Ministry of Science and Higher Education of the Republic of Kazakhstan

SDU University

Shakhnazar-Sultan Manbay

Blockchain based configuration files backup system

THESIS

Presented in Partial Fulfilment for the

Degree of Master of Technical Science in Computer Science

(degree code: 7M06102)

Department of Computer Science

Faculty of Engineering and Natural Sciences

Supervisor: **PhD Dana Utebayeva**

Kaskelen, June 2024

SDU University
Faculty of Engineering and Natural Sciences
Department of Computer Science

Dean of Faculty of Engineering and Natural Sciences

Assistant Professor, PhD Akhmedov Ramis

_____

« _____» _____ 2024

Topic of the thesis:

Blockchain based configuration files backup system

Thesis submitted as part of the requirements for the award of the MSc in "7M06102 - Computer Science", SDU University, 2022-2024

Head of Department _____ Assistant Professor, PhD Mukash Zh.

Academic Supervisor _____ PhD Dana Utebayeva

Master student _____ Manbay Shakhnazar-Sultan

Kaskelen, 2024

Declaration

I confirm that this is my own work and the use of all material from other sources has been properly and fully acknowledged.

Shakhnazar-Sultan Manbay

June 2024

Acknowledgements

I would like to extend my sincerest gratitude to a number of individuals and institutions whose support was invaluable in the completion of this master's thesis. I wish to acknowledge the Cisco Netacad laboratory and the CYCNET Community at SDU University for providing the essential infrastructure, resources, and unwavering support that greatly facilitated my research. I am particularly thankful to Dana Utebayeva, my Supervisor, and Inkar Shoganova, the head of the laboratory, whose guidance, insights, expertise and encouragement have been pivotal.

I would like to express my appreciation for the role of artificial intelligence, specifically the use of ChatGPT, which has been an invaluable tool in refining my writing style, enhancing the readability of my content, and reorganizing any poorly structured sentences. This technology has served as an aid in the editing phase, ensuring that the final document is coherent and well-presented. It is important to clarify that while AI technologies have been utilized to assist in the editing process, at no point has any content generated by such technologies been presented as my original work. The research, analysis, and conclusions contained within this thesis are solely my own, crafted through diligent study and unwavering commitment to academic integrity.

In closing, my acknowledgements would be incomplete without mentioning my family, friends, and all who provided moral support throughout my academic pursuit. Their belief in my capabilities has been a source of strength and motivation.

Dedication

This thesis is dedicated to:
Alyara Abilbashar, Gulnazik Kubasheva, Seitmurat Seitkul, Bekzada Ushtay, Malika Token, Arina Ussubaliyeva, Bauyrzhan Berlikozha and many other for their support, help, sense of humour and useful comments for improving this project.

Abstract

In today's digital age, the need for robust data security and backup systems has become increasingly critical, especially in the face of rising cyber threats such as ransomware attacks. Traditional backup systems have shown vulnerabilities in safeguarding crucial data, prompting a search for innovative solutions to enhance data integrity and protection. This research presents a groundbreaking approach to address the challenges in data security and backup systems by leveraging blockchain technology. Blockchain technology, renowned for its decentralized and immutable nature, offers a secure and transparent platform for storing and safeguarding data. By harnessing the programmable and decentralized features of blockchain, this thesis proposes a novel blockchain-based configuration files backup system. The system aims to ensure the confidentiality and integrity of data backups in network environments, paving the way for enhanced network security measures. The research questions aim to explore how blockchain technology can be utilized to enhance the security of configuration files backup systems, the advantages of implementing a blockchain-based backup system over traditional methods, the impact of blockchain technology on cybersecurity innovation and data protection mechanisms, and how blockchain technology can contribute to the expansion of information security and improve overall data resilience in network environments. The methodology section delves into the fundamentals of blockchain technology, explaining different types of blockchain networks, consensus protocols, proof of work, and asymmetric encryption. The proposed system includes a detailed system architecture, data storage mechanisms, and blockchain algorithms for securing data and configuration files. Through experimentation and evaluation of the proposed system, the effectiveness of protecting data against vulnerabilities in real-world scenarios, including ransomware attacks, integration of blockchain, and evaluation of performance are analyzed. This thesis aims to make significant contributions to the field of information security by showcasing the transformative capabilities of blockchain technology in enhancing data security innovation, fostering data resilience in network environments, and advancing network security practices in the digital era.

Аңдатпа

Бүгінгі цифрлық ғасырда сенімді деректер қауіпсіздігі мен сақтық көшірме жүйелеріне деген қажеттілік, әсіресе төлемдік бағдарламалық жасақтама шабуылдары сияқты өсіп келе жатқан киберқауіптер жағдайында өте маңызды болып отыр. Дәстүрлі сақтық көшірме жүйелері маңызды деректерді қорғауда осалдықтарды көрсетті, бұл деректер тұтастығы мен қорғауды жақсарту үшін инновациялық шешімдерді іздеуге шақырды. Бұл зерттеу блокчейн технологиясын қолдану арқылы деректер қауіпсіздігі мен сақтық көшірме жүйелеріндегі қиындықтарды шешудің жаңашыл әдісін ұсынады. Орталықтандырылмаған және өзгермейтін табиғатымен танымал блокчейн технологиясы деректерді сақтау және қорғау үшін қауіпсіз және мөлдір платформаны ұсынады. Блокчейннің бағдарламаланатын және орталықтандырылмаған мүмкіндіктерін пайдалана отырып, бұл диссертация блокчейнге негізделген жаңа конфигурация файлдарының сақтық көшірмесін жасау жүйесін ұсынады. Жүйе желілік орталардағы деректердің сақтық көшірмелерінің құпиялылығы мен тұтастығын қамтамасыз етуге, желілік қауіпсіздік шараларын жақсартуға жол ашуға бағытталған. Зерттеу сұрақтары блокчейн технологиясын конфигурация файлдарының сақтық көшірме жүйелерінің қауіпсіздігін арттыру үшін қалай пайдалануға болатынын, блокчейн негізіндегі сақтық көшірме жүйесін енгізудің дәстүрлі әдістерге қарағанда артықшылықтарын, блокчейн технологиясының киберқауіпсіздік инновацияларына және деректерді қорғау механизмдеріне әсерін зерттеуге бағытталған. blockchain технологиясы ақпараттық қауіпсіздікті кеңейтуге және желілік орталардағы жалпы деректер тұрақтылығын жақсартуға қалай үлес қоса алады. Әдістеме бөлімі блокчейн технологиясының негіздерін зерттейді, блокчейн желілерінің әртүрлі түрлерін, консенсус хаттамаларын, жұмыс дәлелін және асимметриялық шифрлауды түсіндіреді. Ұсынылған жүйе егжей-тегжейлі жүйе архитектурасын, деректерді сақтау механизмдерін және деректер мен конфигурация файлдарын қорғауға арналған блокчейн алгоритмдерін қамтиды. Ұсынылған жүйені эксперимент және бағалау арқылы нақты әлемдегі сценарийлердегі осалдықтардан деректерді қорғаудың тиімділігі, соның ішінде төлемдік бағдарламалық қамтамасыз ету шабуылдары, блокчейн интеграциясы және өнімділікті бағалау талданады. Бұл диссертация деректер қауіпсіздігінің инновациясын арттыруда, желілік орталарда деректердің тұрақтылығын арттыруда және цифрлық дәуірде желілік қауіпсіздік тәжірибесін ілгерілетуде блокчейн технологиясының трансформациялық мүмкіндіктерін көрсету арқылы ақпараттық қауіпсіздік саласына елеулі үлес қосуға бағытталған.

Аннотация

В современную цифровую эпоху необходимость в надежных системах защиты данных и резервного копирования становится все более острой, особенно перед лицом растущих киберугроз, таких как атаки ransomware. Традиционные системы резервного копирования показали свою уязвимость в защите важнейших данных, что побудило искать инновационные решения для повышения целостности и защиты данных. В данном исследовании представлен новаторский подход к решению проблем безопасности данных и систем резервного копирования с помощью технологии блокчейн. Технология блокчейн, известная своей децентрализованной и неизменяемой природой, предлагает безопасную и прозрачную платформу для хранения и защиты данных. Используя программируемые и децентрализованные возможности блокчейна, в данной диссертации предлагается новая система резервного копирования конфигурационных файлов на основе блокчейна. Система призвана обеспечить конфиденциальность и целостность резервных копий данных в сетевых средах, прокладывая путь к усилению мер сетевой безопасности. Вопросы исследования направлены на изучение того, как технология блокчейн может быть использована для повышения безопасности систем резервного копирования конфигурационных файлов, преимуществ внедрения системы резервного копирования на основе блокчейна по сравнению с традиционными методами, влияния технологии блокчейн на инновации в области кибербезопасности и механизмы защиты данных, а также того, как технология блокчейн может способствовать расширению информационной безопасности и повышению общей устойчивости данных в сетевых средах. В методологическом разделе рассматриваются основы технологии блокчейн, объясняются различные типы блокчейн-сетей, протоколы консенсуса, доказательство работы и асимметричное шифрование. Предлагаемая система включает в себя подробную архитектуру системы, механизмы хранения данных и алгоритмы блокчейна для защиты данных и конфигурационных файлов. В ходе экспериментов и оценки предложенной системы анализируется эффективность защиты данных от уязвимостей в реальных сценариях, включая атаки ransomware, интеграция блокчейна и оценка производительности. Данная диссертация призвана внести значительный вклад в область информационной безопасности, продемонстрировав трансформационные возможности технологии блокчейн в повышении инновационности защиты данных, повышении устойчивости данных в сетевых средах и развитии практики сетевой безопасности в цифровую эпоху.

Abbreviations

AAA	– Authentication, Authorization, and Accounting
AES	– Advanced Encryption Standard
AONT	– All-or-Nothing Transform
ASA	– Adaptive Security Appliance
BTC	– Bitcoin
CPU	– Central Processing Unit
DCS	– Decentralized Cloud Storage
DDoS	– Distributed Denial of Service
DFS	– Decentralized File Systems
DHT	– Distributed Hash Tables
DPoS	– Delegated Proof Of Stake
ECC	– Elliptic Curve Cryptography
FHRP	– First Hop Redundancy Protocol
FTP	– File Transfer Protocol
HDFS	– Hadoop Distributed File System
HTTP	– Hypertext Transfer Protocol
IPFS	– Interplanetary File System
LAN	– Local Area Network
MTFS	– Merkle-Tree-Based File System
PBFT	– Practical Byzantine Fault Tolerance
PoB	– Proof of Burn
PoET	– Proof of Elapsed Time
PoS	– Proof of Stake
PoW	– Proof of Work
PRF	– Pseudorandom Function
RAID	– Redundant Array of Independent Disks
RAP	– Ransomware Protection
RSA	– Rivest–Shamir–Adleman
SHA	– Secure Hash Algorithm
SSD	– Solid–State Drive
SSL	– Secure Sockets Layer
TFTP	– Trivial File Transfer Protocol
TLS	– Transport Layer Security
VLAN	– Virtual Local Area Network
WLAN	– Wireless Local-Area Network
WLC	– Wireless LAN Controller

Table of Contents

Chapter 1

Background and motivations

1.1 Introduction

In today's rapidly evolving technological landscape, the proliferation of cyber threats has elevated network security to a critical priority for organizations worldwide [1]. As businesses continue to explore innovative methods to fortify their defenses, the potential of blockchain technology has emerged as a focal point of interest. Known for its decentralized and immutable nature [2], blockchain technology holds the promise of revolutionizing network security by providing a secure and transparent platform for storing and safeguarding data.

Networks play a pivotal role in both our daily lives and the business sphere, making them susceptible targets for cyber threats. Hackers exploit vulnerabilities within networks to gain unauthorized access and pilfer sensitive information, with a particular focus on personal data such as login credentials, passwords, and configuration files. The security of data backups, especially in light of escalating ransomware attacks [3], poses a significant challenge for organizations striving to protect their network infrastructure [4].

The emergence of ransomware as a potent form of malware has underscored the critical need for robust data protection mechanisms in the face of malicious cyber activities [5]. Traditional backup systems have proven inadequate in thwarting sophisticated ransomware attacks [6], highlighting the urgency for innovative solutions to secure backup files and uphold data integrity. The prevalence of ransomware incidents targeting high-profile organizations, such as the Colonial Pipeline cyberattack [7], emphasizes the pervasive threat posed by cybercriminals exploiting vulnerabilities in network security.

This dissertation aims to address the pressing challenges of data security and backup systems by proposing a novel approach centered on blockchain technology. By harnessing the decentralized and programmable features of blockchain, this study sets out to develop a cutting-edge solution that ensures the confidentiality and integrity of data backups in network environments. The adoption of blockchain technology holds the potential to catalyze advancements in cybersecurity innovation and bolster information security practices across diverse industries.

Through the development of a blockchain-based security system for storing backup configuration files of network devices, this research seeks to pave the way

for enhanced network security measures. The objectives of this study include creating an Enterprise Network prototype for testing purposes, designing a blockchain algorithm to secure data and configuration files, and implementing and testing the algorithm to fortify data against vulnerabilities.

By leveraging the transformative capabilities of blockchain technology, this dissertation endeavors to contribute to the expansion of information security, foster data resilience in network environments, and propel the evolution of network security practices in the digital age.

1.2 Problem Statement

In the realm of network security, the secure storage of data and configuration files stands out as a critical challenge amidst the ever-evolving landscape of cyber threats, particularly the escalating prevalence of ransomware attacks [3]. Cybercriminals target configuration files containing vital network setup information, posing a significant risk of unauthorized access and data theft for organizations. Conventional backup systems have demonstrated vulnerabilities in safeguarding against sophisticated ransomware attacks, underscoring the imperative for innovative solutions to protect backup files and uphold data integrity [6]. The proliferation of ransomware, characterized by its encryption of user files and extortion demands for decryption [8], has emerged as a grave threat to both individual users and enterprises alike. The inherent financial motivations driving ransomware attackers to encrypt and store files containing sensitive user data necessitate robust data protection measures to mitigate the impact of cyber incidents [9]. The reliance on backups as a means of data recovery in the aftermath of ransomware attacks is undermined by attackers' capabilities to target and compromise backup systems [4, 10, 11], rendering conventional backup solutions inadequate in combating sophisticated cyber threats [6]. According to the Fortinet 2023 Global Ransomware Report, 66% of enterprises were targeted by ransomware attacks, with half becoming victims [12]. Moreover, according to Veeam's 2023 Ransomware Trends Report, more than 93% of attackers use backups during attacks, with 75% of such attempts being successful [13]. Backup systems are not completely immune to ransomware assaults. Notable ransomware incidents targeting critical infrastructure, such as the Colonial Pipeline cyberattack [7], have brought to light the pervasive vulnerabilities within network security frameworks and underscored the urgent need for resilient data protection mechanisms. The persistent threat of ransomware, exemplified by high-profile attacks like WannaCry [14] and Ryuk [15, 16], continues to pose formidable challenges to information security and data resilience in network environments.

