Institut Riset dan Publikasi Indonesia (IRPI)
MALCOM: Indonesian Journal of Machine Learning and Computer Science
Journal Homepage: https://journal.irpi.or.id/index.php/malcom
Vol. 4 Iss. 4 October 2024, pp: 1390-1402
ISSN(P): 2797-2313 | ISSN(E): 2775-8575

Design and Analysis of Cybersecurity Information Sharing Mechanism Between Computer Security Incident Response Teams (CSIRT) in Indonesia on Blockchain Technology Through Hyperledger Composer and Interplanetary File System (IPFS)

Fajar Hariyanto[1], Kalamullah Ramli[2]

[1,2]Program Studi Teknik Elektro, Fakultas Teknik, Universitas Indonesia, Indonesia

E-Mail: [1]fajar.hariyanto@ui.ac.id, [2]kalamullah.ramli@ui.ac.id

Received Jun 13th 2024; Revised Jul 15th 2024; Accepted Jul 25th 2024
Corresponding Author: Fajar Hariyanto

Abstract

Sharing cybersecurity information among the Computer Security Incident Response Team (CSIRT) is a crucial step in enhancing organizational cybersecurity. However, a primary challenge faced is the lack of trust among users regarding the confidentiality, integrity, and availability of shared information. This study proposes a new approach by designing a mechanism for sharing cybersecurity information among CSIRTs in Indonesia on blockchain technology using Hyperledger Composer. This approach offers an innovative solution by leveraging the advantages of blockchain technology. Through this approach, cybersecurity information can be shared in a decentralized manner, overcoming the weaknesses of centralized systems, and enhancing overall information security. Another advantage of blockchain technology is its high performance and scalability, enabling increased speed, and user capacity in the process of sharing information. By implementing a blockchain-based mechanism for sharing cybersecurity information, this research aims to ensure crucial aspects of information security, namely confidentiality, integrity, and availability. The contribution of this study is not only in enhancing organizational cybersecurity but also in providing an innovative solution to practical challenges in sharing cybersecurity information among CSIRTs.

Keywords: Blockchain, CSIRT, Hyperledger Composer, Information Security, Information Sharing

1. INTRODUCTION

In an increasingly advanced digital era, threats to cyber security have become one of the most critical issues faced by organizations throughout the world, including in Indonesia. Cyberattacks, such as ransomware, malware, and phishing are becoming more frequent and more sophisticated, causing large financial losses, and damaging an organization's reputation [1]. In Indonesia, the need to improve cyber security is increasingly urgent along with the increasing adoption of digital technology in various sectors, such as banking, health, and government [2].

The Computer Security Incident Response Team (CSIRT) in Indonesia has an important role in detecting, responding to, and overcoming cyber security incidents. However, one of the main challenges faced by CSIRT is the lack of effective and secure information-sharing mechanisms between teams. Information sharing is a key element in responding quickly and appropriately to cybersecurity incidents, but data security and integrity, as well as a lack of trust between teams often hinder this process [3].

The main problem in sharing information between CSIRTs is a lack of trust. Without strong trust, it is difficult to ensure that sensitive information can be shared without the risk of data misuse or manipulation. These concerns often hinder the flow of information that could help prevent or resolve similar cybersecurity incidents at other organizations. In addition, current information-sharing mechanisms often lack sufficient transparency and auditability [4]. Transparency and auditability are essential to ensure that shared data is kept intact and is not altered by unauthorized parties. Existing mechanisms are also vulnerable to various cyber-attacks, such as man-in-the-middle attacks, which can compromise data integrity during the information-sharing process [5].

Numerous studies have explored various approaches to improve information sharing in the context of cybersecurity. One promising approach is the use of blockchain technology. Blockchain, with its decentralized, transparent, and immutable nature, offers a potential solution to address cybersecurity information-sharing challenges. Blockchain has been identified as a solution for the secure and decentralized sharing of

cybersecurity incident data by providing a robust and transparent audit mechanism [1]. Blockchain-based frameworks increase trust and collaboration between organizations in sharing cyber threat information [6], as well as reducing the risk of data misuse by ensuring the integrity and authenticity of information [7]. In the financial sector, blockchain increases the efficiency and security of information sharing by reducing response times to threats [3], while Hyperledger Fabric can meet the needs of secure information sharing in industrial environments [8]. In the healthcare sector, blockchain ensures the integrity and privacy of patient data [4] and generally increases transparency and trust between organizations [9]. Blockchain also provides a secure and efficient platform for sharing information in the public sector [10], addresses the challenges of trust and data security in the education sector [11], and provides a secure mechanism for sharing information in the technology industry [5]. In addition, blockchain improves collaboration and reduces security risks in manufacturing environments [12], ensures data integrity, and increases trust in the energy sector [13] as well as increases transparency and trust in information sharing in the transportation sector [14]. In the banking sector, blockchain reduces the risk of fraud and increases trust between banks [15], ensures the privacy and security of patient data in the health sector [16], and also ensures the authenticity and integrity of data in the telecommunications sector [17]. Moreover, blockchain also ensures information security in the education sector [18], increases transparency and trust between government agencies [19], increases the efficiency and security of information sharing in the technology sector [20], ensures data authenticity in the retail sector [21], and increases trust and collaboration between financial entities [22]. Blockchain ensures the authenticity and integrity of data in the automotive sector [23], increases transparency and security in logistics processes [24], and ensures information security in the education sector [25]. Last, blockchain improves data integrity and trust in the energy sector [26], as well as increases transparency and trust in the transportation sector [27].

