of the developed prototype was tested.

7.2 Recommendations

The study presented a different way of providing trust to shared cyber threat intelligence between financial institutions in Kenya. For these financial institutions to use automated threat sharing solutions, the following recommendations are advised:

i. Financial institutions are encouraged to refrain ad hoc traditional methods of sharing cyber threat intelligence and adopt automated methods of sharing cyber threat intelligence amongst themselves.
ii. Kenyan financial institutions can adopt a common platform for their cyber threat intelligence sharing. This can be done by leveraging blockchain technology which encourages transparency and trust.
iii. Regulators such as Central Bank of Kenya and Insurance Regulatory Authority should overlook how the cyber threat intelligence is shared to financial institutions. These regulators would be the blockchain network administrators who create the users and control their access and permissions.

7.3 Future Work

The following are the recommendations for future work relating to the blockchain-based appliction for cyber threat intelligence sharing:

References

Adam, A. M. (2020). Sample Size Determination in Survey Research. *Journal of Scientific Research and Reports*, *26*(5), 90-97. https://doi.org/10.9734/jsrr/2020/v26i530263

Adams, C. (2020). *Communicating job skills to individuals living with developmental disabilities: Preparation of a wireframe prototype*. Creative Components. 464. https://lib.dr.iastate.edu/creativecomponents/464

AlienVault Open Threat Exchange. (2020). *AlienVault - Open Threat Exchange*. Retrieved 24 July 2020, from https://otx.alienvault.com/

American Banker. (2020). *Cybersecurity Assessment Tool Remains Voluntary: Regulators*. Retrieved 24 July 2020, from https://www.americanbanker.com/news/cybersecurity-assessment-tool-remains-voluntary-regulators

Androulaki, E. et al. (2018). Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains. *Proceedings of the Thirteenth EuroSys Conference*, 1–15. https://doi.org/10.1145/3190508.3190538

Anomali. (2020). *ThreatStream - Threat Intelligence Platform*. Retrieved 24 July 2020, from https://www.anomali.com/products/threatstream

Ayoade, G., Karande, V., Khan, L., & Hamlen, K. (2018). Decentralized IoT Data Management Using BlockChain and Trusted Execution Environment. *2018 IEEE International Conference On Information Reuse And Integration (IRI)*. https://doi.org/10.1109/iri.2018.00011

Björck, F., Henkel, M., Stirna, J., & Zdravkovic, J. (2015). Cyber Resilience – Fundamentals for a Definition. *New Contributions in Information Systems and Technologies*, 311–316. https://doi.org/10.1007/978-3-319-16486-1_31

https://www.centralbank.go.ke/wp-content/uploads/2017/09/GUIDANCE-NOTE-ON-CYBERSECURITY-FOR-THE-BANKING-SECTOR.pdf

Central Bank of Kenya. (2018). *2018 Bank Supervision Annual Report.* Central Bank of Kenya. Retrieved 3 July 2020, from https://www.centralbank.go.ke/uploads/banking_sector_annual_reports/1174296311_2018%20Annual%20Report.pdf

Cheng, X., & Degryse, H. (2010). *The impact of bank and non-bank financial institutions on local economic growth in China*. Journal of Financial Services Research, 37(2), 179-199.

Choi, P. M. S., & Huang, S. H. (Eds.). (2021). *Fintech with Artificial Intelligence, Big Data, and Blockchain*. Springer Nature.

Communications Authority of Kenya (2021). *FOURTH QUARTER SECTOR STATISTICS REPORT FOR THE FINANCIAL YEAR 2020/21 (APRIL-JUNE 2021).* Central Bank of Kenya. Retrieved 31 August 2021, from https://ke-cirt.go.ke/wp-content/uploads/2021/08/Quarter-4-FY-2020_21-National-KE-CIRT_CC-Cybersecurity-Report-Public-Version.pdf

Cossentino, M., Hilaire, V., Molesini, A., & Seidita, V. (Eds.). (2014). *Handbook on agent-oriented design processes*. Springer Berlin Heidelberg.

CRITs (2020). *CRITs: Collaborative Research Into Threats.* CRITs. Retrieved 24 July 2020, from http://crits.github.io/.

Desai, S., & Srivastava, A. (2016). *Software testing: a practical approach.* PHI Learning Pvt. Ltd..

Eilts, D., & Levy, Y. (2018). *Towards an Empirical Assessment of Cybersecurity Readiness and Resilience in Small Businesses*.