Table 1.1 encapsulates details of these incidents, including the name of the attack, the year it occurred, the entities affected, estimated financial losses, as well as the current status of each attack [17, 18].

Table 1.1 – Summary of Notable Ransomware Attacks

Attack Name	**Year**	**Entities Affected**	**Approximate Losses**	**Current Status**
TeslaCrypt	2015	Windows XP, Vista, 7, and 8	$500/individual	Inactive
WannaCry	2017	Microsoft Windows users	$4 billion	Decryption available
NotPetya	2017	Businesses and Public Offices in Ukraine, Germany, and France	$10 billion	Decryption available
SamSam	2018	Windows servers	$6 million	Active
Sodinokibi	2019	JBS and Kaseya organizations	$200 million	Decryption available
Attack on Travelex	2019	Pulse Secure VPN servers	$2.3 million	Mitigated by paying the ransom
Colonial Pipeline Attack	2021	Colonial Pipeline	$4.4 million	Mitigated by paying the ransom
Attack on the Costa Rican Government	2022	30 Costa Rican Government Offices	$30 million per day of the attack	Active
Attack on Swissport	2022	Swissport	Unknown	Ransomware removed. 1.6 TB data stolen.
Attack on Impressa	2022	Portuguese Media Company Impressa	Unknown	Mitigated

As illustrated in Table 1.1, cyber attacks have evolved over time, targeting a range of systems from individual computers to widespread corporate networks. The TeslaCrypt ransomware primarily affected personal computers running older versions of Windows and is now considered inactive. In contrast, the WannaCry and NotPetya attacks of 2017 caused widespread damage to Microsoft Windows users and businesses respectively, with financial repercussions estimated in the billions. Fortunately, decryption solutions have become available for these attacks, mitigating their long-term impact. The table also highlights ongoing threats, such as the SamSam ransomware, which continues to target Windows servers. Furthermore, high-profile cases like the attacks on Travelex and the Colonial Pipeline demonstrate the willingness of affected entities to pay ransoms to restore operations, despite the broader implications for cybersecurity. Recent attacks on national infrastructure and public services, such as those experienced by the Costa Rican Government, underscore the growing trend of cybercriminals targeting essential public sector operations, resulting in significant daily financial losses. The

data breach at Swissport and the mitigation of the attack on Portuguese media company Impressa highlight the diverse outcomes of cyber attacks, where response strategies range from ransom payment to the successful removal of ransomware, though often with substantial data loss. In summary, the landscape of cyber threats remains dynamic, with attackers continually adapting their strategies to exploit new vulnerabilities. This necessitates ongoing vigilance and investment in cybersecurity measures to protect against future attacks. Addressing the shortcomings of existing security systems, this dissertation seeks to investigate the utilization of blockchain technology as a transformative solution to enhance the security of configuration files backup systems. By examining the advantages of implementing a blockchain-based backup system over traditional methods, this study aims to illuminate the potential impact of blockchain technology on cybersecurity innovation and data protection mechanisms. Through the exploration of blockchain's role in expanding information security and enhancing overall data resilience in network environments, this research endeavors to contribute to the ongoing advancement of network security practices in the digital era.

1.3 Research Questions

1. How can blockchain technology be utilized to enhance the security of configuration files backup systems?
2. What are the key advantages of implementing a blockchain-based backup system over traditional methods?
3. How can blockchain technology contribute to the expansion of information security and improve data backup in network environments?

1.4 Relevance of Research and Novelty

1.4.1 Relevance of Research

In today's digital age, data security and backup solutions are crucial in protecting sensitive information from an increasing variety of cyber attacks. Despite technological developments, enterprises still face persistent issues in guaranteeing the security and confidentiality of their data backups. *This study is extremely relevant since it addresses these continuing issues by investigating the potential of blockchain technology to change data protection systems.* Using blockchain's programmable and decentralized capabilities, this study intends to develop a cutting-edge solution that can improve the security and resilience of data backup systems in the face of growing cyber threats. The findings of this study are likely to provide useful insights and practical consequences for organizations looking to improve their information security procedures and reduce the risks associated with data breaches.

1.4.2 Novelty

The novelty of this research lies in its exploration of the innovative application of blockchain technology in the realm of network security and data backup systems. While blockchain technology has received a lot of attention for its usage in cryptocurrency transactions, its potential for improving data security procedures is still underexplored. This study adds to the growing topic of blockchain-based cybersecurity solutions by looking into how blockchain technology can be integrated into data backup systems. The proposed solution provides a fresh viewpoint on how enterprises might use blockchain to maintain the integrity and confidentiality of data backups, paving the door for improved information security policies and resilience to cyber threats. This study's novel character is expected to expedite advances in data protection techniques and drive additional research at the interface of blockchain technology and cybersecurity.

1.5 Aims and Objectives

This study aims to develop a blockchain-based security system for storing backup configuration files of network devices. Based on the challenges of network security highlighted in the document, it is proposed to implement a system for storing and protecting backup configuration files data based on blockchain technology. The following objectives were set for developing such a system:

- To create a Enterprise Network prototype for testing purposes.
- To develop the structure of the blockchain algorithm for the protection and security of data and configuration files of the network.
- To implement and test the algorithm for protecting data against vulnerabilities.

This study suggests the use of Blockchain technology to safeguard and store data, providing a new perspective on internet cybersecurity technology by leveraging programmable mechanisms, distributed systems, and decentralized structures of the Blockchain. The adoption of blockchain technology is expected to significantly advance data security innovation and enhance information security practices.

1.6 Thesis outline

The following chapters of this master's thesis on "Blockchain based configuration files backup system" provide a structured and thorough overview of the research:

Introduction:

- Overview of the rapidly evolving technological landscape and the importance of network security.
- Rationale for the research on blockchain technology for data security and backup systems.
- Research questions, relevance of research, aims, and objectives.

Literature Review

- Review of traditional backup systems and their vulnerabilities to ransomware attacks.

- Exploration of blockchain-based data storage systems, including IPFS and decentralized storage solutions.
- Examination of blockchain-based security mechanisms and their potential in enhancing network security.

Methodology

- Explanation of blockchain technology and its role in ensuring data integrity and security.
- Description of different types of blockchain networks and their characteristics.
- Implementation of blockchain in data backup and recovery systems.

Proposed System

- Development of a blockchain-based security system for storing backup configuration files of network devices.
- Design of the system architecture and data storage mechanisms.
- Integration of blockchain algorithms for securing data and configuration files.

Experiment and Results

- Evaluation of the proposed system through various scenarios, including ransomware attacks to traditional backup systems and blockchain-based backup systems.
- Assessment of performance and effectiveness in protecting data against vulnerabilities.

Conclusions and Future Work

- Summary of key findings and conclusions drawn from the research.
- Identification of future research directions and potential enhancements for the proposed blockchain-based backup system.

Chapter 2

Literature review

Given the rapid evolution of cyber-attacks in current technological landscape, security of networks is a top priority. Blockchain technology could be a feasible option as businesses explore for new methods to strengthen their defenses. This section's research builds on previous studies and contributions to illustrate how blockchain technology improves network security. This section includes a thorough review of relevant literature in the fields of backup security and blockchain technology. The selected studies and research articles cover a wide range of issues, including data backup strategies, decentralized storage systems, and novel blockchain-based approaches to ransomware protection. The purpose of examining these contributions was to better understand the growing landscape of data security and to investigate new techniques that use blockchain technology. These assessments collectively add to our understanding of blockchain's critical role in improving data integrity, security, and resilience in the face of increasing threats.

2.1 Traditional Backup Systems

Ransomware is a growing threat in business and government because it causes instant financial harm or the loss of critical data. There is a mechanism to identify and block ransomware in advance, yet advanced malware can still strike without being detected. Another option is to backup the original data. However, ransomware can take control of existing backup solutions and destroy backup copies. In 2018, Donghyun Min et al. [10] proposed Amoeba, an SSD system that provides automated backup. Amoeba, in particular, is equipped with a hardware accelerator capable of rapidly detecting page infection by ransomware attacks, as well as a fine-grained backup control system to reduce space overhead for original data backup. For evaluation, the Microsoft SSD simulator was updated to include Amoeba and analyzed using realistic block-level traces acquired while running the actual malware. According to the author's research, Amoeba has little overhead and surpasses the state-of-the-art SSD, FlashGuard, which allows for data backup within the device. Moreover, in 2022 [19] was presented AMOEBA, a device-level backup method that does not need any additional storage. AMOEBA is equipped with a hardware processor that allows it to run content-based ransomware detection algorithms at high speeds, as well as a fine-grained backup management

system that reduces storage overhead for data backup. The authors' assessments of real ransomware workloads reveal that AMOEBA offers high ransomware detection precision with low performance overhead.

In 2018 [20], a safe container-based backup technique was presented to withstand destructive ransomware attacks. The technique performs the backup in a highly limited local docker container, and only the container has access to both source and backup data stored in local and distant storage. That is, the host is only permitted to view the source data, while the container is only permitted to complete the backup procedure without any additional connections. As a result, any other processes on the host are unable to access the backup data saved in the container or remotely. Thus, even if the host and container are entirely destroyed, the data can still be restored from distant storage. The authors built a prototype system and demonstrated that it can back up data with excellent usability while also storing it securely.

Vaclav Oujezsky et al. [21] proposed a solution to address the issue of system data backups, which is a hot topic given the potential of cyber attacks. The project described in this paper intends to investigate, create, and develop a semi-intelligent malware protection system to safeguard backup data from cyber-attacks that include ransomware and malware. The emphasis was on artificial intelligence, automation, and support for the majority of backup and archiving applications, as well as full-agnostic solutions that included a malware protection system. The developed approach allows for both the active prediction of information infections and the detection of contaminated data on previously backed-up systems.

Jianping Zhang and Hongmin Li [22] created a security-enhanced data backup and recovery system to meet the demanding security standards of the military, national defense, and other key industries. The system uses existing backup and recovery technologies, such as digital certificate authentication, role-based access control, business model-driven process management, and operation log-based auditing, to assure the authenticity of data backup, operators, and recovery processes. This comprehensive approach effectively protects data confidentiality by prohibiting unauthorized operators from backing up data to illicit locations and restoring data to unauthorized target machines.

The report by Almountassir Bellah Balhasan et al. [23] sheds light on the information security architecture put in place by the Information Security Unit at Al Wahda Bank in Libya. The exam focuses on two key areas: software security and information/data security. In terms of software security, the study dives into the policies and tools that regulate two crucial aspects: the software development process for all applications in the bank's ecosystem, and the safeguards in place to protect devices from malware attacks. The research focuses on five key components of information and data security: classification, storage, backup, transmission, and disposal of information and data assets. Each of these areas is critical to ensuring the integrity, confidentiality, and availability of sensitive data throughout the bank's activities. The subsequent review of the study's information security system reveals three prominent areas that require further inquiry. To begin, the challenges associated with monitoring third-party software development are enormous, possibly exposing the bank to external threats. Second, differences

between established policies and their actual implementation call into doubt the effectiveness of security measures in practice. Finally, the retention time of 'unwanted' information and data emerges as a source of controversy, emphasizing the necessity for clearer data disposal norms. By integrating the study's findings, researchers obtain significant insights into the challenges of sustaining strong information security frameworks within financial institutions, opening the path for future research and security practice improvements.

Table 2.1 – Traditional Backup Systems

Paper Authors	**Key Contribution**	**Methodology/Approach**
Min et al. [10, 19]	Amoeba and AMOEBA: SSD systems with automated backup and ransomware detection	Equipped with hardware accelerators for ransomware detection, fine-grained backup control, evaluation using Microsoft SSD simulator with realistic block-level traces
Jin et al. [20]	Safe container-based backup technique to withstand ransomware attacks	Backup performed in a highly limited local docker container, secure storage of backup data
Oujezsky et al. [21]	Semi-intelligent malware protection system for safeguarding backup data	Focus on artificial intelligence and automation, active prediction of information infections, detection of contaminated data
Zhang and Li [22]	Security-enhanced data backup and recovery system for military and key industries	Use of digital certificate authentication, role-based access control, business model-driven process management, operation log-based auditing
Balhasan et al. [23]	Information security architecture at Al Wahda Bank in Libya	Examination of software security and information/data security, focus on classification, storage, backup, transmission, and disposal of information and data assets

Table 2.1 summarizes major scientific contributions in data backup and ransomware protection. Ransomware poses a huge danger to organizations and governments, prompting experts to investigate alternative strategies and systems for protecting sensitive data. The table includes noteworthy publications that propose automated backup solutions with ransomware detection mechanisms, safe container-based backup strategies, and semi-intelligent malware security systems. Each row in the table describes the authors' contributions, which include hardware accelerators for ransomware detection, safe storage approaches, and sophisticated security mechanisms for data backup and recovery. By reviewing these research initiatives, this study hopes to shed light on the changing environment of traditional backup systems and their role in mitigating the dangers posed by ransomware and

other cyber attacks.

2.2 Blockchain-Based Data Storage System

Wuqiang Shen et al. [24] present a novel technique to improving network server security using blockchain technology. The strategy entails building a data security storage alliance with several data acquisition base stations and optimizing the data storage procedure. The storage federation module securely stores collected data by compressing features and removing unnecessary data. The experimental results show promising outcomes, with a peak data storage integrity of 87.5%, minimal CPU utilization at 4.8%, and consistently low system congestion rates below 5%. These findings support the method's effectiveness by proving its capacity to assure secure and efficient data storage.

The Interplanetary File System (IPFS) has emerged as a pioneering approach for decentralizing web infrastructure and increasing its speed and efficiency. IPFS orchestrates a network of networked computing devices to allow for seamless information exchange, leveraging established technologies such as BitTorrent and Git. Since its introduction in 2016, IPFS has gained considerable awareness and adoption among a diverse range of user groups, including both individual users and large-scale enterprise enterprises. One of IPFS' most significant advantages is its distributed architecture, which allows users to share files and data internationally, breaking the traditional limits of centralized file storage and retrieval systems. IPFS, which is particularly well-suited to handle huge files that require significant bandwidth for transmission, has sparked interest for its potential to revolutionize Internet data transfer protocols. IPFS' versatility is further demonstrated by its interoperability with other protocols like as FTP and HTTP, which allows for simple incorporation into existing network infrastructures. Despite its various advantages, there are still worries about IPFS's security and access control measures. One of the most pressing concerns is the lack of traceability surrounding file access, which raises concerns about the integrity and confidentiality of data kept within the IPFS ecosystem. In response to these difficulties, Emmanuel Nyaletey et al. [25] presented novel techniques to strengthening IPFS with additional security measures, with a particular emphasis on blockchain technology. Blockchain technology, known for its decentralization and immutability, offers a compelling alternative for increasing the integrity of data saved and sent via IPFS. By adopting a novel approach known as BlockIPFS, researchers want to create a transparent audit trail for tracing all activity associated with a specific file, solving concerns about data integrity and authorship protection. Their research aims to highlight IPFS's strengths and limits through a thorough assessment of existing literature and technology, as well as to propose a promising way to mitigate its inherent security flaws. BlockIPFS, by combining blockchain technology with IPFS, provides a strong framework for securing the integrity and accountability of data transfers in decentralized file-sharing contexts.