Hyperledger Composer and Hyperledger Fabric, as two popular implementations of blockchain technology, offer various advantages in the context of sharing cybersecurity information. Hyperledger Composer provides tools to create and disseminate blockchain solutions quickly and easily, allowing organizations to define data models, business logic, and access control flexibly (H. Foundation, 2022). Meanwhile, Hyperledger Fabric offers a modular architecture that supports privacy and scalability, making it suitable for various cases of use in the industry [28].

Various studies have examined the use of Hyperledger Composer and Fabric in sharing information. The use of Hyperledger Fabric to share data safely in the IoT industry shows a significant increase in data security and data efficiency [29]. The Hyperledger Fabric application in health data management emphasizes the ability of this technology to ensure the integrity and privacy of patient data [30]. Various blockchain applications in cyber security, including the use of Hyperledger Fabric to share information on security incidents, have been reviewed [31]. The benefits and challenges of using blockchain in the public sector, focusing on Hyperledger Fabric to share data between government institutions, have also been studied [32]. The use of hyperledger composers in the education sector to share academic data safely and decentralized has been [33]. Besides, the use of Hyperledger Fabric in the technology industry to improve information security and reduce the risk of cyber-attacks has been discussed [34]. An exploration of how Hyperledger Fabric can increase collaboration and security in the manufacturing sector has been carried out [35]. Research on how blockchain can ensure data integrity in the energy sector, using Hyperledger Fabric as a main example, has also been carried out [35], and the use of Hyperledger Fabric to increase transparency and security in the transportation sector has been reviewed [37]. Finally, the exploration of how blockchain, including Hyperledger Fabric, can reduce the risk of fraud and increase trust in the banking sector has also been explored [38]. This study aims to design a mechanism for sharing cyber security information between CSIRT in Indonesia based on blockchain using Hyperledger Composer and Fabric. This design is adjusted to the Traffic Light Protocol (TLP) standard from the First Framework, which ensures that sensitive information is distributed with high levels of security and trust. This approach is used to overcome the challenges existing in sharing information between CSIRT, increasing responses to cyber security incidents, and supporting national cyber protection efforts.

2. MATERIALS AND METHOD

This research consists of four stages of research as shown in Figure 1. The stages of the problem identification were carried out to determine the problems raised in this study based on the trend of cyber incidents, CSIRT development, CSIRT development, and coordination between CSIRT. The problems found and raised in this study are the lack of trust between CSIRT and confidentiality, integrity, and availability of cyber security information that is shared.

The literature study stage was carried out to find connections with previous research and as a reference in finding new ideas and developing research to avoid plagiarism. The literature study in this research includes cyber security information sharing, information security, blockchain technology, CSIRT, hyper ledger framework, hyper ledger tools, hyper ledger composer, hyper ledger fabric, and related research. The design stage of the mechanism for sharing cyber security information between CSIRTs based on blockchain

technology was carried out to make it easier to create the system. At this design stage, the following steps were carried out:

1. Requirements analysis includes hardware and software requirements
2. Designing an information-sharing mechanism to determine and provide an overview of the flow of information sharing between CSIRTs in Indonesia.
3. Designing file structures to determine participants, assets, and transactions in a cybersecurity information sharing mechanism system that will be built in Hyperledger Composer.
4. Implementation and simulation using Hyperledger Composer Playground.
5. Testing and analysis of the information sharing design in this research consist of functionality testing, performance testing, and information security analysis. The final stage will produce conclusions from this research.

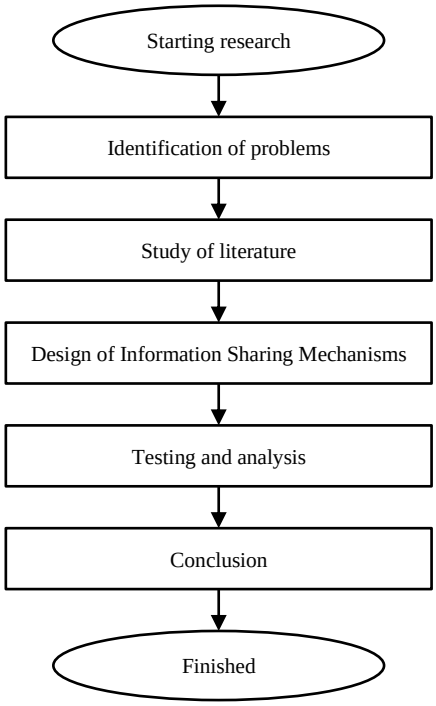

Figure 1. Research Stages

3. RESULTS AND DISCUSSION

3.1. System Design

3.1.1. Needs Analysis

The needs analysis in this research is related to hardware and software requirements to implement and simulate the cyber security information sharing mechanism designed as shown in Table 1.

Table 1. Hardware and Software Specifications

Hardware	*Software*
1. Type: Dell Latitude 7400 2. Processor: Intel(R) Core (TM) i7-8665U CPU @ 1.90GHz 2.11 GHz 3. RAM: 8GB 4. System Type: 64-bit	1. Operating Systems: Ubuntu Linux 18.04 LTS 2. Composer Playground v0.19 3. IPFS v0.14.0 4. Yeoman v3.1.1 5. Fabric-dev-server v1.2 6. Docker Engine: Version 20.10.7 7. Docker-Compose: Version 1.13.0 8. Node: v8.17.0 9. npm: v6.13.4 10. git: 2.43.2 11. Python: 2.7.12 12. Visual studio code 1.87.0

3.1.2. Design of Information Sharing Mechanisms

The mechanism for sharing cyber security information between CSIRTs in Indonesia proposed in this research is based on blockchain technology using hyper ledger composer and InterPlanetary File System

(IPFS). This mechanism is divided into two phases, namely the Off-Chain phase and the On-Chain phase, which is carried out by the CSIRT sender to the CSIRT recipient as shown in Figure 2.