IBM. (2020). *IBM X-Force Exchange – Overview*. IBM. Retrieved 24 July 2020, from https://www.ibm.com/products/ibm-xforce-exchange.

ICT Authority. (2014). *National Cybersecurity Strategy*. ICT Authority. Retrieved 3 July 2020, from http://icta.go.ke/pdf/NATIONAL%20CYBERSECURITY%20STRATEGY.pdf.

Insurance Regulatory Authority. (2018). *Insurance Regulatory Authority 2017*. Retrieved 24 July 2020, from https://www.ira.go.ke/images/docs/2017annual/Insurance-Industry-Annual-Report-2017.pdf.

Jaiwai, M., & Sammapun, U. (2017). Extracting UML class diagrams from software requirements in Thai using NLP. *2017 14th International Joint Conference on Computer Science and Software Engineering (JCSSE)*, 1–5. https://doi.org/10.1109/JCSSE.2017.8025938

Johnson, C. S. et al. (2016) Guide to Cyber Threat Information Sharing. NIST SP 800-150. National Institute of Standards and Technology, p. NIST SP 800-150. doi: 10.6028/NIST.SP.800-150.

Johnson, C., Badger, M., Waltermire, D., Snyder, J., & Skorupka, C. (2016). *Guide to Cyber Threat Information Sharing*. National Institute of Standards and Technology. https://doi.org/10.6028/nist.sp.800-150

Jover, E., & Mlambo, C. (2014). *A review of factors affecting the attractiveness of Angola to private equity (PE) investments*. South African Journal of Economic and Management Sciences, 17(5), 609-623.

Kashmira, P., & Sumathipala, S. (2018). Generating Entity Relationship Diagram from Requirement Specification based on NLP. *2018 3rd International Conference on Information Technology Research (ICITR)*. https://doi.org/10.1109/icitr.2018.8736146

Kaur, K., & Sharma, R. (2017). Critical: Threat model for an outsourcing business. *2017 8th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, 1–5. https://doi.org/10.1109/ICCCNT.2017.8204093

Marsh and Microsoft. (2019). *2019 Global Cyber Risk Perception Survey*. Retrieved 26 May 2020, from https://www.microsoft.com/security/blog/wp-content/uploads/2019/09/Marsh-Microsoft-2019-Global-Cyber-Risk-Perception-Survey.pdf

MISP. (2020). *MISP - Open Source Threat Intelligence Platform and Open Standards for Threat Information Sharing (formerly known as Malware Information Sharing Platform)*. MISP. Retrieved 24 July 2020, from https://www.misp-project.org/index.html

Mukherjee, M. (2016). Object-Oriented Analysis and Design. *International Journal of Advanced Engineering and Management*, *1*(1), 1-11.

Nweke, L. O., & D., S. (2020). A Review of Asset-Centric Threat Modelling Approaches. *International Journal of Advanced Computer Science and Applications*, *11*(2). https://doi.org/10.14569/IJACSA.2020.0110201

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Retrieved 3 July 2020, from https://bitcoin.org/bitcoin.pdf

Nayyar, A. (2019). *Instant approach to software testing: Principles, applications, techniques, and practices*. BPB Publications.

Panigrahi, S. S., Shaurya, S., Das, P., Swain, A. K., & Jena, A. K. (2018, December). Test Scenarios Generation Using UML Sequence Diagram. In *2018 International Conference on Information Technology (ICIT)* (pp. 50-56). IEEE.

PricewaterhouseCoopers. (2018). *The Global State of Information Security Survey 2018*. PwC. Retrieved 26 May 2020, from https://www.pwc.com/us/en/services/consulting/cybersecurity/library/information-security-survey.html

Purvis, R. S., Abraham, T. H., Long, C. R., Stewart, M. K., Warmack, T. S., & McElfish, P. A. (2017). Qualitative study of participants' perceptions and preferences regarding research dissemination. *AJOB empirical bioethics*, 8(2), 69-74.