An IPFS-based blockchain storage architecture was presented by Randhir Kumar and Rakesh Tripathi [26] to address the issue of storing transactions in a block. In the proposed storage technique, the blockchain's blocks are generated by

hashing the returned IPFS hash of each transaction that miners save to the IPFS distributed file system storage. It has been proposed to use content-addressed (IPFS hash) storage to protect transaction access to a specified block. The authors applied their method to a transaction that included blockchain hash storage and IPFS picture storage. Miners save transactions to IPFS, lowering block size using the generated IPFS hashes. The paper suggests a content-addressed storage method for protected transaction access in a block of data. The approach is implemented with Anaconda Python, Python Ask, and IPFS, resulting in a succinct and creative solution to blockchain storage concerns.

Md. Nasim Uddin et al. [27] present a complete plan for addressing secure file-sharing concerns by leveraging Blockchain and IPFS. The design stresses critical security principles like as authentication, confidentiality, integrity, and availability. Key system elements, including content owners, content users, Blockchain, and IPFS, work together to provide secure file sharing. To further security, the design uses encryption, smart contracts, and cryptographic authentication using Metamask. The Oyente vulnerability analysis tool guarantees robust protection against Smart contract vulnerabilities, with a focus on secure coding practices. In terms of cost, the system demonstrates cost-effectiveness, with little gas usage thanks to IPFS integration and the storing of file hashes in Blockchain. The paper also provides new features like as signature-based authentication, cryptographical authentication with Metamask, and advanced encryption algorithms like AES. These advances help to achieve the paper's goal of improving security and usability in file sharing systems.

Jia Kan and Kyeong Soo Kim [28] introduced the MTFS, a pioneering secure private file storage system. It employs a novel "Group Path" mechanism in which each node's hex hash string ID is compared throughout the network to identify linked nodes. For secure file uploading, the system uses PRE, an asymmetric encryption method. When users upload files, they are encrypted using a public key, resulting in both a cipher text and a supplementary 'capsule' file. This architecture generates objects using a Merkle tree, which allows for efficient handling of both small and big data. Additionally, MTFS is based on blockchain technology, which ensures data integrity and security. File exchanges, for example, are similar to sending an email, and they use PRE to ease procedures while preserving file content. The system also prioritizes data replication and periodic verification to prevent data loss and fraudulent node activity. MTFS provides a novel solution for high-performance, blockchain-based private file storage. An advance proxy re-encryption method was used by authors to ensure safe file exchanges with permission. In addition to being utilized for personal file storage and sharing, the proposed MTFS can also be employed in business when contract-making processes, such as insurance, call for mutual trust in file uploading and downloads.

Ismail A. et al. [29] demonstrate the interoperability of blockchain technology and decentralized file systems. While acknowledging the benefits of blockchain's dependability and openness, it tackles the difficulty of keeping vast amounts of data on-chain. The focus is on decentralized file systems that enable efficient data storage and retrieval for blockchain applications. The study compares the prices and latency performance of nine systems, emphasizing the importance of strik-

ing a balance between efficiency and decentralization. Overall, it delivers concise insights about enhancing data storage using blockchain. Authors [29] evaluate the performance of various DFS solutions, focusing on IPFS, Swarm, Storj DCS, and Sia. Notably, IPFS is known for its reliability and strong community support, despite latency issues that might vary depending on node bandwidth and DHT operations. Swarm outperforms IPFS on private networks in terms of performance and resource usage. Storj DCS touted excellent availability and quick speeds, however, users experienced performance issues. Sia's promised speeds were not routinely met during tests. Furthermore, in 2023, Jyotsna Anthal et al. [30] investigate the disruptive potential of integrating blockchain technology and the Interplanetary File System (IPFS) to enable secure and decentralized file sharing. It criticizes centrally hosted servers for their privacy and security issues with file sharing. The examination includes specific use examples, such as File Coin, which uses IPFS and blockchain to create a storage marketplace. The article acknowledges problems such as scalability and regulatory issues, but emphasizes the transformative implications of this technology on digital content delivery. It compares various decentralized storage options (such as Sia, Storj, and MaidSafe) to IPFS and blockchain-based file sharing. The study [30] expands its scope to consider potential effects on industries such as media, entertainment, and healthcare. Finally, it presents a thorough grasp of the subject, arguing that blockchain and IPFS show promise for the future of secure and efficient file sharing, addressing long-standing issues in the industry.

Ashwini S. et al. [31] address the critical topic of securely and efficiently storing medical images in the healthcare business, taking into account the sensitive nature of patient data and the growing threat of cyberattacks. The authors offer a new framework that combines blockchain technology and the InterPlanetary File System (IPFS) to create a safe and decentralized storage solution. In the proposed paradigm, each medical image is allocated a unique cryptographic hash and saved on IPFS, which enables content-addressable storage, assuring data integrity and preventing manipulation. The Ethereum blockchain is used to record transaction details, enabling for off-chain storage of medical photos without regard for blockchain size. This combination provides a compelling answer to the security and scalability concerns associated with medical picture storage. The experimental prototype demonstrates the approach's practicality, with a focus on content-addressing to improve security. The suggested system shows great potential for protecting sensitive healthcare data while allowing for rapid access and retrieval, constituting an important step toward securing data privacy and integrity in the healthcare arena.

Kai-Wei Lin and Yu-Chi Chen [32] present a file verification mechanism based on Verkle trees that improves information security by allowing users to check downloaded files without requiring third-party participation. The system protects files and detects tampering by utilizing the Inter-Planetary File System (IPFS) and blockchain. Verkle trees, which are noted for their efficient proof size, are used for strong file verification. The study covers the growing worry about malware assaults using various file formats, highlighting the Verkle tree's advantage in reducing proof size. The proposed solution involves uploading original files to IPFS and assigning

them hash values stored on the blockchain. Verifiers compare hash values from decompressed files to the Verkle tree generated from blockchain data. In the event of a discrepancy in verification, users can obtain the correct file from the blockchain via IPFS. This solution improves information security by providing users with a reliable way to validate downloaded files while exhibiting the efficiency of Verkle trees in comparison to Merkle trees.

In 2023, Rupsingh Mathwale and Ramarao Ramisetty [33] introduced a blockchain-based inter-organizational safe file-sharing system, which provides a solid method for securely exchanging files across a dispersed coalition of businesses. Using Hyperledger Fabric, an enterprise-grade blockchain framework, for network setup and smart contract development, as well as the InterPlanetary File System (IPFS) for distributed storage of files, the suggested system addresses the pressing need for secure and efficient file sharing in inter-organizational contexts. The workflow provided in the paper combines identity management and file-sharing protocols to provide a comprehensive framework for protecting the confidentiality, integrity, and availability of shared data inside the consortium. Using blockchain technology, the system makes transactions visible and auditable, reducing the risk of illegal access or tampering. The use of Hyperledger Fabric and IPFS demonstrates the authors' dedication to leverage cutting-edge technology to address the issues of secure file sharing across organizational boundaries. Hyperledger Fabric's permissioned blockchain design provides granular access control and scalability, making it ideal for consortium situations where participants trust one another. In the meantime, IPFS's decentralized storage architecture improves data resilience and availability, making files available even during network disruptions or node failures. The suggested approach has great potential for improving collaboration and data interchange among businesses while ensuring strong security and data integrity. However, additional research is needed to assess the system's scalability, performance, and interoperability in real-world deployments across a variety of sectors and use cases. Furthermore, concerns for regulatory compliance and governance frameworks may be required to secure the system's adoption and long-term viability in inter-organizational situations.

Pearl Alisha Lobo and V Sarasvathi [34] introduced a novel technique for improving the security of patients' medical data kept digitally in the present centralized architecture. The study identifies problems with illegal access to sensitive information, such as patients' personal information and medical records. To overcome these issues, the researchers propose a distributed file system based on the Interplanetary File System (IPFS) and blockchain technology. The solution entails keeping the hash value of medical reports in the blockchain, thereby lowering their size, while the real files are saved in IPFS as hash values. This framework protects patient privacy while allowing authorized users, such as doctors and patients, convenient and safe access to information. The research concludes that the suggested system manages medical data with availability, integrity, and consistency.

Table 2.2 – Analytical Evaluation of Research Papers

Paper Authors	**Key Contribution**	**Methodology/Approach**
Shen et al. [24]	Improving network server security using blockchain technology	Data security storage alliance with data acquisition base stations, storage federation module
Kumar and Tripathi [26]	IPFS-based blockchain storage architecture	Generating blockchain blocks by hashing IPFS hashes of transactions, content-addressed storage
Uddin et al. [27]	Secure file-sharing using Blockchain and IPFS	Authentication, encryption, smart contracts, cryptographic authentication with Metamask
Kan and Kim [28]	MTFS for secure private file storage	"Group Path" mechanism, PRE encryption, Merkle tree-based architecture
Ismail et al. [29]	Interoperability of blockchain technology and decentralized file systems	Performance evaluation of DFS solutions, emphasis on efficiency and decentralization
Anthal et al. [30]	Integrating blockchain technology and IPFS for secure and decentralized file sharing	Critique of centrally hosted servers, comparison of decentralized storage options
Ashwini et al. [31]	Secure and decentralized storage of medical images using blockchain and IPFS	Unique cryptographic hash for each medical image, Ethereum blockchain for transaction recording
Lin and Chen [32]	File verification mechanism using Verkle trees, IPFS, and blockchain	Strong file verification, efficient proof size with Verkle trees
Lobo and Saraswathi [34]	Distributed file system for secure storage of patients' medical data using IPFS and blockchain	Hash value storage in blockchain, real files saved in IPFS

Thomas Renner et al. [35] recently introduced Endolith, a groundbreaking auditing platform that automatically verifies file integrity and tracks file history, removing the need for third-party intermediaries. Endolith uses a smart contract-based blockchain infrastructure to enable tamper-proof storage of annotated files and change-related metadata, such as file hashes. This novel approach allows Endolith to demonstrate whether a file, which has been stored for a long time, has been unauthorizedly altered, and if so, to trace the timing and responsible party for the changes. Endolith's implementation is built on Ethereum, a popular blockchain technology known for its programming ability and smart contract capabilities, as well as the Hadoop Distributed File System (HDFS), which is noted

for its scalability and fault tolerance. Endolith provides a comprehensive solution for data integrity and transparent auditing processes by continuously monitoring annotated files and storing information on blockchain. Renner et al.'s [35] examination of a public blockchain network highlights Endolith's efficiency, particularly for files that are rarely modified but frequently accessed—a prevalent feature of data archives. This validation illustrates Endolith's practical usefulness in real-world circumstances where data integrity and traceability are critical. Endolith's significance extends beyond its immediate application, as it adds to the broader discussion about blockchain-based solutions for data integrity and auditing. Endolith demonstrates the potential of blockchain technology to transform traditional approaches to data management and verification by utilizing decentralized, immutable ledgers and smart contracts. Despite its promise, more research is needed to determine Endolith's scalability and usefulness across a wide range of use cases and environments. Furthermore, investigations into potential security concerns and efficiency enhancements may improve Endolith's uptake and effectiveness in real-world deployments.

Table 2.2 provides a comparative analysis of the reviewed research publications connected to IPFS/MTFS and data storage, highlighting each paper's features and contributions to the security of data and blockchain technology.

2.3 Blockchain-Based Security

O. S. Abuomar and R. Y. Gross [36] offer a theoretical yet viable solution for protecting digital evidence from ransomware assaults. The suggested method combines RAID 10 (1+0) technology for data stripping and mirroring, BitTorrent for network evidence distribution, and blockchain algorithms for authenticity certification. Key features of the proposed system:

- Digital evidence is securely kept utilizing RAID 10 technology, which provides data redundancy and protection against disk failures.
- All evidence is hashed with SHA-256 within a blockchain, ensuring great data integrity. Any changes to the evidence will be discovered owing to hash differences.
- BitTorrent technology is used to distribute evidence throughout a peer-to-peer network, eliminating the need for centralized servers while also improving security.
- The system's design is intended to prevent data loss in the case of a ransomware attack. Even if some of the evidence is compromised, the system can be reconstructed using mirrored nodes.
- The mechanism assures authenticity by hashing the headers of each block on the blockchain. This makes audits easier and helps identify any evidence.

While the theoretical concept appears promising, it also emphasizes the need for additional research and testing. The combination of RAID 10 with blockchain and BitTorrent is novel and has potential applications beyond securing digital evidence, such as in the medical profession to preserve patient information and in other government sectors to ensure data integrity and secrecy.

Wei Cai and Jian Qu [37] in their thesis focus on blockchain-based network information security, examine the overall state of the information security system based on the distributed and clustered characteristics of the blockchain. Due to its non-tamperable and high credibility properties, the network security mechanism built on the foundation of blockchain to safeguard connected data and information can be utilized as a potent tool to enhance the security of data and information in cyberspace.

In 2020 Ke Yang et al. [38] offer a security protection solution based on blockchain technology from the perspectives of identity authentication, data protection, and security operation and maintenance, and provide a technical idea for enhancing the network security protection capability of the energy industry.

Saha Reno et al. [39] announced a new solution for safe forensic information storage in 2021, based on the Inter-Planetary File solution (IPFS) and a private Hyperledger blockchain. Their method allows for the detection of unauthorized entry or data modification by intruders, providing strong security safeguards for forensic applications. The hybrid technique presented by the authors is a substantial improvement over traditional public blockchain systems like Bitcoin and Ethereum, particularly in terms of transaction processing time. Their technology outperforms standard public blockchains in terms of transaction processing speed, with an average of 11.99 seconds, increasing operational efficiency and responsiveness. Furthermore, Reno et al.'s [39] method allows for the storage of heavyweight

features, which is not possible with current blockchain frameworks. This feature broadens the range of applications for blockchain technology, particularly in sectors that need the storing of vast or complex datasets. The authors developed a strong platform for safe forensic information storage by integrating IPFS's decentralized and resilient properties with the permissive and efficient features of a Hyperledger-based private blockchain. This technique not only overcomes the difficulties of data integrity and tamper resistance, but it also provides better performance and scalability than traditional blockchain solutions. The authors emphasize the ability of hybrid blockchain architectures to overcome the limits of traditional systems and open up new opportunities for data management and security. However, more research is needed to assess the scalability, interoperability, and security implications of this technique in many real-world contexts. Furthermore, ongoing breakthroughs in blockchain technology and forensic sciences may create chances for future system capability and functional enhancements.