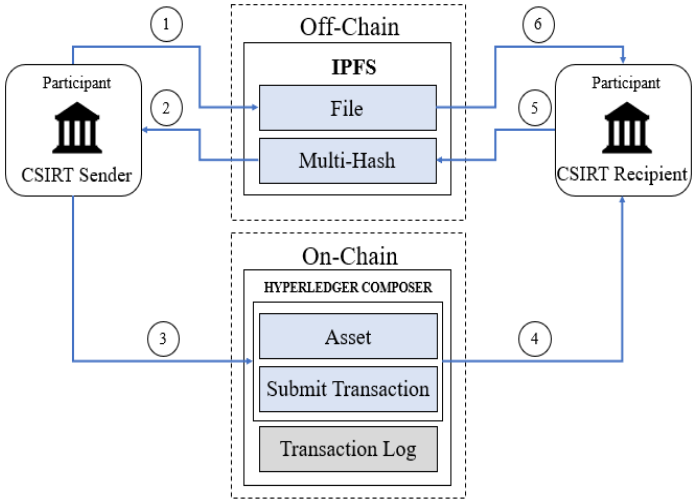

Figure 2. Proposed Cybersecurity Information Sharing Mechanism

The Off-Chain phase is the phase where each participant, which in this research is CSIRT, can carry out the process of uploading and downloading files regarding shared cyber security information. Meanwhile, the On-Chain phase is a phase that functions to regulate trusted transactions between CSIRTs through setting access control and recording transaction logs. In the On-Chain phase, the assets distributed are based on the multi-hash value generated in the Off-Chain phase. The following is the flow of the proposed information-sharing mechanism between CSIRTs in Figure 2:

1. CSIRT sender uploads the cybersecurity information file to be shared with IPFS. These information files include formats, such as .pdf, .txt, .jpg, .mp3, and .mp4.
2. IPFS provides feedback to the CSIRT sender in the form of a multi-hash value from the file uploaded by the CSIRT sender. Besides being the address where the file is stored, this multi-hash value is also used as a link to access or download the file.
3. After getting the multi-hash value from the file uploaded to IPFS, the CSIRT sender creates assets and submits transactions in Hyperledger Composer to the CSIRT recipient.
4. CSIRT recipient receives shared cybersecurity information including multi-hash values.
5. CSIRT recipient accesses or downloads cybersecurity information shared from IPFS using a multi-hash value link.
6. IPFS verifies the multi-hash value, if the hash value used is verified to be in IPFS, then IPFS will send feedback in the form of a cyber security information file, which is shared with the CSIRT recipient.

3.1.3. File Structure Design

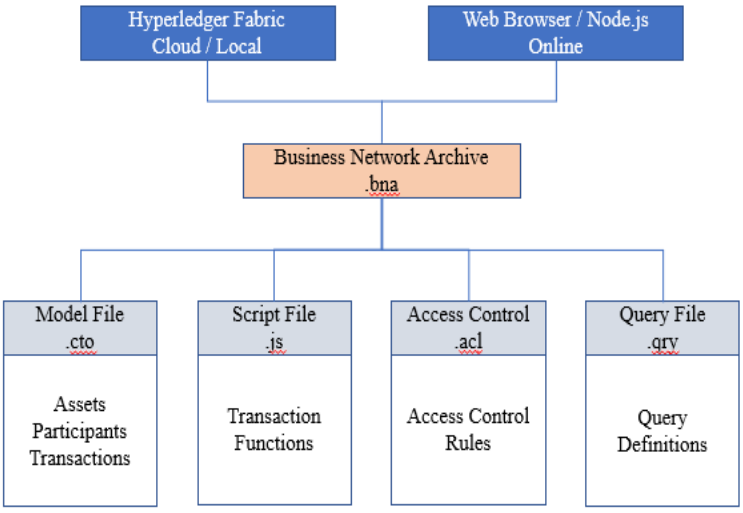

Figure 3. File Structure of the mechanism for sharing cyber security information

In Figure 3, the file structure is shown in the Hyperledger Composer, which consists of file models, file scripts, access control, and query files to support the implementation of the cyber security information sharing mechanism. The file structure used in this study includes:

1. File models, are used to define assets, participates, and transactions. Assets are represented into information titles and information types, and TLP participant information categories can be divided into four categories namely national CSIRT, sectoral CSIRT, organizational CSIRT, and special CSIRT as shown in Figure 4.
2. File scripts, used to define transactions in sharing information implemented in this study.
3. Access Control, used to regulate access control against each CSIRT as a participant in the information sharing mechanism.

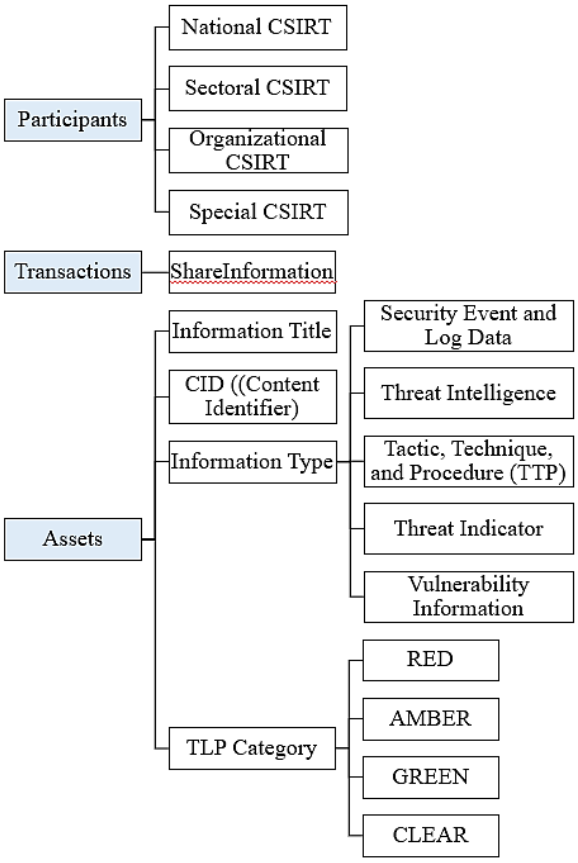

Figure 4. Defining Participants, Transactions, and Assets

3.2. Implementation and Simulation

Implementation discusses the stages to realize the design stage. Based on the results of system design, implementation is divided into off-chain and on-chain implementation.