Wang, G., Huo, Y., & Ma, Z. M. (2019). Research on University's Cyber Threat Intelligence Sharing Platform Based on New Types of STIX and TAXII Standards. *Journal of Information Security*, *10*(4), 263–277. https://doi.org/10.4236/jis.2019.104015

Wu, Y., Qiao, Y., Ye, Y., & Lee, B. (2019). Towards Improved Trust in Threat Intelligence Sharing using Blockchain and Trusted Computing. *2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS)*, 474–481. https://doi.org/10.1109/IOTSMS48152.2019.8939192

☐ Loss of reputation ☐ Other: _____

8. The financial systems or networks are at significant risk for cyberattacks.
☐ Not Sure ☐ Strongly disagree ☐ Disagree ☐ Neutral ☐ Agree ☐ Strongly agree

9. Please select the important third party dependencies for the institution (Check all that apply)
☐ Software Vendors ☐ Outsourced IT services ☐ Business partners
☐ Hardware Suppliers ☐ Other: _____

10. Our financial institution has confidence in the cyber security of our third party dependencies.
☐ Not Sure ☐ Strongly disagree ☐ Disagree ☐ Neutral ☐ Agree ☐ Strongly agree

11. Please select the infrastructure critical for the financial institution's mission. For those selected, please state if there are contingency plans (e.g. backup system, UPS, generators).

(Check all that apply)	Established Contingency Plans (Yes or No)
☐ Power grid	
☐ Internet	
☐ Telecommunications/Phone	
☐ Financial networks	
☐ Transportation	
☐ Water	
☐ Other: _____	

PART B: THREAT AWARENESS AND TRAINING

1. Senior management of the financial institution consistently emphasizes the importance of cybersecurity.
☐ Not Sure ☐ Strongly disagree ☐ Disagree ☐ Neutral ☐ Agree ☐ Strongly agree

2. Senior management understands the current cyber threat environment
☐ Not Sure ☐ Strongly disagree ☐ Disagree ☐ Neutral ☐ Agree ☐ Strongly agree

3. Which best describes the nature of training for existing cybersecurity roles?
☐ Training does not exist
☐ Training occurs rarely
☐ Training is well-defined, focusing on tool usage
☐ Training is well-defined, focusing on tool usage and good analytic process

4. What describes nature of cross training between functions (functions such as incident response, cyber threat intelligence or malware analysis)?
☐ There is no cross-training between functions
☐ Cross-training occurs for some functions

☐ Common infrastructure assets (servers, networking equipment etc.)

3. There are clear policies and procedures in place for log data capture and access (e.g. what logs are to be collected, stored for how long, collected by whom, and how they are to be accessed).
☐ Not Sure ☐ Strongly disagree ☐ Disagree ☐ Neutral ☐ Agree ☐ Strongly agree

4. What are the main challenges when collecting logs? (Check all that apply)
☐ Outsourced Logs (not provided by vendor) ☐ Inconsistent Logs
☐ Short Retention Period of Logs ☐ Rely on informal social network
☐ Disorganized Logs ☐ Non-Indexed Logs ☐ Need to log into another server to view logs
☐ Filling request form and the wait ☐ Other: _____
☐ Not seeing the importance of logs and their storage

5. Does the cyber security team/ICT team have access to Help Desk tickets to review for potential indicators?
☐ There is no reliable access
☐ There is access to help desk tickets - but no regular process for review and escalation
☐ There is access to help desk tickets - and a process for review and escalation

6. Are there mechanisms that exist for users to submit tips on potentially suspicious emails or other suspicious events?
☐ There is no mechanism
☐ Users have developed their own mechanisms
☐ There is a standard mechanism but no process for review and escalation
☐ There is a standard mechanism and a process for review and escalation

PART D: INTERNAL PROCESS AND COLLABORATION
1. Does the financial institution have someone responsible for information security, such as a CISO (Chief Information Security Officer)?
☐ Yes ☐ No

2. There is regular communication between the cybersecurity team/ICT Team and the following groups: (Check all that apply)
☐ Senior management ☐ Mid-level management ☐ Corporate security ☐ Departments ☐ Users

3. How often does a member of the cyber security/ICT Team (whether CISO, Head of ICT or other) brief the financial institution's senior management? (Check all that apply)
☐ Weekly ☐ When a threat or incident affects operations
☐ Monthly ☐ Other: _____
☐ Quarterly

☐ Not Sure ☐ Strongly disagree ☐ Disagree ☐ Neutral ☐ Agree ☐ Strongly agree

PART E: TRACKING AND ANALYTICS

1. How does the financial institution track cyber threat indicators?
☐ Not tracked ☐ Spreadsheet ☐ Database ☐Other: _____

2. If any indicators are tracked, what types of indicators? (Check all that apply)
☐ IPs ☐ Domains ☐ Email addresses
☐ URLs ☐ File hashes ☐ Email headers ☐ Other: _____