Noor Thamer and Raaid Alubady [40] proposed a revolutionary solution meant to protect healthcare patient records against Ransomware assaults by exploiting blockchain technology's extensive security capabilities. This system addresses both external and internal risks by utilizing smart contract algorithms, resulting in a multi-layered protection mechanism. The results show a significant reduction in transaction costs while also increasing the anticipated time necessary for attackers to penetrate the system. Although these findings are encouraging, there are various areas for additional research. First, transferring from a theoretical foundation to practical execution remains difficult. The system's scalability, performance in real-world scenarios, and compatibility with existing healthcare infrastructure all require more investigation. Furthermore, a more comprehensive security evaluation is required to certify the system's resilience to a larger spectrum of cyber attacks. The study focuses mostly on Ransomware attacks, although healthcare systems confront a wide range of other security threats, including botnets, rootkits, and Distributed Denial of Service (DDoS). Future work could improve the system's ability to prevent these threats and provide comprehensive protection for sensitive patient data.

The Blockchain-Enabled Security Framework Against Ransomware Attacks in Smart Healthcare (BSFR-SH) [41] is a complete framework for protecting smart healthcare systems from ransomware attacks. It consists of five essential steps, beginning with the development of secure healthcare data backups using blockchain technology. During this phase, data is saved as encrypted transactions to ensure its integrity and security. The following phase includes data collecting, signature generation, and feature development for ransomware detection using machine learning approaches. Various methods, including as random forest, logistic regression, decision tree, and k-nearest neighbors, are used to detect ransomware patterns and behaviors. If ransomware is discovered, the framework begins a mitigation process that includes isolating the compromised system, deleting the ransomware, and, if required, negotiating a secure payment to the attacker for data recovery. Blockchain technology is utilized in data recovery to ensure that encrypted backups are safely retrieved and delivered to the damaged system. The framework's security analysis confirms its resistance to numerous threats, while practical ap-

plication demonstrates its effectiveness. Future work could focus on improving functionality and accuracy while retaining security, thereby strengthening smart healthcare systems against ransomware threats.

Table 2.3 – Summary of Research Papers on Blockchain-Based Security

Paper Authors	**Key Contribution**	**Methodology/Approach**
Abuomar and Gross [36]	Theoretical solution for protecting digital evidence from ransomware assaults	Combination of RAID 10 technology, BitTorrent, and blockchain algorithms
Cai and Qu [37]	Focus on blockchain-based network information security	Examination of blockchain's characteristics for enhancing network security
Yang et al. [38]	Security protection solution for the energy industry based on blockchain technology	Identity authentication, data protection, security operation, and maintenance
Reno et al. [39]	Solution for safe forensic information storage using IPFS and a private Hyperledger blockchain	Integration of IPFS and Hyperledger for secure storage and efficient transaction processing
Thamer and Alubady [40]	Proposal for protecting healthcare patient records against ransomware assaults using blockchain technology	Utilization of smart contract algorithms for multi-layered protection
BSFR-SH [41]	Framework for protecting smart healthcare systems from ransomware attacks using blockchain technology	Development of secure healthcare data backups, ransomware detection using machine learning, and blockchain-based data recovery
Arifudin et al. [42]	Validation of data authenticity using blockchain and IPFS combined with a vote system	Combining blockchain, IPFS, and voting mechanisms for transparent and democratic verification

In recent years, experts have begun to notice the possibilities of blockchain and IPFS. In 2023, Akhmad Rizal Arifudin et al. [42] developed a revolutionary way for validating data authenticity by combining these technologies with a vote system. The authors attempted to address the development of hoaxes and disinformation in the digital age, which poses a serious challenge to society, affecting areas such as politics, public health, and social cohesion. Their approach assures information security and integrity while providing transparent and democratic verification mechanisms. The inclusion of a voting system adds a layer of validation, allowing users to collectively assess the authenticity of data and prevent the inclusion of inaccurate or deceptive material. This participatory approach

adheres to democratic and transparent ideals, allowing people to make contributions to the verification procedure while also creating trust in the dataset. While earlier research has looked into numerous techniques to combating misinformation, the suggested system is a one-of-a-kind combination of blockchain, IPFS, and voting mechanisms designed to meet the specific issues of protecting datasets from hoaxes. By leveraging the benefits of these technologies, researchers hope to establish a solid framework for preserving trustworthy information sources in an age of digital misinformation. The authors' methodologies and algorithms are remarkably similar to those offered for countering ransomware assaults. However, more study is needed to assess the usefulness and scalability of this strategy in real-world scenarios and across disciplines.

Table 2.3 provides a full summary of the important contributions and methodologies/approaches covered in the evaluated literature, allowing for a thorough examination of the research landscape around data storage systems and their security mechanisms. Each row in the table corresponds to a research article written by specialists in the area, explaining their individual contributions to the improvement of blockchain-based data storage security. The 'Key Contribution' column highlights the key focus or innovation offered by each publication, which might range from novel techniques for preserving digital evidence from ransomware attacks to frameworks created expressly for securing healthcare patient records. On the other hand, the 'Methodology/Approach' column gives information about the techniques or approaches used by the authors to handle the highlighted issues and achieve their goals. These techniques include leveraging blockchain technology, using machine learning algorithms to detect ransomware, and incorporating decentralized storage solutions such as IPFS. By summarizing the important findings of each paper in a systematic manner, the table provides a clear and succinct summary of the many tactics and advances suggested in blockchain based security.

2.4 Blockchain-Based Backup System

An important challenge in disaster recovery systems, particularly in multi-cloud setups, was addressed in 2022 [43]. The authors stress the vulnerabilities associated with centralized storage, stating that a storage server compromise can pose considerable data security threats. To reduce these risks, they suggest a distributed and decentralized storage approach based on blockchain technology to ensure data integrity and security. The main components of this proposed solution are:

- Data backup is dispersed among multiple cloud storage nodes, lowering the chance of data loss in the event of a security compromise.
- Blockchain technology is used to build an immutable and transparent ledger for tracking data access and assuring its integrity. Smart contracts, cryptography, and consensus procedures all play an important part in sustaining confidence.
- Data is saved redundantly across numerous storage nodes to ensure data availability even in the event of a failure.
- The system includes a rigorous security auditing procedure that monitors user identities, rights, and data integrity.

However, Bin Liu et al. [43] recognize the difficulty of establishing real-time data backup and recovery, especially for applications that require low latency. This constraint emphasizes the need for additional research and development to meet the demands of real-time catastrophe recovery in essential applications.

Jinqian Chen et al. [44] suggest a blockchain-based data recovery solution. Power Internet of Things data nodes use edge data processing servers to encrypt important data and backup those files to the blockchain system. Real-time data node integrity detection is performed by the data processing server. On the basis of the test findings, this system's data backup and recovery speeds are faster than the conventional plan by 15.3% and 19.8%, respectively.

SK Mouleeswaran et al. [45] in their study provide a novel architecture for transparent, authenticated online storage that eliminates data duplication from file security and raises the legitimacy of blockchain technology. The usage of double hazing and symmetrical encryption are two distinct methods for achieving data deduplication secrecy that are covered in their article.

In 2018 [46] was suggested a system that has a graphical user interface and allows system administrators to make backup copies of specific data, that were preserved utilizing the blockchain approach in an encrypted fashion and the prior key can be used by system administrators to verify the validity of files.

Ransomware Protection (RAP) strategy based on blockchain was presented in 2022 by Weilun Lao et al. [6] RAP uses an improved all-or-nothing transform (AONT) and provides a secure channel for setup, uploading backups, and data recovery. Authors launch RAP on an Ethereum-based consortium blockchain and assess its functionality. As a result, each RAP phase runs in less than 1 millisecond, read/write delays for typical data sizes excluded. The authors' key contribution is the development of a novel RAP system model. This model employs a consortium blockchain for access control, guaranteeing that only trustworthy users gain access. The inclusion of permitted gateways is an important element that improves secu-

rity against DDoS attacks. The authors go on to describe a specific RAP scheme that combines a pseudorandom function (PRF) with an optimized all-or-nothing transform (AONT) for data encoding, providing greater efficiency than typical AONT. Notably, the system's practical implementation on the Ethereum platform yielded amazing results, with data recovery times estimated in milliseconds. This paper presents a viable blockchain-based method for ransomware defense that prioritizes security and efficiency.

Table 2.4 – Summary of Research Papers on Blockchain-Based Backup Systems

Paper Authors	**Key Contribution**	**Methodology/Approach**
Liu et al. [43]	Proposal for a distributed and decentralized storage approach based on blockchain technology for disaster recovery	Utilization of blockchain for immutable ledger, data redundancy across multiple nodes, and rigorous security auditing
Chen et al. [44]	Blockchain-based data recovery solution for Power Internet of Things data nodes	Encryption of important data, backup to blockchain system, and real-time data node integrity detection
Mouleeswaran et al. [45]	Novel architecture for transparent, authenticated online storage using blockchain	Use of double hashing and symmetric encryption for data deduplication secrecy
Aleidi et al. [46]	System with graphical user interface for blockchain-based backup of specific data	Encryption of data and verification using prior key
Lao et al. [6]	Ransomware Protection (RAP) strategy based on blockchain with improved all-or-nothing transform (AONT)	Implementation on Ethereum-based consortium blockchain, secure channel for setup, uploading backups, and data recovery
Sokolov et al. [47]	Framework for decentralized regulation of restore strategies and evaluation criteria for backup service providers	Decentralized backup algorithm, encryption of files, distribution among different nodes, and evaluation of backup service providers

In 2022 [47] was provided a method for enhancing the effectiveness of backup restoration procedures using blockchain technologies. Strahil Sokolov et al. [47] proposed a framework for decentralized regulation of restore strategies, along with an overview of current cloud providers and backup strategies. They present a decentralized backup algorithm and evaluation criteria for backup service providers, highlighting the need of a strong data backup strategy in protecting against the numerous hazards outlined. The paper emphasizes the importance of choosing

the correct backup service provider and the requirement for a well-structured data backup strategy. It identifies potential risks, such as cyberattacks and natural catastrophes, and proposes criteria for selecting service providers, such as budget considerations and employee training. Furthermore, the study provides a decentralized backup mechanism that encrypts files and distributes them among different nodes. The strategy appears to be a promising way to secure and distribute data efficiently. The paper's [47] usability and evaluation of proposed techniques indicate that the use of blockchain in the backup process enhances the reliability of decentralized storage.

Blockchain technology has received a lot of interest for its potential uses in assuring data integrity, security, and resilience in disaster recovery and backup systems. Table 2.4 summarizes research papers that investigate various approaches and methodologies for implementing blockchain in backup systems.

This chapter tried to consider the evolving landscape of data security and resilience by exploring the role of blockchain technology in traditional backup systems, blockchain-based data storage systems, and blockchain-based security mechanisms. Through an in-depth review of literature, various research contributions were analyzed, highlighting innovative approaches and methodologies to enhance network security and data integrity. By examining the key contributions and methodologies presented in the literature, this chapter has shed light on the potential of blockchain technology to improve data backup, storage, and security systems. From safeguarding digital evidence against ransomware assaults to enhancing the efficiency of backup restoration procedures, blockchain technology has demonstrated its versatility and effectiveness in addressing critical challenges in data security. As organizations continue to face evolving cyber threats, integrating blockchain technology into backup and security systems can provide a robust layer of protection against data breaches and unauthorized access. The findings presented in this chapter lay the foundation for further research and exploration in leveraging blockchain technology to enhance data security practices in various sectors. Moving forward, continued research and innovation in blockchain-based solutions will be crucial in mitigating the risks posed by cyber threats and ensuring the integrity, confidentiality, and availability of sensitive data in an increasingly digitized world.

Chapter 3

Methodology

3.1 Concepts of Blockchain technology

This research proposes a new approach to protect and store data based on Blockchain technology. Blockchains are well recognized for their critical function in cryptocurrency structures in storing a safe and independent record of transactions, but they may also be used to make data unchangeable in any business. This system recognizes users as the owner of their data without transferring and storing it in a centralized server [48], which is frequently exposed to cyberattacks. Blockchain is a network of hashed blocks that store data, unlike traditional database structures [49].

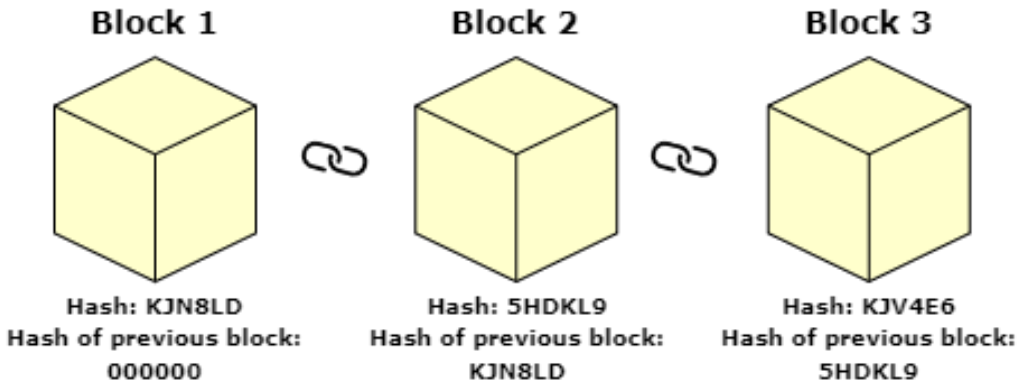

Figure 3.1 – The blockchain's fundamental concept

The primary distinction between a traditional database and a distributed ledger, such as a blockchain, is how the data is organized and accessible. The blockchain contains transaction information in a block of data. When it is filled, the data is processed through a hashing algorithm, which produces a hexadecimal number known as the hash. Figure 3.1 illustrates that each block stores both information and the hash of the previous block. The initial block is known as the genesis since it contains no information regarding the hash of the previous block. The data is saved in a block then hashed, and the resulting hash is added to the following block's data; the hash used as a salt changes each time. The hash is then placed

into the next block header and encrypted alongside the rest of the block's data. This results in a chained sequence of blocks.