1. Off-Chain Implementation
   In off-chain implementation, IPFS installation was carried out in the Ubuntu 18.04 environment that is run with a virtual box. The following installation commands are run through the terminal:

```
$   wget   https://dist.ipfs.io/go-ipfs/v0.14.0/go-
ipfs_v0.14.0_linux-amd64.tar.gz
$   tar   -xvzf   go-ipfs_v0.13.2_linux-amd64.tar.gz
$ cd go-ipfs
$ sudo bash install.sh
```

   Before uploading the cyber security information file to IPFS, the first initialized repository is shown in Figure 5.

Figure 5. Initialization of Repository

After the repository initialization is successful, the off-chain stage can be carried out by the Participant or CSIRT Sender to upload the cyber security information file that will be shared with IPFS. After the file is uploaded, then IPFS will provide a multi-hash value as a CID (Content Identifier) of the uploaded file. From the sample implementation in Figure 6, a CID value was obtained, namely Qme1KRhmxmUX6xRCGRmTMLDpP2FiAkjLi11WcqsDbfiw9k.

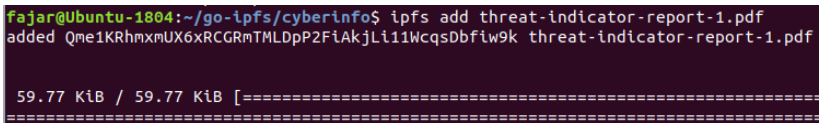

Figure 6. Upload Cybersecurity Information File

The node in the above process is still local so that the uploaded file can be accessed globally, the IPFS Daemon command was carried out, as in Figure 7.

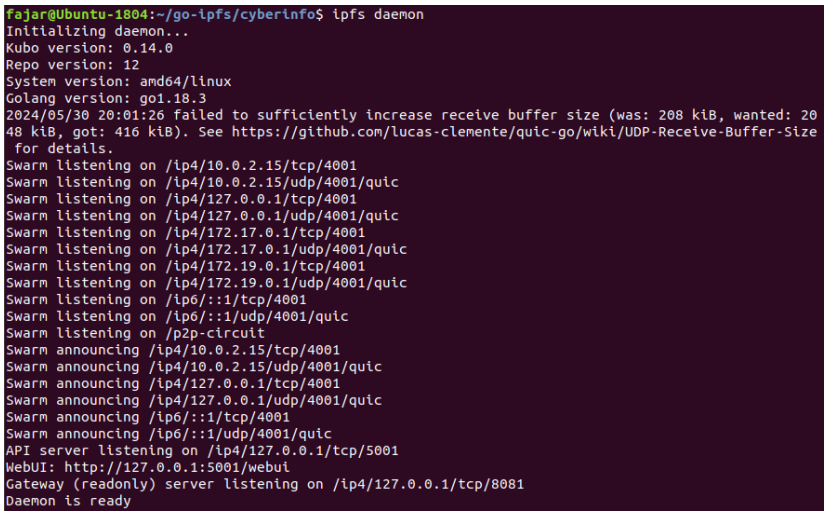

Figure 7. Merging nodes to public networks

After combining IPFS to the public network, the uploaded file can be downloaded publicly with the commands that can be seen in Figure 8.

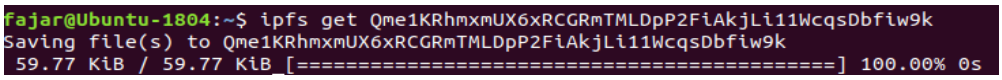

Figure 8. Download the cyber security information file

2. On-Chain Implementation

On-chain implementation is an implementation of sharing of cyber security information between blockchain-based CSIRT using Hyperledger Composer. Implementation is carried out in the form of a web playground-based simulation. Preparation aims to do the Hyperledger Composer Playground installation on Ubuntu 18.04, which can be seen in Figure 9.

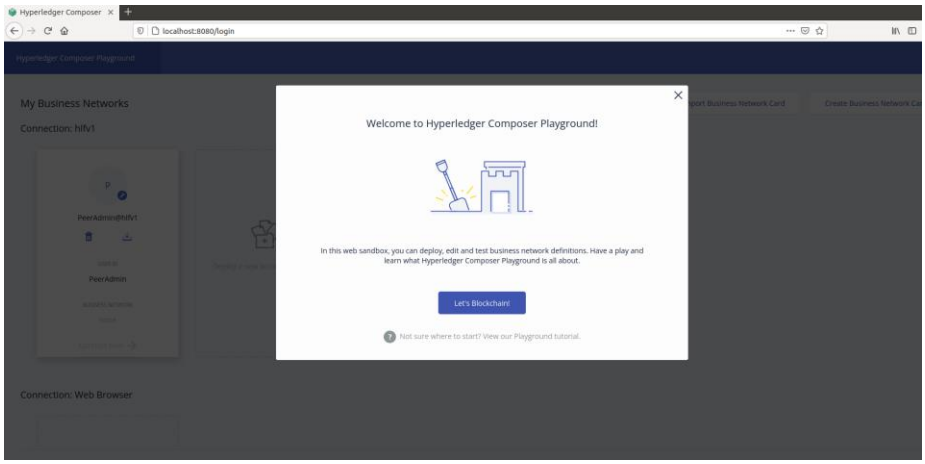

Figure 9. Installation of Hyperledger Composer Playground

Next configuration of file models, file scripts, and access control was according to the desired simulation. Then, a deployment process was carried out on the Hyperledger Composer Playground. On pages that have been deployed, tab tests were used to make participants, make assets, and submit transactions. Participant in this study was defined as CSIRT in Indonesia, which was divided into four types of CSIRT namely National CSIRT, Sectoral CSIRT, Organization CSIRT, and Special CSIRT. The following are some of the coding samples to make CSIRT participants as shown in Figure 10-13.

```
{
  "$class":
"org.example.security.CSIRTNasional",
  "CSIRTId": "0097",
  "name": "CSIRT Nasional"
}
```