3. If indicators are tracked, what incidental details are collected? (Check all that apply)
☐ Attribution ☐ Valid time window ☐ Source(s) ☐ Date added ☐ Related incidents
☐ Actions taken ☐ Description ☐ Role in cyberattack lifecycle ☐ Confidence level
☐ Other: _____

4. Are known cyber threat indicators checked by the financial institution?
☐ Not Applicable ☐ Near real time sensor alerts ☐ Scheduled queries of new logs
☐ Historical log search ☐ Ad hoc/manual queries ☐ Other: _____

5. Describe the tracking of cyberattacks/incidents in the financial institution
☐ There is none
☐ There is manual tracking of attacks/incidents
☐ Attacks/incidents are tracked routinely with some tools (spreadsheet, database)
☐ There is a dedicated security attack/incident tracking system

6. What cyberattack/incident data does the financial institution collect? (Check all that apply)
☐ Number of incidents ☐ How attack was stopped, if prevented
☐ Detection method ☐ Whether vulnerability patched or not ☐ Attributed threat actor(s)
☐ Affected assets ☐ Impact of incident, if not prevented
☐Whether user(s) clicked on link or attachment
☐ Other: _____

7. Which of the following types of analytics are performed? (Check all that apply)
☐ Historical analysis ☐ Dynamic analysis ☐ Memory forensics
☐ Attribution ☐ Network traffic analysis ☐ Proactive Data mining for new signs of attack
☐ Reverse engineering of binaries ☐ Social media analytics

8. Which best describes your knowledge management of cybersecurity expertise?
☐ Expertise is shared verbally but not usually documented
☐ Expertise is informally documented

Threat Analysis	☐	☐
Aggregated threat intelligence feeds	☐	☐
Defensive Measures and Courses of Action	☐	☐
Malware samples	☐	☐
Log files	☐	☐
Best Practices and Lessons Learned	☐	☐
Vendor Reviews	☐	☐
Points of contact	☐	☐
Other: _____	☐	☐

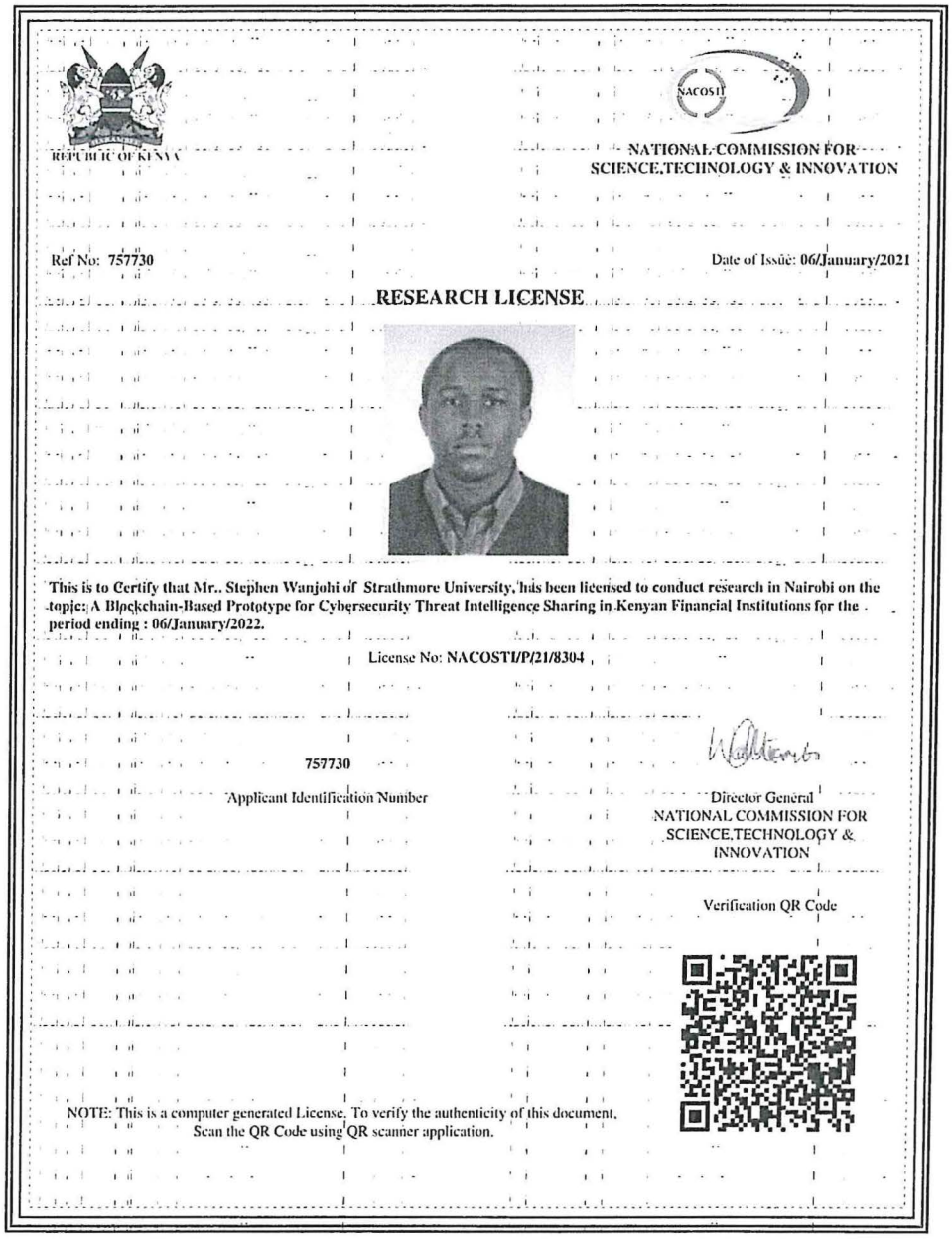
5. Please state the mechanism(s) used for threat intelligence sharing. (Check all that apply)
☐ Telecom or VTC ☐ Automated feeds (e.g., STIX and TAXII) ☐ Wiki
☐ Forum or chat room ☐ Face to face meetings ☐ Portal
☐ Email distribution list ☐ Shared repository (for indicators, samples, etc.)
☐ Private communications ☐ Other: _____