A blockchain is a distributed database that distributes records across numerous network nodes, providing data redundancy and security. If one node attempts to modify a record, the decentralized nature of the other nodes precludes such changes. This distributed configuration prohibits any single node from altering the stored data. Because of this distribution and the crypto verification process, once data is recorded, such as digital currency transactions, it becomes irreversible. Aside from transactions, blockchains can hold a variety of data kinds, such as legal agreements, state IDs, and company inventory records [50]. In blockchain technology, since following blocks won't accept this information if the block's hash changes, it is not possible to change the data in a block.

3.1.1 Blockchain Network Types

There are various sorts of blockchain networks, which differ in terms of accessibility, governance, and participants [51, 52]:

- Public Blockchain Networks: These are public networks, similar to Bitcoin, in which anybody can join, take part, and validate transactions. They do, however, have drawbacks like as high processing requirements, restricted privacy, and possible security issues, making them less suitable for some corporate applications.
- Private Blockchain Networks: Private blockchains, in contrast with public blockchains, are decentralized but regulated by a single entity. This organization decides that is eligible to join the network, validates transactions, and keeps the ledger up to date. Private blockchains, which operate behind company firewalls or on-premises, can improve trust among participants in specific use cases.
- Permissioned Blockchain Networks: Permissioned networks, a subclass of private blockchains, add another level of access restriction. Permissioned models can exist even within public blockchains, defining that are eligible to participate along with what transactions they are able to perform. Access is often granted through an invitation or through specified permissions, allowing for more controlled and secure operations.
- Consortium Blockchains: This strategy entails numerous entities working together to maintain a blockchain. Instead of a single institution administering the system, a group of already chose organizations share authority. Consortium blockchains are useful when all parties require permissioned access and shared responsibility, which makes them appropriate for collaborative corporate situations.

3.1.2 Blockchain Consensus Protocols

Consensus protocols, which promote agreement among network members on the present state of the distributed ledger, maintain the security and dependability of a blockchain network. These algorithms are critical for creating trust and main-

taining the blockchain's integrity. Here are several popular consensus algorithms [52]:

- Proof of Work (PoW): Used by Bitcoin, PoW forces miners to use computer power to solve complicated mathematical challenges. The miner who solves the riddle first validates and adds the next block to the blockchain receives a reward. While successful, PoW uses a significant amount of energy due to its processing requirements.
- Practical Byzantine Fault Tolerance (PBFT): PBFT is a consensus mechanism used in distributed systems to achieve agreement even when some nodes are broken or hostile. It reaches consensus through the way nodes communicate in numerous rounds, with transactions verified in two stages.
- Proof of Stake (PoS): Popularized by Ethereum's transition, PoS incentivizes its validators to verify blocks based on their network stake rather than processing capacity. Validators stake coins, and those chosen to confirm and add blocks are rewarded proportionally, boosting network security and efficiency.
- Delegated Proof Of Stake (DPoS): In DPoS, users delegate voting power to selected delegates who confirm transactions and build blocks. Delegates are elected on the basis of their reputation and efficiency, and they share block rewards with other voters in order to encourage active involvement and delegation.
- Proof of Burn (PoB): In PoB, validators "burn" or transfer coins to unspendable accounts to demonstrate their dedication to the network. Validators are then chosen to construct blocks based on the number of coins burned, aligning incentives while avoiding the computational waste related to PoW.
- Proof of Capacity: Validators assign hard disk space to solve cryptographic problems in this proof of capacity. The more storage the validator devotes, the more likely it is that they will be selected to add the following block, increasing efficiency and accessibility.
- Proof of Elapsed Time (PoET): PoET is a permissioned blockchain-specific consensus algorithm. Those wait for a random amount of time, demonstrating their delayed time to the network. To ensure fairness and prevent monopolization, the validation device with the least amount of time is chosen to add the following block.

Algorithms for consensus serve a critical role in blockchain networks by ensuring participant agreement, security, and trust. Each algorithm provides distinct ways for validating transactions and maintaining network integrity, hence catering to a wide range of blockchain contexts and requirements.

3.2 Proof of Work

Proof-of-Work (PoW) is a fundamental consensus mechanism in the blockchain system that encourages miners to verify network transactions with computational efforts [52]. Miners increase their chances of receiving rewards in this system by contributing more processing power. Notably, PoW accounts for around 60% of all bitcoin market capitalization. The PoW consensus mechanism's primary purpose is to ensure the safety and reliability of every transaction within the distributed ledger network.

3.2.1 The Nodes

A network of decentralized computers known as nodes is critical in the Proof-of-Work blockchain technology. These nodes are responsible for two things: accepting batches of transactions from other nodes and validating or suggesting additional blocks of transactions to the network. These nodes, known as miners, invest computational power in exchange for the blockchain network's inherent coinage. In Proof-of-Work, the term "work" refers to the computational power that nodes supply to authenticate a new transaction block. The SHA-256 cryptographic hashing algorithm represents this computational effort, distinguishing this consensus process from others. An algorithmic technique called as difficulty adjustment recalibrates every 2,016 blocks, or nearly two weeks, to ensure consistent block validation time of 10 minutes [53]. Individual miners entering or leaving the network have no direct effect on the difficulty adjustment. Miners are rewarded when they find a hash that is less than the network-defined threshold. When a miner discovers a valid block hash, he or she distributes it to peers for quick validation and inclusion into their own blockchain records. This rigorous authentication process reduces the danger of fraudulent acts such as trying to double-spend digital funds.

3.2.2 The Reward

The remuneration granted to miners after completing the proof-of-work procedure is governed by a specified regulation. According to the most recent data [54], miners consistently earn a reward of 6.25 BTC for each validated block, in addition to all transaction fees. This reward structure acts as a motivator, encouraging miners to participate in the proof-of-work mechanism honestly, given that any kind of fraud would result in a waste of resources. It is worth noting, however, that this incentive is halved roughly every 210,000 blocks, which corresponds to a four-year period. The halving cycle is a reduction technique that gradually reduces the block payment by half. Concerns have been raised that if the market value of Bitcoin doesn't keep on climb at the same rate, miners' incentives may dwindle. Nonetheless, a self-adjusting mechanism kicks in: as miners leave owing to lower profitability, the system's difficulty level decreases, reducing the operational costs connected with Bitcoin mining.

3.2.3 Mining and Proof-of-Work (PoW) Relationship

Mining and Proof-of-Work (PoW) are ideas that are inextricably linked inside the blockchain ecosystem. PoW specifies the particular approach miners must follow in order to demonstrate to their peers that they have completed the required calculations by generating a hash that matches the block's goal criteria [55]. At the same time, mining stresses the act of adding a new block to the ledger and receiving the associated coin rewards. The processing of transactions made with Bitcoin can be used to better understand the interaction between PoW and mining. Every transaction initiated by a user on the Bitcoin network congregates in a communal pool known as the memory pool, or mempool. Miners explore this mempool, selectively selecting transactions to include in the next Bitcoin block that they hope to confirm. Nonetheless, the validation process for a candidate block is demanding. Miners must perform computational operations in order to generate a hash that falls below the barrier set by Bitcoin's PoW method. The first miner to reach this milestone distributes the confirmed block to other miners, allowing for a smooth verification and inclusion process into the larger blockchain ledger. Finally, the victorious miner receives all the block rewards and the relevant transaction fees, indicating the insertion of a genuine block to the Bitcoin network. As a result, the Bitcoin blockchain's stature rises, signaling the start of a new mining search for subsequent blocks.

3.3 Asymmetric Encryption

To secure data communications, asymmetric encryption, often known as public-key cryptography, uses a dual-key method. This system includes a public key that can be distributed and a corresponding private key that is kept safe by its holder [56]. When using asymmetric encryption, the sender uses the recipient's public key to encrypt data, while the recipient uses their private key to decode it [57]. This cryptographic approach has several advantages over symmetrical encryption, which uses a single key for both encryption and decryption. A fundamental advantage of asymmetric encryption is the elimination of the need to share secret keys, which can be time-consuming, especially in multi-party communications. Furthermore, asymmetric encryption makes it easier to generate digital signatures, which strengthens data authenticity verification processes. Asymmetric encryption is useful in securing online interactions, including email secrecy, online purchasing, and financial transactions. Furthermore, it is critical in verifying digital documents and messages via the use of digital signatures. Asymmetric encryption techniques of note include RSA, Diffie-Hellman, and Elliptic Curve Cryptography (ECC), which jointly enable a wide range of secure digital communication modalities [58].

3.3.1 Advantages of Asymmetric Encryption

Asymmetric encryption, often known as cryptography with a public key, is a type of cryptography that employs two distinct keys to both encrypt and decrypt data. Here are some of the benefits of asymmetric encryption.

- Increased Security: Unlike symmetric encryption, which utilizes a single key for both encryption and decryption, asymmetric encryption employs separate keys for these operations. The recipient keeps the private key, making intercepting and decrypting the data far more difficult for potential attackers.
- Authentication: Asymmetric encryption makes sender authentication easier. The sender's identity can be verified by encrypting a message with their private key, which can only be decrypted by their corresponding public key. The successful decryption confirms that the communication was sent by the legitimate sender who possesses the private key.
- Non-repudiation: This cryptographic method ensures non-repudiation, which means that senders cannot deny sending a message or change its content. Because messages encrypted using the sender's private key require their public key to decrypt, recipients may determine the message's origin and integrity.
- Key Distribution: Asymmetric encryption simplifies the difficulties of safe key distribution, which is required in symmetric encryption methods. While symmetric encryption requires the secure sharing of a single key between parties, asymmetrical encryption, on the other hand, permits public key dissemination while keeping the recipient's private key secret.
- Asymmetric encryption's applicability spectrum spans a wide range of industries, including safe electronic correspondence, online banking, and e-commerce activities. Furthermore, it supports SSL/TLS connections, which are critical for securing internet traffic.

In summary, the numerous benefits of asymmetric encryption include increased security, robust authentication procedures, non-repudiation assurances, streamlined key distribution processes, and broad applicability. These benefits, taken together, cement its position as the dominant cryptographic technology for protecting sensitive data across diverse digital domains.

This Methodology chapter attempted to study and clarify the core principles of blockchain technology, including its possible uses and the many types of blockchain networks and consensus algorithms. This chapter sought to provide a full grasp of blockchain technology by digging into its complexities, such as its decentralized nature and cryptographic hashing algorithms. Furthermore, the chapter delves into the Proof of Work (PoW) consensus process, a key component of blockchain security, explaining its role in confirming transactions and compensating miners. The conversation focused on the relationship between mining and PoW, emphasizing the computing efforts required to generate valid blocks inside the blockchain network. Moreover, the chapter examined asymmetric encryption, a critical cryptographic technique used to safeguard data communications in blockchain networks and beyond. By discussing the benefits of asymmetric encryption, such as enhanced security, authentication, and non-repudiation, the chapter highlighted its vital role in preserving the integrity and secrecy of digital transactions.

In conclusion, this Methodology chapter provides a thorough understanding of the fundamental principles that drive blockchain technology, consensus processes, and cryptography techniques. By clarifying these concepts, this study lays the framework for future investigation and implementation of blockchain-based solutions to satisfy the research objectives mentioned in this paper.

Chapter 4

Proposed System

The suggested solution uses a private blockchain network to maintain the confidentiality and integrity of server and network configuration backup files. This section describes the architecture, encryption technologies, consensus process, and data retrieval process used in the system.

4.1 System Architecture

The proposed system architecture aims to introduce a revolutionary method for preserving and ensuring the confidentiality of backup configurations from servers and network devices by integrating a tailor-made blockchain network.

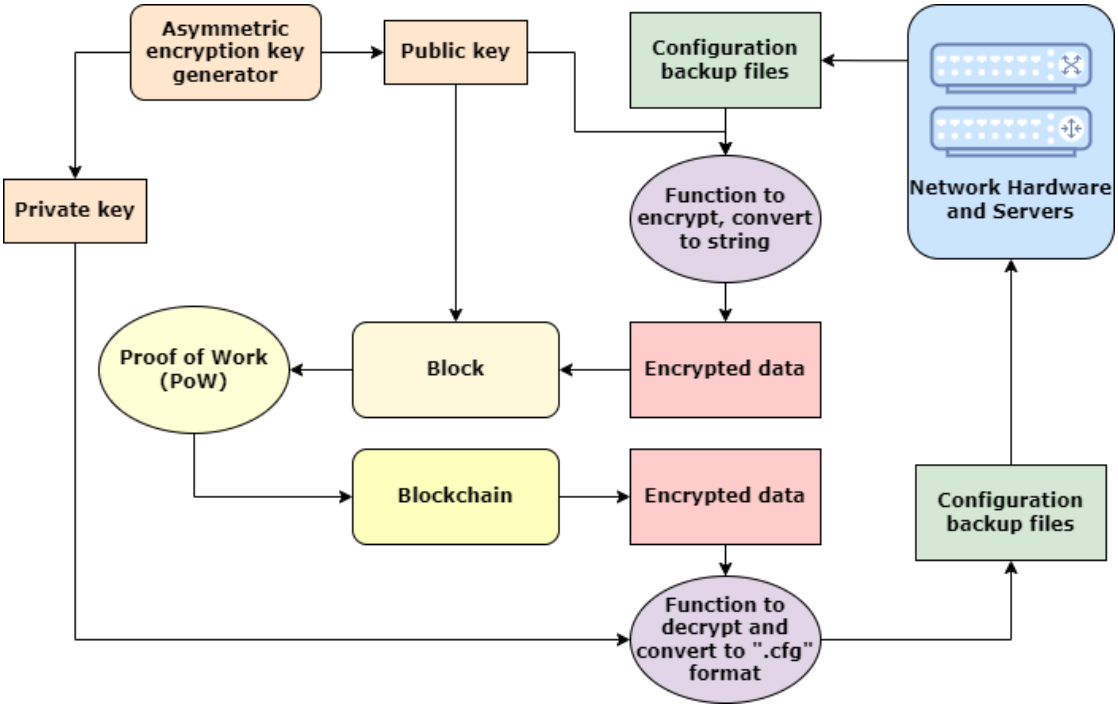

Figure 4.1 – Proposed Algorithm: Blockchain-based configuration file backup system

This particular network is graphically represented in figure 4.1, which depicts the intricate design and procedural flow of our suggested model. By embedding the backup files within a blockchain, it aspires to create an indelible and immutable record that significantly bolsters the security and fidelity of data.

At the foundation of envisioned architecture lies an unwavering commitment to securing data. It planned to encapsulate backup configurations from essential servers and network systems within a blockchain ledger designed to be alteration-proof. This ledger is envisioned to serve as a fortified repository, creating an enduring record that resists unauthorized changes, thus maintaining the integrity of the data within.

Proposed system's security is anchored by a cutting-edge asymmetric encryption scheme. This scheme generates cryptographic keys, with the public key being distributed for encrypting backup files and the private key remaining safeguarded for decryption. This approach to encryption is designed to ensure that data remains unintelligible to unauthorized entities, even in the event of interception during transmission.