Figure 10. Sample Code Making National Participant CSIRTs

```
{
  "$class":
"org.example.security.CSIRTSektoral",
  "sektor": "pemerintahan",
  "CSIRTId": "9584",
  "name": "CSIRT Sektoral Pemerintahan"
}
```

Figure 11. Sample Code Making Participant CSIRT Sectoral

```
{
  "$class":
"org.example.security.CSIRTOrganisasi",
  "organisasi": "Organisasi Pemerintahan 1",
  "sektor": "pemerintahan",
  "CSIRTId": "3935",
  "name": "CSIRT Organisasi Pemerintahan 1"
}
```

Figure 12. Sample Making Participant CSIRT Organizational

```
{
  "$class":
"org.example.security.CSIRTKhusus",
  "CSIRTId": "3617",
  "name": "CSIRT Khusus 1"
}
```

Figure 13. Special Participant CSIRT Making Samples

The Code of Making Participants in Hyperlederger Composer produces a list of registered CSIRT and has access to share cyber security information. The registered list of registered participants appears on the Participants menu at the Hyperledger Composer as shown in Figure 14.

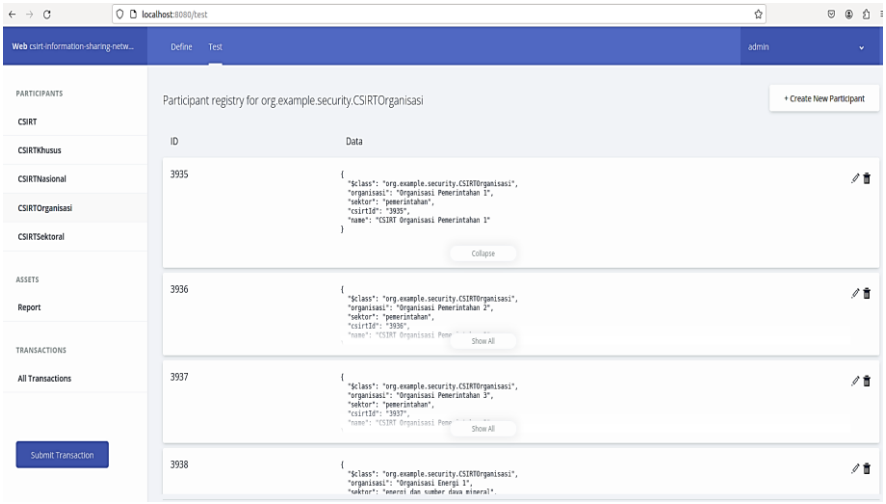

Figure 14. Registered List of Registered Participant CSIRT

In the On-Chain implementation, the registered CSIRT participant has access to make assets, namely cyber security information that will be distributed to other CSIRT. Assets in this simulation are defined as reports that contain information between Laing ReportIds, Tittle Information, CID, Description, TLP, and Type of Information. Samples of coding Cyber Security Information Asset Code in this simulation are shown in Figure 15.

```
{
  "$class": "org.example.security.Report",
  "reportId": "0478",
  "title": "Perkembangan Terbaru dalam
Threat Indicator (Mei 2024)",
  "CID":
"Qme1KRhmxmUX6xRCGRmTMLDpP2FiAkjLi11WcqsDbf
iw9k",
  "description": "Pentingnya Threat
Indicator dalam keamanan siber: Membantu
dalam deteksi dini dan mitigasi ancaman",
  "tlp": "RED",
  "type": "THREAT_INDICATOR",
  "shared": false,
  "owner":
"resource:org.example.security.CSIRT#3935",
  "recipients": []
}
```

Figure 15. Sample Asset-Making Code

On-chain implementation aims to make a transaction to share cyber security information in the blockchain network using the Hyperledger Composer. After successfully making participants and assets, a simulation of sharing information between participants is CSIRT, as the owner of the information to CSIRT recipient. Information received by the CSIRT recipient is still in the form of an identity that was pressed by the CID value of the cyber security information file. In sharing information on the Hyperledger Composer, the CSIRT sender makes a submitted transaction code, such as the sample code shown in Figure 16. The value of 0478 refers to the reportId value of the asset that has been made by the CSIRT sender.

```
{
  "$class":
"org.example.security.ShareReport",
  "report":
"resource:org.example.security.Report#0478"
,
  "sender":
"resource:org.example.security.CSIRT#3935",
  "recipients":
["resource:org.example.security.CSIRT#3937"
]
}
```

Figure 16. Sample Submit Transaction Code

After the CSIRT sender submits the transaction, the CSIRT recipient will receive information including the CID value. This value was used by the CSIRT recipient to download the cyber security information file shared through IPFS. That way, the CSIRT recipient could find out the content of cyber security information shared by the CSIRT sender. The file download stage by the CSIRT recipient is an Off-Chain simulation because it was done outside the blockchain network on the Hyperledger Composer.

