International Journal of Cyber and IT Service Management (IJCITSM) p-ISSN: 2797-1325
Vol. 3 No. 2 October 2023 e-ISSN: 2808-554X

Enhancing Cybersecurity Information Sharing: A Secure and Decentralized Approach with Four-Node IPFS

Zaleha Fauziah[1], Novi Putri Anggraini[2], Yulia Putri Ayu Sanjaya[3], Tarisya Ramadhan[4]
Communication Studies[1,2], Retail Management[3], Information System[4]
Manipal International University[1,2], University of Raharja[3,4]
No 1, MIU Boulevard, Putra Value, 71800 Value, Negeri Sembilan[1,2], Modern, Jl. Jenderal Sudirman No.40, Cikokol, Kec. Tangerang, Tangerang City, Banten 15117[3,4]
Malaysia[1,2], Indonesia[3,4]
e-mail: zalehafauziah@yahoo.com[1], nanggraeni820@gmail.com[2], yulia.putri@raharja.info[3], tarisya@raharja.info[4]

Author Notification
12 October 2023
Final Revised
29 October 2023
Published
31 October 2023

To cite this document:
Fauziah, Z., Anggraini, N. P., Ayu Sanjaya, Y. P., & Ramadhan, T. . (2023). Enhancing Cybersecurity Information Sharing: A Secure and Decentralized Approach with Four-Node IPFS. *International Journal of Cyber and IT Service Management, 3(2), 153–159. Retrieved from https://iiast.iaic-publisher.org/ijcitsm/index.php/IJCITSM/article/view/139*

DOI:
https://doi.org/10.34306/ijcitsm.v3i2.139

Abstract

The act of sharing cybersecurity information plays a proactive and collaborative role in bolstering organizational security through the exchange of data using a centralized repository service. However, the real-world application of centralized services comes with certain risks. It leaves organizations vulnerable to distributed denial-of-service (DDoS) attacks, leading to system failures and creating a single point of failure. Additionally, it opens the door to man-in-the-middle (MITM) attacks, potentially altering or pilfering exchanged information. These threats undermine user confidence in the confidentiality, integrity, and availability of their data. This study presents a secure solution, the design of a Cybersecurity Information Sharing (CyberShare) system that employs a private interplanetary file system (IPFS) network as a decentralized information storage solution. Unlike centralized storage, which relies on a single node, the CyberShare system utilizes a four-node IPFS network interconnected with swarm keys for authentication. This design enables users to store and share information securely from sender to recipient, eliminating the need for reliance on a central server and reducing the server load. An analysis of the proposed CyberShare system demonstrates its capability to ensure the confidentiality, integrity, and availability of cybersecurity information. By enhancing information security, CyberShare systems empower organizations to securely share and utilize cybersecurity data.

Keywords*: Cybersecurity, InterPlanetary File System, CyberShare*

1. Introduction

After the global outbreak of the COVID-19 pandemic, the frequency of cyberattacks has been on the rise. This underscores the insufficiency of relying solely on technological cybersecurity measures to protect organizations from sophisticated cyber threats [1]. Therefore, a need arises for proactive security techniques aimed at preventing and detecting cyberattacks at an early stage. These techniques involve more advanced security technologies and processes oriented toward preventing and early detection of cyber threats, rather than merely

responding after an attack has occurred. One effective approach involves the sharing of cybersecurity information, which can originate from within or outside an organization[2].

Internally, sharing cybersecurity information within an organization can help stakeholders make informed decisions regarding defense techniques, detection, strategies, and threat mitigation[3]. Stakeholders who receive this information can subsequently utilize it to enhance their organization's security, extending protection to other stakeholders by preventing the spread of cyber threats. The implementation of cybersecurity information sharing often relies on centralized storage, which is the most common information storage model used across various organizations. Centralized storage offers efficiency and streamlined information management, facilitating rapid data storage and retrieval[4]. However, this model comes with vulnerabilities, such as susceptibility to distributed denial-of-service (DDoS) attacks that can lead to system failures and single points of failure. Another concern is Man in The Middle (MITM) attacks on the transmission of cybersecurity information, resulting in unauthorized entities intercepting and leaking this data. These entities can compromise data integrity by altering information, which is then forwarded to the recipient, who receives the modified data. Therefore, there is a need for distributed and decentralized storage technologies that ensure data confidentiality, integrity, and availability[5].