The internal structure of blockchain is a pivotal component of the proposed system, as detailed in figure 4.2.

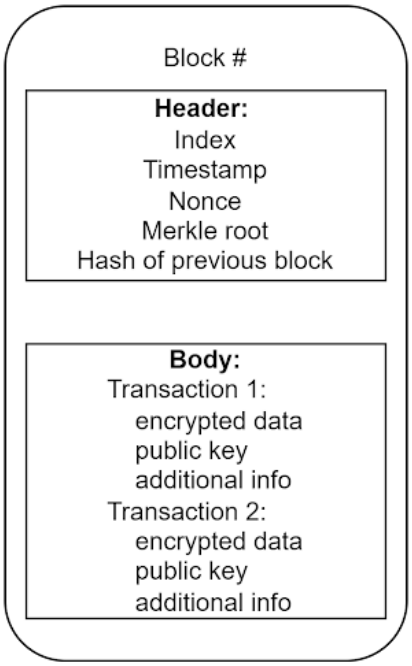

Figure 4.2 – Block structure in the blockchain

Each block is meticulously engineered to house:

- The header, which acts as a vessel for metadata integrity, comprising elements such as the block's identifier, a timestamp of creation, the nonce which is central to the mining process, the Merkle root summarizing the transactions, and the previous block's hash which secures the blockchain's lineage.

- The body, which functions as the vault for transactions. These transactions are not monetary exchanges but are the lifeblood of our system—the encrypted backup configuration files. Within each transaction, several critical fields are included:
  - Encrypted Data: This is the essence of the transaction, representing the configuration information in an encrypted state for secure transmission and storage.
  - Public Key: Serving multiple functions, the public key is employed both as the tool for encryption and as the identifier for the entity submitting the data to the blockchain.
  - Additional Information: This supporting information is vital for tracking the backup to its origin, pinpointing the specific network device that generated the data.

The blockchain's integrity and the authenticity of its transactions are reinforced by the implementation of a sophisticated Proof of Work (PoW) consensus protocol. This protocol is esteemed for its security assurance, mandating an intensive computational task to be concluded before a new block is appended to the chain. Beyond securing the network, it also promotes the distribution of control and safeguards against a plethora of cyber threats, including advanced ransomware onslaughts.

Nodes within the network each possess a synchronized version of the blockchain, which encompasses the encrypted backups. This distributed nature is designed to ensure that the integrity and accessibility of the data prevail, even if parts of the network are compromised.

The restoration process within the envisioned system is crafted with user experience in mind. Should there be a need to revert to a previous configuration or to recover from an incident, the encrypted data can be retrieved from the blockchain and decrypted with the private key. This process, which restores the data to a functional configuration format, is secure and ensures network administrators can expediently recover from disruptions, upholding business operations and reducing downtime.

The proposed system offers a robust solution to the challenges of safeguarding configuration backups. By combining the unalterable nature of blockchain technology with state-of-the-art encryption methods, was created a resilient structure for storing sensitive information. This strategic amalgamation of technologies presents a proactive approach to defending critical infrastructure from the dynamic realm of cyber threats. It ensures that network administrators maintain high operational integrity and swiftly recover from disturbances, rendering it an indispensable element of any organization's security strategy.

Chapter 5

Experiment and Results

This section presents a thorough experimental investigation into the newly proposed framework. This system leverages a bespoke private blockchain network to enhance the security and durability of network configuration backups for corporate infrastructures. The experiments were carefully designed and executed to evaluate the efficacy and practical applicability of the blockchain solution in resisting cyber threats, with a particular focus on mitigating the risks posed by ransomware attacks that jeopardize network stability and business continuity.

5.1 Experimental Cyber Range

For research purposes, a cyber testing ground with an emulation of a corporate test network was used. The experimental platform was an intricate network consisting of Cisco devices, chosen for their ubiquity in business settings.

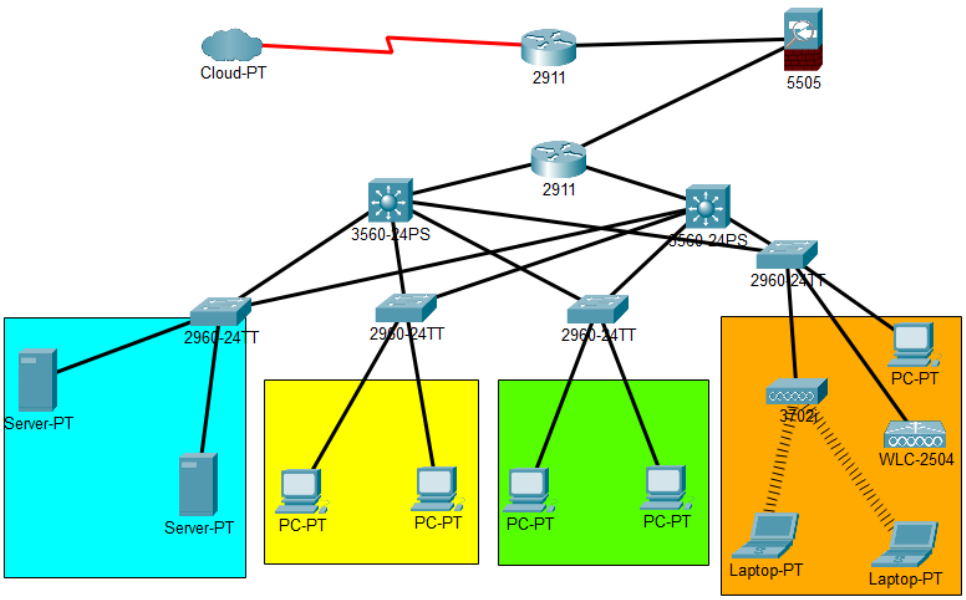

Figure 5.1 – Corporate test network

The network was composed of an ASA 5505 firewall, a Router 2111, Catalyst

3560 and 2960 switches, a CAP 3702 access point, and a WLC 2500 wireless LAN controller. Figure 5.1 illustrates this setup, which was designed to emulate a comprehensive corporate network, complete with essential networking features vital for an enterprise's day-to-day functions.

It introduces a range of networking protocols and services to mimic actual network conditions within the testbed. This included Inter-VLAN routing for cross-VLAN communications, FHRP protocols to ensure router redundancy and network reliability, default routing for traffic directed to unknown destinations, WLAN services for wireless needs, and AAA protocols to secure and manage user access and activity.

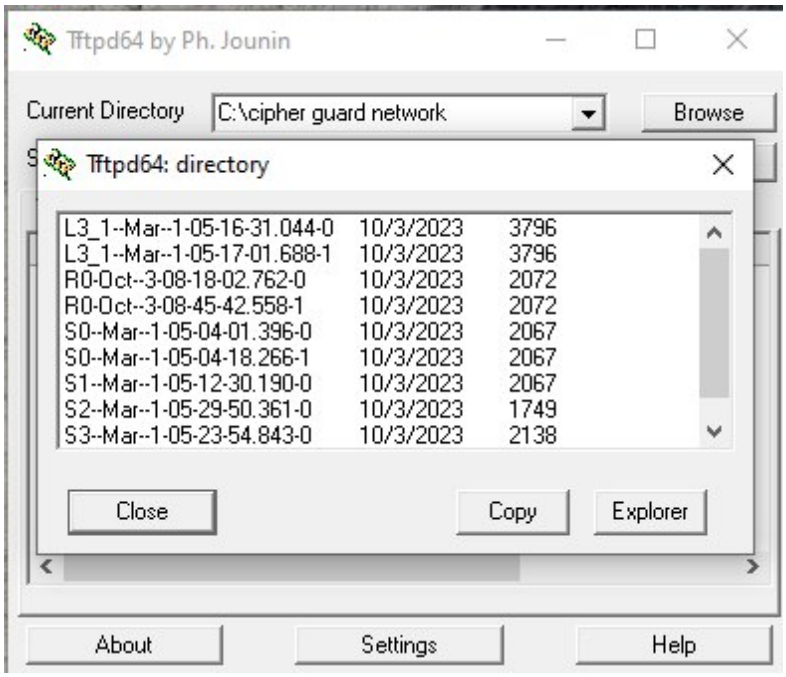

Figure 5.2 – Backup files on the TFTP server

A TFTP server was integrated to facilitate realistic backup scenarios, holding the configuration files for all devices within the network. This is essential for the swift restoration of network operations, as can be seen in figure 5.2, which demonstrates the process of storing backup configuration files on the TFTP server.

5.2 Ransomware - Proof of Concept (PoC)

During the experimental part of this study, a controlled environment was created to imitate a ransomware assault while inflicting no actual harm to real-world systems. This simulation was based on the Ransomware-Proof of Concept (PoC) open-source project. This project is well-documented and freely available for teaching purposes, and it gives a practical foundation for understanding the mechanics of a ransomware assault. All trials were carried out on isolated workstations to avoid the potential of unintended ransomware propagation or the leakage of simulated malicious activities to external systems.

The ransomware simulation begins with the Ransomware-PoC malware. The PoC was designed to start an encryption process with an AES key created internally by the malware. The encryption target was a local file, and the path was hardcoded within the PoC for the experiment's purposes. This file served as a placeholder for the victim's information. After encrypting the local file, the ransomware encrypts the generated AES key using an embedded RSA public key, which is also hardcoded in the PoC. This asymmetric encryption method assured that the AES key could only be decrypted using the accompanying RSA private key, which in this case was safely held on the attacker's command and control (C2) server (Figure 5.3).

Figure 5.3 – The result of an attack on the file

Following the encryption procedure, the ransomware simulates sending the encrypted AES key to the C2 server. This conduct imitated the traditional behavior of ransomware, in which the attacker must get the encryption key in order to perform a decryption service after the ransom is paid. After successfully encrypting the target file and transmitting the encrypted AES key, the Ransomware-PoC presented a ransom notice to the victim. This note alerted the simulated victim about the encryption and provided payment methods for regaining access to the encrypted file. To test the decryption procedure, the experiment imitated the victim paying the ransom. During this simulation, the C2 server sent the victim a decryptor and the RSA private key. This permitted the successful decryption of the AES key, resulting in the restoration of the encrypted file to its original condition as shown in figure 5.4

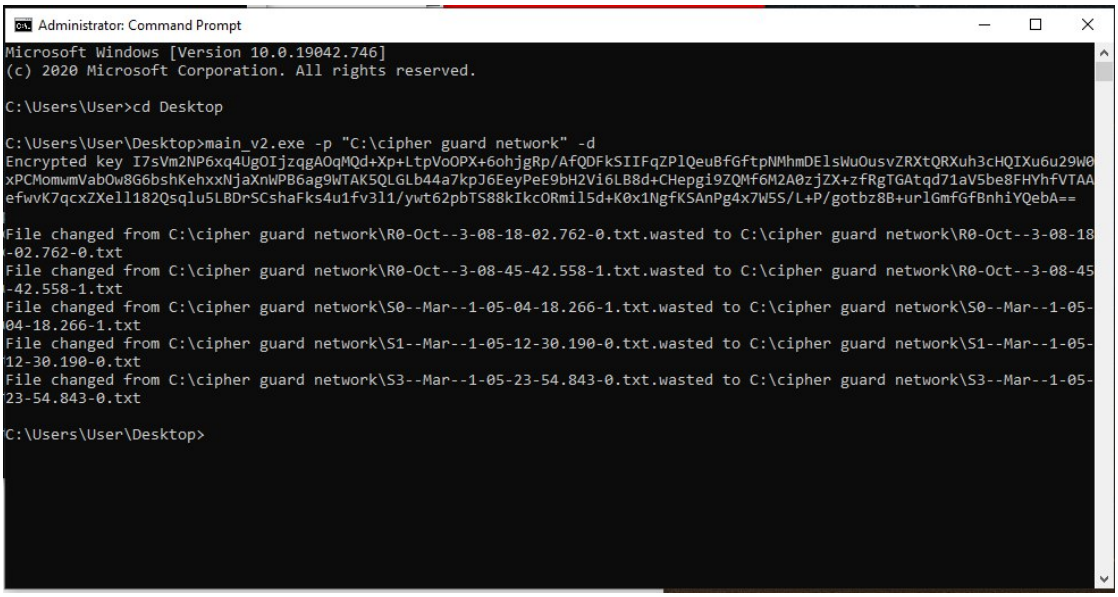

Figure 5.4 – Decryption of files

Throughout the trial, all activities were rigidly limited to the controlled environment. No actual ransom was paid, and no real data was jeopardized during the scenario. The major goal of the experiment was to learn without engaging in unethical behavior or inflicting harm. The results of these tests are intended to add significantly to the body of knowledge about ransomware attacks and to serve as a foundation for future study into the creation of security measures to avoid and minimize the impacts of such harmful actions.

5.3 Ransomware Attack to the Traditional Backup System

The analysis of the conventional backup system's vulnerabilities involved simulating a ransomware attack within a normally functioning network. The TFTP server, which served as the backup configuration repository, was compromised and the configuration files were encrypted.

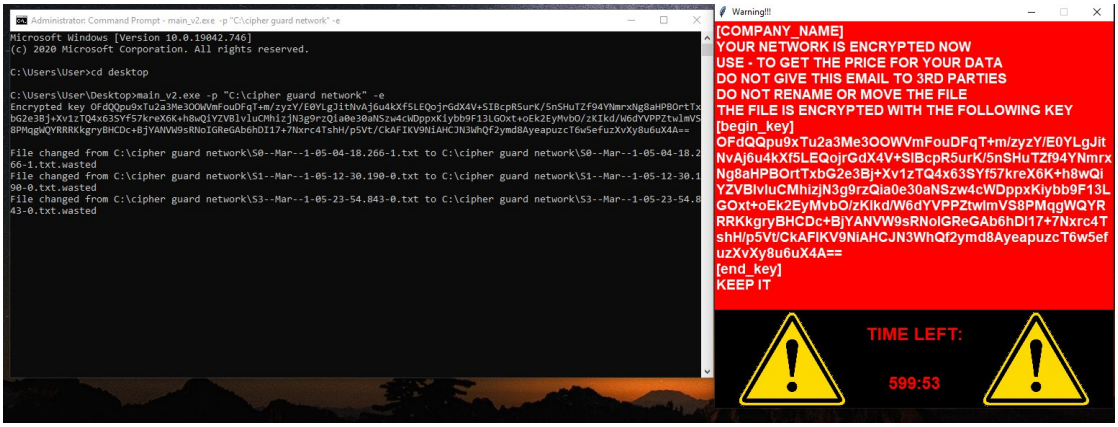

Figure 5.5 – The result of an attack on the TFTP backup server

This scenario is depicted in figure 5.5, showing the backup files as encrypted and highlighting the inherent weakness of traditional backup systems to cyber threats.