3.3. Test and Analysis

3.3.1. Performance Test

Performance test on the system was carried out by conducting several tests of IPFS performance in uploading and downloading cyber security files using a special script to measure the average lay with a certain number of rounds and send rate. The test script was run through the Ubuntu Terminal 18.04 LTS.

Testing Performance uploading Cybersecurity Information Files to IPFS was carried out with various levels of shipping (send rate) ranging from 5 to 50 requests per second (RPS). The test results displayed in Table 2 indicate that the average latency (AVG. Latency) and throughput vary depending on the delivery rate.

In Send Rate 5 RPS, the average latency is 0.373 seconds with a throughput of 2,989 RPS. Along with an increase in send rates up to 50 RPS, the average latency shows a trend decrease up to 0.255 seconds, while the throughput increases to reach 4,080 RPS at the highest send rate tested. The peak throughput is achieved at Send Rate 25 RPS with a value of 4,435 RPS and a latency of 0.242 seconds.

These latency and throughput fluctuations can be influenced by network loads and the efficiency of demand handling by IPFS. The increase in the number of demands is not always directly proportional to the increase in latency or decreased throughput, which shows the optimization in handling uploads by IPFS at a certain level of demand.

Table 2. Testing Performance Upload Cyber Security Information Files to IPFS

Round	Send (rps)	Avg. Latency (s)	Throughput (rps)
1	5	0.373	2.989
2	10	0.296	3.518
3	15	0.277	3.804
4	20	0.312	3.329
5	25	0.242	4.435
6	30	0.228	4.713
7	35	0.256	4.240
8	40	0.269	3.882
9	45	0.233	4.472
10	50	0.255	4.080

Performance test downloading files from IPFS was also carried out with the same send rate, from 5 to 50 RPS. In Send Rate 5 RPS, the average latency is 0.137 seconds with a throughput of 8,815 RPS. When a send rate increases to 50 RPS, the average latency (AVG. Latency) drops to 0.075 seconds and throughput reaches 15,848 RPS.

Table 3 show that the lowest latency value is achieved in a send rate of 30 RPS with 0.070 seconds, while the highest throughput is 16,455 RPS on the same send rate. This test shows that the IPFS system is more efficient in handling downloads than uploads, with lower latency and higher throughput as a whole.

Table 3. Testing Performance Download Cyber Security Information Files to IPFS

Round	Send (rps)	Avg. Latency (s)	Throughput (rps)
1	5	0.137	8.815
2	10	0.091	12.511
3	15	0.094	11.883
4	20	0.073	15.844
5	25	0.076	15.741
6	30	0.070	16.455
7	35	0.091	12.635
8	40	0.099	11.174
9	45	0.074	15.250
10	50	0.075	15.848

The graph in Figure 17 shows the ratio between Transaction Rate and Average Latency and Throughput in the file upload process to IPFS. From the graph, it can be seen that along with an increase in send rate, Average Latency tends to decrease, which indicates an increase in system efficiency in dealing with higher demand. Throughput increases significantly in send rates to 25 RPS before experiencing a slight decrease in a higher send rate, which is likely caused by the capacity of the network or IPFS server to handle the volume of large data simultaneously.

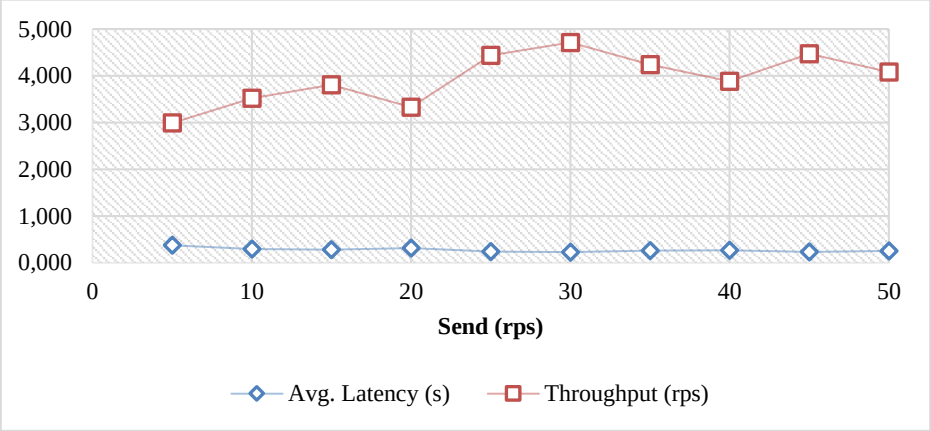

Figure 17. Comparison of Transaction Rate with Average Latency and Throughput in the File Upload Process to IPFS

Figure 18 indicates the same comparison for the process of downloading files from IPFS. This graph shows the trend of decreased average latency, which is more consistent than the upload chart, as well as increasing through more significant and stable throughput. This confirms that IPFS is more optimized for download operations, with a sharper decrease in latency and high throughput even at a higher level of demand.

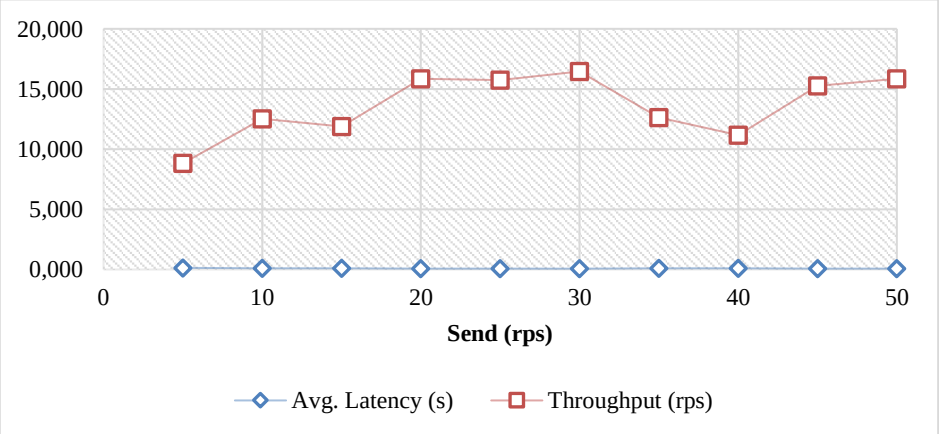

Figure 18. Comparison of Transaction Rate with Average Latency and Throughput in the process of downloading files to IPFS

Overall, the results of this test indicate that IPFS has a solid performance in handling uploads and downloads of cyber security information files, with better efficiency in download operations. Further optimization may be needed to improve upload performance, especially on higher send rates.