The InterPlanetary File System (IPFS) is a peer-to-peer (P2P) network protocol that allows users to store and access information in a decentralized fashion, reducing reliance on central servers and alleviating server load. IPFS operates through a decentralized distribution system, enabling file storage across multiple nodes for secure and rapid access. Each file is uniquely identified by a hash and can be retrieved from any node within the network. In the IPFS network, all nodes are of equal significance and have the capability to store and retrieve data. The benefits of utilizing IPFS encompass heightened security, as files are not concentrated in a single location and cannot be deleted by specific entities. Furthermore, IPFS facilitates swifter file transfers by allowing retrieval from the nearest node. It also accommodates different file versions, granting users access to both historical and current iterations of the same file[6].

Hence, this research proposes the design of a secure Cybersecurity Information Sharing (CyberShare) system that utilizes a private IPFS network with four nodes for decentralized file storage[7]. The analysis results demonstrate that the CyberShare system can ensure the availability, integrity, and confidentiality of cybersecurity information, allowing organizations to securely share and leverage this information.

2. Related Research

Previous research has explored proposals for sharing cybersecurity incident information with a primary focus on safeguarding sensitive information shared among sectoral organizations through centralized storage[8]. Furthermore, prior studies have examined proposals for government information sharing schemes to promote cross-departmental collaboration, employing blockchain technology. There has also been previous research concerning information sharing models among governments utilizing blockchain technology. Additionally, there has been research concentrating on cybersecurity collaboration, involving cybersecurity operational activity models and intelligence threat sharing maturity models among sectoral organizations[9].

In previous research, the sharing of cybersecurity information was carried out through a peer-to-peer (P2P) communication model via centralized storage services due to its flexibility and convenience for involved government entities[10]. Centralized services encompass various features, including cloud storage. However, in practice, centralized storage for implementing cybersecurity information sharing has introduced several threats that could impact the components forming an organization's infrastructure, such as its networks and communication systems. Centralized storage management systems involve central authorities controlling a significant volume of information, leading to user distrust regarding the confidentiality, integrity, and availability of data[11].

Given the prior research related to the security threats of information sharing through centralized services in the realm of cybersecurity, it becomes imperative to advance research in the field of cybersecurity information sharing using secure decentralized services[12]. These decentralized services must be capable of ensuring information availability, integrity, and

confidentiality. In this context, there is a need to analyze the security factors of decentralized information sharing systems. Consequently, further research is expected to yield solutions that fulfill the security requirements for implementing cybersecurity information sharing[13].

3. Research Methods

The stages employed in this research include the following: problem identification, goal description, literature review, system design, testing and analysis, and conclusion drawing. The research stages are illustrated in Figure 1 and detailed as follows:

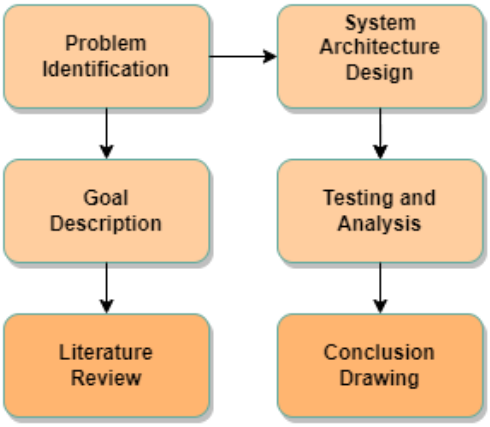

Figure 1. Research stage

3.1 Problem Identification

In this phase, issues motivating the research are identified. The problem relates to the utilization of Cybersecurity Information Sharing (CIS) with centralized storage in organizations. However, in practice, centralized storage in the implementation of CIS is vulnerable to distributed denial-of-service (DDoS) attacks, which can result in a single point of failure, and Man in The Middle (MITM) attacks, leading to information modification. These attacks lead to user distrust regarding the confidentiality, integrity, and availability of information[14].

3.2 Goal Description

In this research, the objective is to develop a secure cybersecurity information sharing system to ensure the confidentiality, integrity, and availability of information. This system is designed using a private Interplanetary File System (IPFS) network to guarantee the security of cybersecurity information. The research aims to provide a solution that can be used by cybersecurity analysts to share cybersecurity information securely[15].

3.3 Literature Review

In this phase, a review of literature related to previous research on information security sharing in various organizations and the utilization of the Interplanetary File System as a solution to the single point of failure issue is conducted[16].