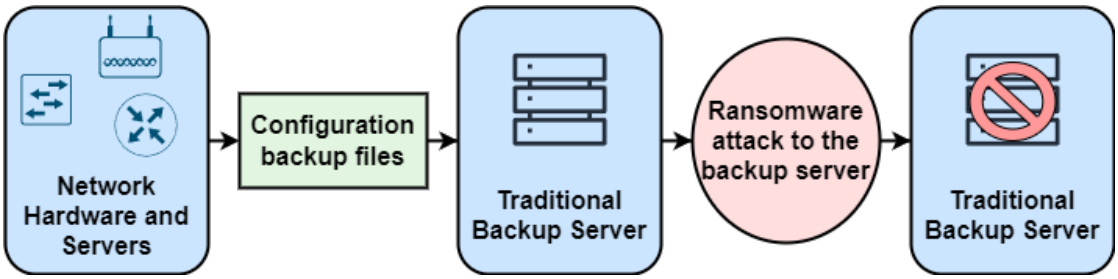

Figure 5.6 – Ransomware attack to backup server

Figure 5.6 further illustrates the consequences of the attack, emphasizing the encrypted state of the backup files and the vulnerability of standard backup strategies.

5.4 Integration of Blockchain to the Network

Following the ransomware attack on the traditional backup system, it was integrated a private blockchain into the corporate network. This integration aimed to leverage the blockchain's decentralized nature to safeguard backup configuration data.

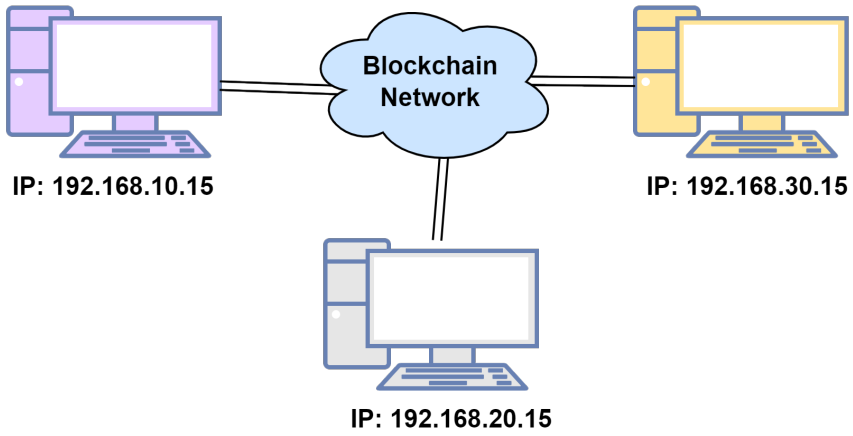

Figure 5.7 – Blockchain network nodes

As shown in figure 5.7, was added three blockchain nodes to the network, each hosted on separate servers with distinct IP addresses. This setup ensures network resilience by allowing network devices to retrieve backups from unaffected nodes in case one is compromised.

5.5 Ransomware Attack to the Blockchain-Based Backup System

It was rigorously tested the durability of the blockchain-integrated backup system by launching ransomware attacks on individual blockchain nodes. The blockchain's redundancy ensured that such attacks did not obliterate the backup configuration files. Figure 5.8 exhibits how the backups were preserved, allowing affected devices to recover using data from any intact node.

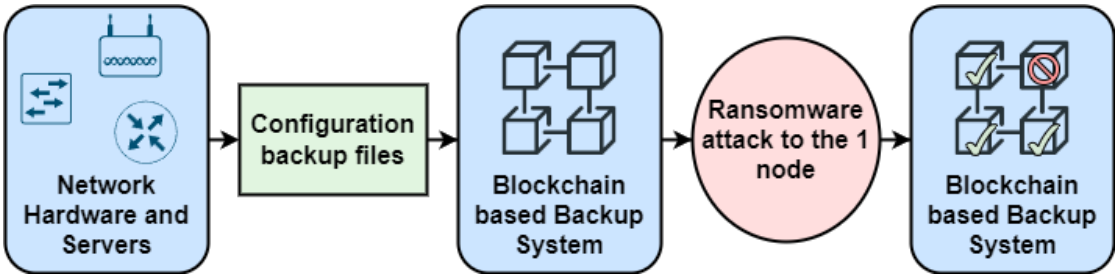

Figure 5.8 – Ransomware attack on Blockchain-based backup system

The experimental findings provide clear evidence of the superiority of the blockchain-based backup system over traditional methods in terms of security and robustness.

When the conventional backup system faced a ransomware attack, it led to the complete encryption of the backup files on the TFTP server, rendering them useless for recovery and exposing the network to extended downtime and potential operational failure.

Conversely, the blockchain-based backup system proved to be remarkably resilient against the same cyber threat. The distributed storage of backup data across various nodes meant that even if some were compromised, the backup information remained reachable. This resilience is intrinsic to the blockchain's architecture, which naturally incorporates redundancy across multiple sites, forestalling a total collapse from an attack on individual nodes.

The blockchain's distributed ledger technology ensures ongoing data availability and negates single points of failure. Each node functions independently, and the compromise of one due to ransomware doesn't equate to the loss of vital backup data. Hence, network operations can be restored quickly, curtailing the impact on business activities and maintaining operational integrity. Moreover, experiments underscore the urgent need to implement advanced security protocols in network architecture, particularly given the growing complexity of cyber threats. It is apparent that networks require backup systems that are not just secure, but also resilient against these evolving threats.

5.6 Evaluation of Performance

The performance of the proposed system was rigorously evaluated to ensure its efficiency and effectiveness. The system was developed using Python and integrated with the React framework to create an interactive and responsive user experience. For the purpose of this evaluation, a benchmark test was conducted on a PC equipped with an Intel(R) Core(TM) i5-10400 CPU operating at 2.90GHz, complemented by 8.00 GB of RAM.

The methodology involved executing each of the five key functions of the system 100 times to obtain a reliable average execution time. These times were meticulously recorded and are presented in Table 5.1. The test utilized a lightweight evaluation file, merely 4KB in size, to minimize any extraneous variables impacting the assessment. It is important to note that certain functions, such as encryption and file upload, as well as file decoding and downloading, were performed concurrently. Consequently, the execution time for these functions was shared, thereby optimizing the overall performance.

Table 5.1 – Average execution time of each function

Proposed Algorithm/Function	Execution time (sec.)
Public & private key generation	0.04645305395
Encryption File Upload	0.009359333515
Adding transaction	0.009866755009
Mining	0.004110248089
Decode file Download	0.04418283701

The performance evaluation was not limited to execution times alone. It also included a comparative analysis with existing blockchain backup solutions, as detailed in Table 5.2. The proposed blockchain-based configuration backup system demonstrated superior performance across several metrics. Specifically, when compared to BlockIPFS, our file uploading process, inclusive of the encryption routine, was 21,854 times faster. Similarly, our file loading operation outpaced the competition by a factor of 1,3127, while also accounting for the time taken by the decoding process.

Table 5.2 – Comparison of the functions of blockchain-based file backup systems

<table>
<tr><th>Algorithm/Function</th><th>This Work</th><th>[25]</th><th>[42]</th><th>[35]</th><th>[39]</th><th>[33]</th></tr>
<tr><td>Encryption</td><td rowspan="2">0.009s</td><td></td><td rowspan="2">0.59s</td><td></td><td></td><td></td></tr>
<tr><td>File Upload</td><td rowspan="3">0.05s</td><td rowspan="3">42s</td><td rowspan="3">12s</td><td></td></tr>
<tr><td>Adding transaction</td><td>0.01s</td><td rowspan="2">18.55s</td><td rowspan="2">0.013s</td></tr>
<tr><td>Mining</td><td>0.004s</td></tr>
<tr><td>Decode file</td><td rowspan="2">0.044s</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Download</td><td>0.06s</td><td></td><td>0.9s</td><td></td><td></td></tr>
</table>

In the context of countering Indonesian hoax news datasets, the proposed system leveraged blockchain, IPFS, and a voting mechanism to expedite file uploads by 62.93 times, and to accelerate the addition of transactions and mining by 1,327 times compared to the baseline.

When benchmarked against a conventional blockchain-based platform for data storage in the cloud, our system's transaction, mining, and file decoding processes were approximately 2,000 times quicker. This remarkable speed is also a function of our system's ability to encrypt files, a feature not present in the traditional cloud storage system.

Moreover, the system's efficiency in processing transactions and mining via IPFS and a Private Blockchain was found to be 513.79 times faster than the alternative solutions. Even when compared to blockchain-based digital diploma verification and distribution schemes, which do not involve decoding, our method processed transactions 35.88 times more swiftly.

In summary, the performance evaluation of the system demonstrated not only its robustness and speed but also its ability to significantly outperform existing solutions in various key operations. These findings underscore the potential of the proposed system to revolutionize the efficiency of blockchain-based data handling processes.

Chapter 6

Conclusion and future works

6.1 Conclusion

The relentless surge of cyberattacks, particularly those involving ransomware, has made it clear that traditional security measures are no longer sufficient in isolating and safeguarding our digital ecosystems. The research presented herein heralds a groundbreaking development in the form of a blockchain-centric backup mechanism tailored for computer networks. The empirical evidence gathered from a carefully orchestrated simulation utilizing a network of Cisco devices, alongside a TFTP server designated for backup operations, stands as a robust testament to the potential of this innovative approach in bolstering network security.

By incorporating the principles of blockchain technology, characterized by distributed processing and an immutable record-keeping system, the proposed solution has demonstrated a superior capability in the secure management and restoration of configuration files. This triumph in technological advancement is particularly poignant in the context of ransomware deflection, offering a level of data protection that was previously unattainable.

A key observation arising from this investigation is the system's proficiency in the seamless and protected dissemination of backup data throughout the network's nodes. This feature alone bears significant strategic value, offering a blueprint for how organizations might evolve their strategies for data replication and emergency recovery. The swift recovery of unaltered backups from secure nodes in the aftermath of a cyber incursion does not merely reduce the threat of data compromise; it also curtails operational interruptions and the associated economic repercussions that could debilitate an organization.

Furthermore, the sterling performance of the blockchain-inspired system in controlled testing scenarios illuminates its potential adaptability across various verticals. As industries around the world are inexorably tethered to sophisticated network systems for their day-to-day functions, the demand for versatile and dependable backup solutions is omnipresent. This system's flexibility to integrate with different network configurations and its scalability suggests that it could emerge as a fundamental safeguard, poised to secure vital electronic assets across diverse sectors including, but not limited to, healthcare, finance, governance, and academia.

To encapsulate, the empirical validation of this blockchain-based backup system within a simulated network setting is an affirmation of the transformative power of forward-thinking security solutions in the digital age. As we navigate an epoch increasingly defined by digital interactions and service delivery, the imperative for dynamic and resilient protective mechanisms is undeniably critical. The insights derived from this study not only underscore the efficacy of the system at hand but also illuminate the pathway for ongoing investigative efforts aimed at the cultivation of increasingly sophisticated and enduring cybersecurity infrastructures. It is through such unwavering dedication to advancing security paradigms that we can aspire to safeguard the structural integrity and dependability of our digitally interconnected society.

6.2 Future works

The promising results of this study lay the groundwork for a plethora of future research endeavors. An essential avenue for exploration involves adapting the blockchain-based backup system to cater to the unique security needs of critical sectors such as banking and diverse cloud service models like Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS). This expansion of the system's applicability promises to enhance data security across a broader spectrum of industry domains.

Delving into alternative consensus algorithms represents another pivotal area for future investigations, as different mechanisms may offer distinct advantages in terms of security, speed, and scalability. Exploring novel consensus protocols and evaluating their impact on the system's performance could lead to refinements that boost overall efficiency and resilience in the face of evolving cyber threats.

Integration with established public blockchain networks like Ethereum presents an exciting opportunity to bolster the system's security posture and enhance its transparency. Leveraging the capabilities of public blockchains can facilitate interoperability, data integrity, and decentralization, further fortifying the system's resilience against sophisticated attacks.

Conducting real-world assessments will be vital for future research, facilitating a comprehensive evaluation of the system's performance metrics and practical implications across varied operational environments. This empirical validation in diverse real-world settings will provide invaluable insights into the system's scalability, adaptability, and effectiveness in mitigating cyber risks in practical scenarios.

Furthermore, exploring the behavioral and psychological dimensions of network security, particularly how the incorporation of blockchain technology influences user behavior and organizational security culture, could yield valuable insights into optimizing the system's usability and effectiveness within human-operated environments. Understanding the human factors at play in cybersecurity can inform the design of user-centric security measures and enhance overall system resilience.

In summation, this research not only signifies a significant leap forward in network security but also heralds a new era of innovation and resilience in the face of evolving cyber threats. The road ahead teems with opportunities for further

advancements, empowering us to fortify our defenses and safeguard the integrity of our network-dependent society through continuous research and innovation in blockchain-based security solutions.

Bibliography

[1] Tim Reed. No excuses: Prioritizing security for mission-critical technology, Oct 2023. URL https://www.forbes.com/sites/forbestechcouncil/2023/10/30/no-excuses-prioritizing-security-for-mission-critical-technology/?sh=2467280f4cea.

[2] Xiaoping Wang, Akhtar Badshah, Shanshan Tu, and Muhammad Waqas. Blockchain-based security management platform. In *2021 2nd Asia Symposium on Signal Processing (ASSP)*, pages 118–121, 2021. doi: 10.1109/ASSP54407.2021.00026.

[3] Usman Javed Butt, Maysam Abbod, Anzor Lors, Hamid Jahankhani, Arshad Jamal, and Arvind Kumar. Ransomware threat and its impact on scada. In *2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3)*, pages 205–212, 2019. doi: 10.1109/ICGS3.2019.8688327.

[4] Ahsan Siddiqui. The importance of keeping backup data safe from cybercriminals, Jan 2023. URL https://www.securitymagazine.com/articles/98823-the-importance-of-keeping-backup-data-safe-from-cybercriminals.

[5] Nikhil Sharma and Ravi Shanker. Analysis of ransomware attack and their countermeasures: A review. In *2022 International Conference on Electronics and Renewable Systems (ICEARS)*, pages 1877–1883, 2022. doi: 10.1109/ICEARS53579.2022.9751949.

[6] Weilun Lao, Zhuozhuo Chen, Birou Gao, Jiabei Wang, Yang Tao, and Rui Zhang. Rap: Ransomware protection scheme based on blockchain. In *2022 2nd International Conference on Consumer Electronics and Computer Engineering (ICCECE)*, pages 13–20, 2022. doi: 10.1109/ICCECE54139.2022.9712682.