3.4. Information Security Analysis

Information security analysis in this study focuses on three aspects, namely confidentiality, integrity, and availability.

1. Confidentiality
   The mechanism for sharing cyber security information between CSIRT proposed in this study prioritizes the confidentiality of information through the use of Blockchain Hyperledger Composer and Interplanetary File System (IPFS). Hyperledger Composer blockchain technology guarantees that only those who have access permits can see or download the information. In the off-chain phase, the file uploaded to IPFS gets a unique multi-cash value that acts as a file identification. This multi-hash value was stored in the blockchain, ensuring that only those who have access rights can access the information through verification on the blockchain. Thus, the confidentiality of information is guarded from the unauthorized party.

2. Integrity
   The integrity of data is guaranteed by the use of blockchain and IPFS technology. Every file uploaded to IPFS is given a multi-hash value that not only acts as an address but also as a checksum to verify the integrity of the file. Each change in the file will produce a different multi-cash value so that every modification effort can be detected easily. In addition, the recording of transactions on the blockchain ensures that all actions taken on data can be audited and validated, maintaining the integrity of information during the data-sharing process. Every transaction carried out between the CSIRT Sender and Recipient was recorded in the blockchain, which cannot be changed or deleted, ensuring that a complete audit trail is available for all information-sharing activities.

3. Availability
   The availability of information in this sharing mechanism was improved by the use of IPFS, which was a distributed file storage system. IPFS allows data to be distributed in many nodes, thereby reducing the risk of loss of data due to server failure or distributed denial of service (DDOS). In the on-chain phase, the use of blockchain ensures that transactions and information remain continuous because the blockchain is decentralized and redundant. By using a combination of blockchain and IPFS technology, this information-sharing mechanism ensures that data is always available for the authorities at any time needed, even in the condition of network failure or cyber-attacks.

4. CONCLUSION

This study has succeeded in designing and implementing a mechanism for sharing cyber safety information based on Blockchain Hyperledger Composer and InterPlanetary File System (IPFS) technology, which is optimized for use by CSIRT in Indonesia. The test results indicate that this system can maintain the confidentiality, integrity, and availability of information well.

In the confidentiality aspect, the use of blockchain and IPFS technology only those who have access permits can access the information. The integrity of information is maintained through the recording of each transaction in the blockchain that cannot be changed, as well as the verification of file integrity through multi-hash values on IPFS. The availability of information is also increased by IPFS distributed storage, reducing the risk of data loss. Performance test results show that this system has a latency and throughput that is quite stable and acceptable, both in the upload process and download files. This shows that the system can handle high demand efficiently. Further research can be focused on performance optimization with various hardware and software configurations, as well as trials on a larger scale to ensure efficiency in a more dynamic environment.

ACKNOWLEDGMENTS

This work was fully funded by the Ministry of Communication and Information Technology, Indonesia – Domestic Masters Scholarship Program.

REFERENCES

[1] Chatterjee, R. S. and K. (2020). Blockchain for Cybersecurity Incident Data Sharing. *J Cybersecur*, *12*, 45–67.
[2] Badan Siber dan Sandi Negara. (2023). *Keamanan Siber Indonesia 2022*. https://www.bssn.go.id/
[3] P. Sharma, N. Kumar, and J. H. P. (2022). Blockchain-based Decentralized Framework for Security and Privacy Management in IoT. *Journal of Network and Computer Applications*, *126*, 102–115.
[4] Q. Liu, P. Li, C. Liu, and H. J. (2022). Enhancing Data Privacy and Security in Cloud Computing Using