3.4 System Architecture Design

The design is based on recommendations obtained from the literature review to serve as a solution to the defined problem. The goal of this system design is to create a cybersecurity information storage and sharing system that can ensure the availability, integrity, and confidentiality of cybersecurity information stored and exchanged among organizations. In pursuit of this goal, the system has been devised utilizing the Interplanetary File System (IPFS)[17]. IPFS serves as a peer-to-peer network protocol designed for data storage within a distributed system. Diverging from the conventional file storage on servers, IPFS disseminates files across numerous nodes within its network. IPFS adopts content-based addressing, wherein file addresses are generated based on the content's hash. Additionally, it makes use of a distributed hash table to pinpoint the data's location or the path leading closer to it. Within the

architecture of this system, IPFS is harnessed as a decentralized file storage solution, allowing files to be spread across diverse nodes integrated into the IPFS network. These technologies are seamlessly integrated into the CyberShare system architecture[18].

3.5 Testing and Analysis

The testing of the system involves the establishment of a virtual environment that mirrors a real-world scenario. Within this environment, the system or application can undergo testing in isolation, without any impact on the actual operational setting[19]. For the CyberShare system simulation, VMware 12.2.4 virtualization software is employed, featuring four distinct Linux operating systems, each representing a separate node with specifications. This configuration enables secure and isolated testing and application development. Furthermore, the CyberShare system simulation offers the capability to evaluate information security without disrupting the primary operating system or the authentic environment. In this phase, a simulation testing of the system is conducted virtually by configuring a Cybershare system with four interconnected IPFS nodes using identical swarm keys.

Table 1. Linux Node Specifications in CyberShare System Simulation

Node	Virtualization Software	Operating System	Testing Type
1	VMware 12.2.4	Linux OS 1	Information Security
2	VMware 12.2.4	Linux OS 2	Information Security
3	VMware 12.2.4	Linux OS 3	Information Security
4	VMware 12.2.4	Linux OS 4	Information Security

This simulation testing includes non-functional testing, such as information security testing, which evaluates confidentiality, integrity, and availability of cybersecurity information in the designed system, leveraging IPFS. The primary objective of information security testing is to identify vulnerabilities or security gaps in the system and safeguard sensitive data from unauthorized access. The simulation testing is carried out on virtual machines based on predefined scenarios. Subsequently, an analysis of the system testing results is performed to form the basis for drawing conclusions and recommendations for future research[20].

3.6 Conclusion Drawing

The ultimate phase encompasses deriving conclusions based on the research discoveries and formulating recommendations and proposals for advancing further research.

4. Results and Discussion

This chapter presents the results of the testing and discussion, which include an analysis of information security encompassing availability, integrity, and confidentiality of cybersecurity information. The results and discussions are presented as follows:

4.1 Test Results

To assess file availability, experiments were designed to evaluate the system's ability to handle unforeseen situations, such as when one node experiences failure or becomes inactive. In the availability testing involving one inactive node out of four, an attempt was made to upload a file from node Ipfs1 into the private IPFS network. Subsequently, an effort was made to download this file from all nodes, including node Ipfs1. However, in this scenario, one of the nodes, i.e., node Ipfs4, was intentionally kept inactive while the others remained active[21].
The integrity testing involved uploading two files to CyberShare. These two files had similar names and sizes (differing by 5,510 bytes) but had slight content differences. According to the principles of hash functions, CyberShare could easily identify both files with different hash

outputs due to content differences. In CyberShare, users can verify the integrity of each file using the hash value generated by the hash function[22].

Table 2. Types of Testing in the CyberShare System

Testing Type	Description
Availability	Testing to assess the system's ability to handle unforeseen situations, such as node failure or inactivity.
	- Attempted file upload from node Ipfs1 to the private IPFS network with one node (Ipfs4) intentionally kept inactive.
	- Downloaded the same file from all nodes, including the inactive one.
Integrity	Testing involving the upload of two files to CyberShare with similar names and sizes but slight content differences.
	- The system uses hash functions to differentiate files based on content differences.
	- Users can verify file integrity using the hash value generated by the hash function.
Confidentiality	Testing considering the possibility of downloading files from IPFS client nodes outside the private network or from unregistered users within the private IPFS network.
	- IPFS outside the private network uses different swarm keys compared to those used within the private IPFS network.
	- Users from outside the private IPFS network have valid hash values for files they wish to download within the private IPFS network.

Regarding confidentiality testing, there was a possibility to download files from IPFS client nodes outside the private network, or even from users who were not registered within the private IPFS network. In this scenario, IPFS used outside the private network had different swarm keys from those used within the private IPFS network. However, users from outside the private IPFS network possessed valid hash values for the files they wished to download within the private IPFS network[23].