[7] A. Hobbs. *The Colonial Pipeline Hack: Exposing Vulnerabilities in U.S. Cybersecurity*. SAGE business cases. SAGE Publications, 2021. ISBN 9781529789768. URL https://books.google.kz/books?id=USuTzgEACAAJ.

[8] Eduardo Berrueta, Daniel Morato, Eduardo Magaña, and Mikel Izal. Ransomware encrypted your files but you restored them from network traffic. In *2018 2nd Cyber Security in Networking Conference (CSNet)*, pages 1–7, 2018. doi: 10.1109/CSNET.2018.8602978.

[9] Noor Thamer and Raaid Alubady. A survey of ransomware attacks for health-

care systems: Risks, challenges, solutions and opportunity of research. In *2021 1st Babylon International Conference on Information Technology and Science (BICITS)*, pages 210–216, 2021. doi: 10.1109/BICITS51482.2021.9509877.

[10] Donghyun Min, Donggyu Park, Jinwoo Ahn, Ryan Walker, Junghee Lee, Sungyong Park, and Youngjae Kim. Amoeba: An autonomous backup and recovery ssd for ransomware attack defense. *IEEE Computer Architecture Letters*, 17(2):245–248, 2018. doi: 10.1109/LCA.2018.2883431.

[11] W. Curtis Preston. Ransomware: It's coming for your backup servers, Dec 2022. URL https://www.networkworld.com/article/3682659/ransomware-it-s-coming-for-your-backup-servers.html.

[12] David Finger. Priorities in preparing for a ransomware attack: People, processes, and technology, Jun 2023. URL https://www.fortinet.com/blog/ciso-collective/ransomware-attack-priorities-in-preparation.

[13] Jeffrey Schwartz. Survey: Backups are prime targets for ransomware attacks, most remain exposed, May 2023. URL https://www.channelfutures.com/security/survey-backups-are-prime-targets-for-ransomware-attacks-most-remain-exposed.

[14] Savita Mohurle and Manisha Patil. A brief study of wannacry threat: Ransomware attack 2017. *International journal of advanced research in computer science*, 8(5):1938–1940, 2017.

[15] Ridho Surya Kusuma, Rusydi Umar, and Imam Riadi. Network forensics against ryuk ransomware using trigger, acquire, analysis, report, and action (taara) method. *Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control*, 2021.

[16] Ondřej Filipec and D Plasil. The cybersecurity of healthcare the case of the benegov hospital hit by ryuk ransomware, and lessons learned. *Obrana a Strategie-Defence & Strategy*, pages 27–51, 2021.

[17] Mary K. Pratt. The 10 biggest ransomware attacks in history, Sep 2023. URL https://www.techtarget.com/searchsecurity/tip/The-biggest-ransomware-attacks-in-history.

[18] James Nivedita. 10 of the biggest ransomware attacks in history, Feb 2023. URL https://www.getastra.com/blog/security-audit/biggest-ransomware-attacks/.

[19] Donghyun Min, Yungwoo Ko, Ryan Walker, Junghee Lee, and Youngjae Kim. A content-based ransomware detection and backup solid-state drive for ransomware defense. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 41(7):2038–2051, 2022. doi: 10.1109/TCAD.2021.3099084.

[20] Yong Jin, Masahiko Tomoishi, Satoshi Matsuura, and Yoshiaki Kitaguchi. A secure container-based backup mechanism to survive destructive ransomware attacks. In *2018 International Conference on Computing, Networking and*

Communications (ICNC), pages 1–6, 2018. doi: 10.1109/ICCNC.2018.8390376.

[21] Vaclav Oujezsky, Pavel Novak, Tomas Horvath, Martin Holik, and Michal Jurcik. Data backup system with integrated active protection against ransomware. In *2023 46th International Conference on Telecommunications and Signal Processing (TSP)*, pages 65–69, 2023. doi: 10.1109/TSP59544.2023.10197687.

[22] Jianping Zhang and Hongmin Li. Research and implementation of a data backup and recovery system for important business areas. In *2017 9th International Conference on Intelligent Human-Machine Systems and Cybernetics (IHMSC)*, volume 2, pages 432–437, 2017. doi: 10.1109/IHMSC.2017.209.

[23] Almountassir Bellah Balhasan, Ibrahim A.M. Alkasih, Wagdi Saad Sallabi, Moftah B.M. Bokhatwa, Adrees Saeid Bilhasan, and Salem Ali Alhuni. A case study on the information security system of al wahda bank. In *2022 International Conference on Electrical and Computing Technologies and Applications (ICECTA)*, pages 196–200, 2022. doi: 10.1109/ICECTA57148.2022.9990540.

[24] Wuqiang Shen, Jinbo Zhang, Zhenyue Long, Lei Cui, and Zheheng Liang. Balanced computing server data security storage system based on blockchain. In *2022 4th International Academic Exchange Conference on Science and Technology Innovation (IAECST)*, pages 707–710, 2022. doi: 10.1109/IAECST57965.2022.10062076.

[25] Emmanuel Nyaletey, Reza M. Parizi, Qi Zhang, and Kim-Kwang Raymond Choo. Blockipfs - blockchain-enabled interplanetary file system for forensic and trusted data traceability. In *2019 IEEE International Conference on Blockchain (Blockchain)*, pages 18–25, 2019. doi: 10.1109/Blockchain.2019.00012.

[26] Randhir Kumar and Rakesh Tripathi. Implementation of distributed file storage and access framework using ipfs and blockchain. In *2019 Fifth International Conference on Image Information Processing (ICIIP)*, pages 246–251, 2019. doi: 10.1109/ICIIP47207.2019.8985677.

[27] Md. Nasim Uddin, Abu Hayat Mohammed Abul Hasnat, Shamima Nasrin, Md. Shahinur Alam, and Mohammad Abu Yousuf. Secure file sharing system using blockchain, ipfs and pki technologies. In *2021 5th International Conference on Electrical Information and Communication Technology (EICT)*, pages 1–5, 2021. doi: 10.1109/EICT54103.2021.9733608.

[28] Jia Kan and Kyeong Soo Kim. Mtfs: Merkle-tree-based file system, 2019.

[29] Aisyah Ismail, Mark Toohey, Young Choon Lee, Zhongli Dong, and Albert Y. Zomaya. Cost and performance analysis on decentralized file systems for blockchain-based applications: State-of-the-art report. In *2022 IEEE International Conference on Blockchain (Blockchain)*, pages 230–237, 2022. doi: 10.1109/Blockchain55522.2022.00039.

[30] Jyotsna Anthal, Shakir Choudhary, and Ravikumar Shettiyar. Decentralizing file sharing: The potential of blockchain and ipfs. In *2023 International Conference on Advancement in Computation & Computer Technologies (InCACCT)*, pages 773–777, 2023. doi: 10.1109/InCACCT57535.2023.10141817.

[31] S D Ashwini, Annapurna P Patil, and Savita K Shetty. Moving towards blockchain-based solution for ensuring secure storage of medical images. In *2021 IEEE 18th India Council International Conference (INDICON)*, pages 1–5, 2021. doi: 10.1109/INDICON52576.2021.9691516.

[32] Kai-Wei Lin and Yu-Chi Chen. A file verification scheme based on verkle trees. In *2023 International Conference on Consumer Electronics - Taiwan (ICCE-Taiwan)*, pages 295–296, 2023. doi: 10.1109/ICCE-Taiwan58799.2023.10226788.

[33] Rupsingh Mathwale and Ramarao Ramisetty. Blockchain based inter-organizational secure file sharing system. In *2023 2nd International Conference for Innovation in Technology (INOCON)*, pages 1–5, 2023. doi: 10.1109/INOCON57975.2023.10101350.

[34] Pearl Alisha Lobo and V Sarasvathi. Distributed file storage model using ipfs and blockchain. In *2021 2nd Global Conference for Advancement in Technology (GCAT)*, pages 1–6, 2021. doi: 10.1109/GCAT52182.2021.9587537.

[35] Thomas Renner, Johannes Müller, and Odej Kao. Endolith: A blockchain-based framework to enhance data retention in cloud storages. In *2018 26th Euromicro International Conference on Parallel, Distributed and Network-based Processing (PDP)*, pages 627–634, 2018. doi: 10.1109/PDP2018.2018.00105.

[36] Osama Sam Abuomar and Rebecca Yale Gross. Using blockchain, raid, & bittorrent technologies to secure digital evidence from ransomware. In *2023 IEEE International Conference on Electro Information Technology (eIT)*, pages 001–006, 2023. doi: 10.1109/eIT57321.2023.10187306.

[37] Wei Cai and Jian Qu. Systematic research on information security based on blockchain technology. In *2022 International Conference on Electronics and Renewable Systems (ICEARS)*, pages 900–903, 2022. doi: 10.1109/ICEARS53579.2022.9751814.

[38] Ke Yang, Hui-min Liao, Li-hua Zhao, Shang-zhuo Zheng, and Hong-wei Li. Research on network security protection technology of energy industry based on blockchain. In *2020 IEEE/CIC International Conference on Communications in China (ICCC Workshops)*, pages 162–166, 2020. doi: 10.1109/ICCCWorkshops49972.2020.9209919.

[39] Saha Reno, Shovan Bhowmik, and Mamun Ahmed. Utilizing ipfs and private blockchain to secure forensic information. In *2021 International Conference on Automation, Control and Mechatronics for Industry 4.0 (ACMI)*, pages 1–6, 2021. doi: 10.1109/ACMI53878.2021.9528180.

[40] Noor Thamer and Raaid Alubady. Security against ransomware attack in medical healthcare records using blockchain technology. In *2022 Fifth College of Science International Conference of Recent Trends in Information Technology (CSCTIT)*, pages 111–117, 2022. doi: 10.1109/CSCTIT56299.2022.10145717.

[41] Mohammad Wazid, Ashok Kumar Das, and Sachin Shetty. Bsfr-sh: Blockchain-enabled security framework against ransomware attacks for smart healthcare. *IEEE Transactions on Consumer Electronics*, 69(1):18–28, 2023. doi: 10.1109/TCE.2022.3208795.

[42] Akhmad Rizal Arifudin, Ray Novita Yasa, and Girinoto. Securing indonesian hoax news dataset with blockchain, ipfs, and voting mechanism. In *2023 3rd International Conference on Electronic and Electrical Engineering and Intelligent System (ICE3IS)*, pages 104–109, 2023. doi: 10.1109/ICE3IS59323.2023.10335318.

[43] Bin Liu, Yang Xin, and Suhuan Dai. Blockchain-based disaster recovery data storage and security auditing solution in multi-cloud environment. In *2022 International Applied Computational Electromagnetics Society Symposium (ACES-China)*, pages 1–4, 2022. doi: 10.1109/ACES-China56081.2022.10065296.

[44] Jinqian Chen, Yong Yan, Shaoyong Guo, Yinlin Ren, and Feng Qi. A system for trusted recovery of data based on blockchain and coding techniques. *Wireless Communications and Mobile Computing*, 2022:1–12, January 2022. doi: 10.1155/2022/8390241. URL https://doi.org/10.1155/2022/8390241.

[45] S K Mouleeswaran, R Aruna, J Visumathi, and S Gurusubramani. Secure cloud backup for data sources based on blockchain. *Journal of Physics: Conference Series*, 1964(4):042062, July 2021. doi: 10.1088/1742-6596/1964/4/042062. URL https://doi.org/10.1088/1742-6596/1964/4/042062.

[46] Badr Aleidi, Abdulaziz A. Albesher, and Mousa T. Al-Akhras. Using blockchain technology to validate the integrity and confidentiality of backup versions on the cloud. In *2018 Al Yamamah Forum on Telecommunications and Information Technology*, 2018. URL https://api.semanticscholar.org/CorpusID:51762037.

[47] Strahil Sokolov, Stefan Vlaev, and Teodor B. Iliev. Technique for improvement of backup and restore strategy based on blockchain. In *2022 International Conference on Communications, Information, Electronic and Energy Systems (CIEES)*, pages 1–6, 2022. doi: 10.1109/CIEES55704.2022.9990781.

[48] Remya Stephen and Aneena Alex. A review on blockchain security. In *IOP conference series: materials science and engineering*, volume 396, page 012030. IOP Publishing, 2018.

[49] Liang Liu and Budong Xu. Research on information security technology based on blockchain. In *2018 IEEE 3rd International Conference on Cloud Computing and Big Data Analysis (ICCCBDA)*, pages 380–384, 2018. doi: 10.1109/ICCCBDA.2018.8386546.

[50] Henry Rossi Andrian, Novianto Budi Kurniawan, and Suhardi. Blockchain technology and implementation : A systematic literature review. In *2018 International Conference on Information Technology Systems and Innovation (ICITSI)*, pages 370–374, 2018. doi: 10.1109/ICITSI.2018.8695939.

[51] P Paul, PS Aithal, Ricardo Saavedra, and Surajit Ghosh. Blockchain technology and its types—a short review. *International Journal of Applied Science and Engineering (IJASE)*, 9(2):189–200, 2021.

[52] Neetu Verma, Saurabh Jain, and Rajesh Doriya. Review on consensus protocols for blockchain. In *2021 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS)*, pages 281–286, 2021. doi: 10.1109/ICCCIS51004.2021.9397089.

[53] Luke Conway. What is bitcoin halving? definition, how it works, why it matters, Apr 2024. URL https://www.investopedia.com/bitcoin-halving-4843769.

[54] Harrison Miller. Bitcoin price retreats. is the halving already priced in?, Apr 2024. URL https://www.investors.com/news/bitcoin-halving-priced-in-miners/.

[55] Joshua A Kroll, Ian C Davey, and Edward W Felten. The economics of bitcoin mining, or bitcoin in the presence of adversaries. In *Proceedings of WEIS*, volume 2013. Citeseer, 2013.

[56] Mohamed Fartitchou, Hanaa El Marraki, Lamyae Lafkir, Anissa Azzouz, Khalid El Makkaoui, and Zakaria El Allali. Public-key cryptography behind blockchain security. In *2022 5th International Conference on Networking, Information Systems and Security: Envisage Intelligent Systems in 5g//6G-based Interconnected Digital Worlds (NISS)*, pages 1–5, 2022. doi: 10.1109/NISS55057.2022.10085236.

[57] Sana Sabah Sabry, Nada Mahdi Kaittan, and Israa Majeed. The road to the blockchain technology: Concept and types. *Periodicals of Engineering and Natural Sciences*, 7(4):1821–1832, 2019.

[58] Sanjay Kumar, Binod Kumar Singh, Akshita, Sonika Pundir, Simran Batra, and Rashi Joshi. A survey on symmetric and asymmetric key based image encryption. In *2nd International Conference on Data, Engineering and Applications (IDEA)*, pages 1–5, 2020. doi: 10.1109/IDEA49133.2020.9170703.