Blockchain. *Future Generation Computer Systems*, *107*, 102–115.
[5] Wang, S., Zhang, Y., & Zhang, Y. (2018). A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems. *IEEE Access*, *6*, 38437–38450. https://doi.org/10.1109/ACCESS.2018.2851611
[6] M. Conti, R. Kumar, C. Lal, and S. R. (2021). A Survey on Blockchain-Based Threat Intelligence Sharing in Cybersecurity. *IEEE Communications Surveys & Tutorials*, *23*(1), 44–56.
[7] Zhang, Y., Kasahara, S., Shen, Y., Jiang, X., & Wan, J. (2019). Smart contract-based access control for the Internet of Things. *IEEE Internet of Things Journal*, *6*(2), 1594–1605. https://doi.org/10.1109/JIOT.2018.2847705
[8] Chen, G., Xu, B., Lu, M., & Chen, N.-S. (2018). Exploring blockchain technology and its potential applications for education. *Smart Learning Environments*, *5*(1). https://doi.org/10.1186/s40561-017-0050-x
[9] Guo, Y., & Liang, C. (2016). Blockchain application and outlook in the banking industry. *Financial Innovation*, *2*(1). https://doi.org/10.1186/s40854-016-0034-9
[10] J. Lee, S. Kim, and H. P. (2024). Hyperledger Fabric in Manufacturing: Enhancing Security and Collaboration. *Int J Prod Res*, *62*(4), 1342–1358.
[11] J. Sun, J. Yan, and K. Z. Z. (2023a). Blockchain-based Secure Data Sharing for Educational Institutions. *IEEE Transactions on Learning Technologies*, *16*(1), 25–36.
[12] Lee, J., Magazine, M. P.-I. C. E., & 2017, U. (2017). How the blockchain revolution will reshape the consumer electronics industry. *Ieeexplore.Ieee.Org*. https://ieeexplore.ieee.org/abstract/document/7948864/
[13] EU Blockchain Observatory and Forum. (2022). *Blockchain Applications in the Energy Sector*. 53. https://www.eublockchainforum.eu/sites/default/files/reports/EUBOF-Thematic_Report_Energy_Sector_0.pdf
[14] X. Huang, Y. Yuan, and F. W. (2023). Blockchain Technology for IoT: Research Issues and Challenges. *Future Generation Computer Systems*, *92*, 357–375.
[15] Yuan, Y., & Wang, F. Y. (2016). Towards blockchain-based intelligent transportation systems. *IEEE Conference on Intelligent Transportation Systems, Proceedings, ITSC*, 2663–2668. https://doi.org/10.1109/ITSC.2016.7795984
[16] Shah, V. P. and M. (2022). Blockchain for Healthcare: Enhancing Security and Privacy. *Journal of Information Security and Applications*, *50*, 102–115.
[17] Malik, R. A. and H. (2022). Blockchain in Telecommunications: Use Cases and Future Trends. *Telecommun Syst*, *73*(2), 245–258.
[18] Q. K. Nguyen. (2023). Blockchain in Education: Opportunities and Challenges. *Educ Inf Technol (Dordr)*, *24*(5), 3233–3251.
[19] Chen, Q. Z. and H. (2023). Blockchain for Government: Challenges and Opportunities. *Gov Inf Q*, *40*(1), 1–10.
[20] Wu, X. L. and X. (2024). Blockchain in the Technology Sector: Benefits and Challenges. *Journal of Strategic Information Systems, 33*(1), 1–15.
[21] Lin, J. W. and C. (2023). Blockchain for Retail: A Comprehensive Survey. *Journal of Retailing and Consumer Services*, *61*, 102–113.
[22] Zhang, S. C. and X. (2024). Blockchain for Finance: Current Trends and Future Directions. *Journal of Financial Technology*, *8*(3), 234–245.
[23] Singh, R. G. and A. (2023). Blockchain in Automotive Industry: Challenges and Opportunities. *J Ind Inf Integr*, *22*, 1–10.
[24] Yasin, H. H. and A. (2022). Blockchain in Logistics: Challenges and Future Trends. *Journal of Business Logistics*, *39*(1), 145–158.
[25] Gerard Sylvester. (2019). Blockchain for Agriculture: Opportunities and Challenges. *Fao*, *4*(1), 88–100. https://www.ictworks.org/wp-content/uploads/2019/02/Blockchain-Agriculture.pdf
[26] Phillips, G., & Kiçeci, İ. (n.d.). *Blockchain in Energy Sector*. https://files.cryptoindexseries.com/cis-files/sector_info/CIS Report- Energy.pdf
[27] Zia, S. K. and T. (2024). Blockchain for Transportation: Current Trends and Future Directions. *IEEE Transactions on Intelligent Transportation Systems*, *25*(1), 123–135.
[28] Androulaki, E., Cachin, C., Ferris, C., Barger, A., & Christidis, K. (2022). Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains. *EuroSys '18: Proceedings of the Thirteenth EuroSys Conference*, 125–147.
[29] L. Chen, L. Xu, Z. Gao, and S. L. (2022). Exploring the Use of Hyperledger Fabric for Secure Data Sharing in Industrial IoT. *IEEE Trans Industr Inform*, *18*(1), 487–497.
[30] Yaqoob, I., Salah, K., Jayaraman, R., & Al-Hammadi, Y. (2022). Blockchain for healthcare data management: opportunities, challenges, and future recommendations. *Neural Computing and Applications*, *34*(14), 11475–11490. https://doi.org/10.1007/s00521-020-05519-w

[31] Y. Guo, C. Liang, and H. W. (2023). Blockchain Application in Cybersecurity: A Survey. *Comput Secur*, *102*, 102489.
[32] D. Kim, S. Lee, and T. K. (2023). Blockchain for Public Sector Data Sharing: Benefits and Challenges. *Gov Inf Q*, *40*(1), 101589.
[33] J. Sun, J. Yan, and K. Z. Z. (2023b). Blockchain-based Secure Data Sharing for Medical Cyber-Physical Systems. *IEEE Trans Netw Sci Eng*, *7*(1), 234–245.
[34] X. Wang, Y. Li, and J. Z. (2024). Enhancing Cybersecurity in the Tech Industry through Hyperledger Fabric'. *Journal of Information Security and Applications*, *63*, 103028.
[35] S. K. Kim, H. S. Lee, and S. Y. K. (2024). Blockchain Technology for Security and Privacy in the Internet of Things: A Survey. *IEEE Internet Things J*, *12*, 932–944.
[36] A. Martinez, S. Thompson, and J. R. (2023). Ensuring Data Integrity in the Energy Sector with Hyperledger Fabric. *Energy Informatics*, *6*(1), 47–59. https://www.apaccioutlook.com/news/ensuring-data-integrity-in-the-era-of-iot-nwid-5565.html
[37] W. Huang, X. Zhou, and L. Y. (2023). Increasing Transparency and Security in Transportation with Hyperledger Fabric. *Transp Rev*, *43*(2), 165–182.
[38] Q. Yuan, H. Sun, and F. W. (2024). Reducing Fraud Risk and Increasing Trust in Banking through Blockchain and Hyperledger Fabric. *Financial Innovation*, *10*(1), 98–115.