4.2 Analysis

To evaluate the availability, integrity, and confidentiality of files within the CyberShare system, various testing scenarios were performed. Availability testing was conducted by disabling one node in the private IPFS network used by the system to simulate system failure or cyberattacks. The results showed that data could still be accessed through active nodes within the private IPFS network. This indicates that the CyberShare storage system using IPFS technology can provide a high level of redundancy and is not dependent on a vulnerable central point for system failure, ensuring data availability in challenging situations[24].
Subsequently, integrity testing was carried out by uploading both original and modified files with similar content and nearly identical sizes into the CyberShare system. The results demonstrated that the CyberShare system could detect changes made to files, even if they were only a few bytes different. This occurs because IPFS within the CyberShare system uses hash technology to ensure data integrity by creating a hash of the file and storing it within the private IPFS network. With this hash, IPFS can ensure that data stored within the network cannot be modified

without the knowledge of network users[25].

Lastly, confidentiality testing was performed by simulating unauthorized access from malicious entities outside the CyberShare system. In this test, downloads were attempted by entities that had not registered as members of the private IPFS network in the CyberShare system and entities located on networks different from the private IPFS network but possessing valid hash values or files of interest. However, the results of the test showed that downloading from unregistered entities and entities outside the private IPFS network could not be executed and failed. This is due to the fact that entities outside the private IPFS network do not possess the same swarm key as members of the private IPFS network, preventing file upload or download into the system. Therefore, this test confirms that the CyberShare system can provide a high level of data confidentiality for the information stored within it.

5. Conclusion

Based on the analysis of test results in this research, it can be concluded that the design and analysis of information security in a secure cybersecurity information sharing (CyberShare) system by utilizing a four-node interplanetary file system (IPFS) private network as decentralized cybersecurity information storage is an effective solution for improving security cyber and user trust in the confidentiality, integrity and availability of information. This way, organizations can share and utilize cybersecurity information safely. In addition, the use of decentralized storage in CyberShare also addresses privacy issues that arise due to a single authority in centralized storage, which can modify and utilize information without the consent of the information owner. However, it should be noted that the CyberShare system still has shortcomings, such as not recording transaction data between the sender and recipient of information, which could lead to potential denial of transferred data. Therefore, further development using blockchain technology as an immutable transaction recording system between the sender and recipient is needed to provide authentic proof and prevent denial of transactions between the two parties.

References

[1] U. Rahardja, Q. Aini, D. Manongga, I. Sembiring, and I. D. Girinzio, “Implementation of Tensor Flow in Air Quality Monitoring Based on Artificial Intelligence,” *Int. J. Artif. Intell. Res.*, vol. 6, no. 1, 2023.

[2] T. Hadi and A. B. Marpaung, “Transformational Leadership and Knowledge Management Impact on Organization Performance: A Systematic Review,” *Int. J. Soc. Serv. Res.*, vol. 3, no. 1, pp. 228–235, 2023.

[3] Z. Lubis, M. Zarlis, and M. R. Aulia, “Performance Analysis of Oil Palm Companies Based on Barcode System through Fit Viability Approach: Long Work as A Moderator Variable,” *Aptisi Trans. Technopreneursh.*, vol. 5, no. 1, pp. 40–52, 2023.

[4] N. M. N. Febrianti and G. S. Darma, “Millennials’ Intention to Invest through Securities Crowdfunding Platform,” *Aptisi Trans. Technopreneursh.*, vol. 5, no. 1, pp. 19–30, 2023.

[5] B. Rawat, A. S. Bist, M. Fakhrezzy, and R. D. Octavyra, “AI based assistance to reduce suicidal tendency among youngsters,” *APTISI Trans. Manag.*, vol. 7, no. 2, pp. 105–112, 2023.

[6] Y. Z. Basri and W. Arafah, “Determinant of Interest in Paying Zakat with Age as a Moderating Variable (Study on Minang Society),” *APTISI Trans. Manag.*, vol. 7, no. 2, pp. 92–104, 2023.

[7] F. Sutisna, T. Handra, and Y. P. Jap, “The Influence of Social Media Marketing on Purchase Impulses with Brand Attentiveness as A Mediating Variable on UMKM X,” *Aptisi Trans. Technopreneursh.*, vol. 5, no. 2, pp. 136–144, 2023.

[8] T. K. Andiani and O. Jayanagara, “Effect of Workload, Work Stress, Technical Skills, Self-Efficacy, and Social Competence on Medical Personnel Performance,” *Aptisi Trans. Technopreneursh.*, vol. 5, no. 2, pp. 118–127, 2023.