6. Please describe what the financial institution does with shared threat information. (Check all that apply)
☐ Manually ingest indicators ☐ Improve training ☐ Brief management
☐ Automatically ingest indicators ☐ Perform analysis ☐ Create signature/indicator for ongoing scan
☐ Scan once for new indicators ☐ Write reports ☐ Other: _____

7. The financial institution is comfortable sharing information with other financial institutions
☐ Not Sure ☐ Strongly disagree ☐ Disagree ☐ Neutral ☐ Agree ☐ Strongly agree

8. Is there anything limiting what threat information you share with other financial institutions? (Check all that apply)
☐ Threat sharing mechanisms are not easy to use ☐ Level of trust
☐ Lack of effective sharing agreements ☐ Manpower/resource constraints
☐ Legal issues ☐ Competition
☐ Internal vetting process/approvals ☐ Concerns about reputation
☐ Lack of confidence in our information's value/relevance
☐ Other: _____

Appendix C: National Commission for Science and Technology Innovation (NACOSTI) Research Permit



REPUBLIC OF KENYA

NATIONAL COMMISSION FOR SCIENCE,TECHNOLOGY & INNOVATION

Ref No: 757730

Date of Issue: 06/January/2021

RESEARCH LICENSE

This is to Certify that Mr.. Stephen Wanjohi of Strathmore University, has been licensed to conduct research in Nairobi on the topic: A Blockchain-Based Prototype for Cybersecurity Threat Intelligence Sharing in Kenyan Financial Institutions for the period ending : 06/January/2022.

License No: NACOSTI/P/21/8304

757730

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 D: Ouriginal Similarity Index

Curigínal

Document Information

Analyzed document	A Blockchain-Based Prototype for Cybersecurity Threat Intelligence Sharing A Case of Kenyan Banking and Insurance Financial Institutions.pdf (D115572618)
Submitted	2021-10-18 10:27:00
Submitted by	
Submitter email	Wanjohi.Stephen@strathmore.edu
Similarity	6%
Analysis address	library.strath@analysis.urkund.com

FINDINGS

40 MATCHING TEXT
High similarity of content

0 WARNINGS
Unusual use of characters

VIEW THE ENTIRE DOCUMENT

An alternative source is a source where we found a text match that is identical to the included sources. However, we found the corresponding matching text in more than one source and we believe it's

LEARN MORE

SIMILARITY

16%
receivers' average

6%
This document

SUBMISSION DETAILS

SUBMITTER
Wanjohi.Stephen@strathmore.edu

FILE
A Blockchain-Based Prototype for Cybersecurity Threat Intelligence Sharing A Case of Kenyan Banking and Insurance Financial Institutions.pdf
2021-10-18T10:27:00

SUBMISSION ID
115572618

WORDS
19737

MESSAGE