[9] N. Lutfiani, S. Wijono, U. Rahardja, A. Iriani, Q. Aini, and R. A. D. Septian, “A bibliometric study: Recommendation based on artificial intelligence for ilearning education,” *Aptisi*

Trans. Technopreneursh., vol. 5, no. 2, pp. 109–117, 2023.
[10] M. H. R. Chakim, P. A. Sunarya, V. Agarwal, and I. N. Hikam, "Village Tourism Empowerment Against Innovation, Economy Creative, and Social Environmental," *Aptisi Trans. Technopreneursh.*, vol. 5, no. 2sp, pp. 162–174, 2023.
[11] A. G. Prawiyogi, M. Hammet, and A. Williams, "Visualization Guides in the Understanding of Theoretical Material in Lectures," *Int. J. Cyber IT Serv. Manag.*, vol. 3, no. 1, pp. 54–60, 2023.
[12] M. Annas and S. N. Wahab, "Data Mining Methods: K-Means Clustering Algorithms," *Int. J. Cyber IT Serv. Manag.*, vol. 3, no. 1, pp. 40–47, 2023.
[13] E. Nurninawati, R. Supriati, and A. Maulana, "Web-Based E-Learning Application to Support the Teaching and Learning Process at Genta Syaputra Senior High School," *Int. J. Cyber IT Serv. Manag.*, vol. 3, no. 1, pp. 12–21, 2023.
[14] E. Nurninawati, M. Y. Effendy, and A. M. Rianputra, "Web-Based Product Marketing Information System Design at Definier Store," *Int. J. Cyber IT Serv. Manag.*, vol. 3, no. 1, pp. 1–11, 2023.
[15] A. G. Prawiyogi, "Southeast Asia's Cyber Security Strategy: Multilateralism or Self-help," *IAIC Trans. Sustain. Digit. Innov.*, vol. 4, no. 2, pp. 119–127, 2023.
[16] M. F. Fazri, L. B. Kusuma, R. B. Rahmawan, H. N. Fauji, and C. Camille, "Implementing Artificial Intelligence to Reduce Marine Ecosystem Pollution," *IAIC Trans. Sustain. Digit. Innov.*, vol. 4, no. 2, pp. 101–108, 2023.
[17] E. Nathanael and W. Sejati, "Effective Government Management of Flood Discharge in Drainage Channels using HEC-RAS 6.3. 1 Application," *APTISI Trans. Manag.*, vol. 7, no. 3, pp. 210–220, 2023.
[18] U. Rahardja, Q. Aini, D. Manongga, I. Sembiring, and Y. P. A. Sanjaya, "Enhancing Machine Learning with Low-Cost P M2. 5 Air Quality Sensor Calibration using Image Processing," *APTISI Trans. Manag.*, vol. 7, no. 3, pp. 201–209, 2023.
[19] Q. Aini, E. P. Harahap, N. P. L. Santoso, S. N. Sari, and P. A. Sunarya, "Blockchain Based Certificate Verification System Management," *APTISI Trans. Manag.*, vol. 7, no. 3, pp. 1–10, 2023.
[20] U. Rahardja, P. A. Sunarya, N. Lutfiani, M. Hardini, and H. R. Dananjaya, "Analysis of Renewable Energy Utilization Using Solar Power Technology in Eliminating Microplastic Emissions," in *2022 IEEE Creative Communication and Innovative Technology (ICCIT)*, 2022, pp. 1–6.
[21] U. Rahardja, "The economic impact of cryptocurrencies in indonesia," *ADI J. Recent Innov.*, vol. 4, no. 2, pp. 194–200, 2023.
[22] U. Rahardja, C. T. Sigalingging, P. O. H. Putra, A. Nizar Hidayanto, and K. Phusavat, "The impact of mobile payment application design and performance attributes on consumer emotions and continuance intention," *SAGE Open*, vol. 13, no. 1, p. 21582440231151920, 2023.
[23] A. Sutarman, U. Rahardja, F. P. Oganda, S. Millah, and N. N. Azizah, "The Role of Information Technology in Empowering the Creative Economy for Sustainable Tourism," *Aptisi Trans. Technopreneursh.*, vol. 5, no. 2sp, pp. 175–185, 2023.
[24] U. Rahardja, "Risk Assessment, Risk Identification, and Control in The Process Of Steel Smelting Using the Hiradc Method," *APTISI Trans. Manag.*, vol. 7, no. 3, pp. 261–272, 2023.
[25] M. Miran and O. Sumampouw, "Superior College Applied Research Competence of SPI Members in the Context of Improving the Quality of Supervisory Performance at Manado State University," *Aptisi Trans. Technopreneursh.*, vol. 5, no. 1, pp. 73–86, 2023.