ISSN: 2477-5126
e-ISSN: 2548-9356

# Desain dan Analisis Sistem CyberShare Menggunakan Four Node Interplanetary File System (IPFS)

**Tony Haryanto[1*)], Kalamullah Ramli[2]**
[1,2]Departemen Teknik Elektro, Fakultas Teknik, Universitas Indonesia, Indonesia
[1,2]Jln. Margonda Raya, Kota Depok, 16425, Indonesia
email: [1]tony.haryanto@ui.ac.id, [2]kalamullah.ramli@ui.ac.id

***Abstract —*** *Cybersecurity information sharing is a proactive and collaborative measure in enhancing organizational security by exchanging cybersecurity information using a centralized repository service. However, in practice, the use of centralized services poses a threat to distributed denial-of-service (DDoS) attacks which can result in system failure and cause single point of failure as well as man-in-the-middle (MITM) attacks which can result in modification of information and theft of exchanged information. This threat results in a lack of user confidence in the confidentiality, integrity, and availability of information. This study proposes the design of a secure cybersecurity information sharing (CyberShare) system using a private interplanetary file system (IPFS) network as a decentralized information storage. Unlike centralized storage which only has a single-node, CyberShare systems use four-node IPFS interconnected with swarm keys as authentication keys. This system allows users to store and share information from the sender to the recipient of information, avoiding dependence on a central server and reducing server load. The results of the analysis show that the proposed CyberShare system can guarantee the confidentiality, integrity, and availability of cyber security information. CyberShare systems can enhance the security of the information exchanged so that organizations can safely share and utilize cybersecurity information.*

***Abstrak –*** Berbagi informasi keamanan siber atau *cybersecurity information sharing* adalah langkah proaktif dan kolaboratif dalam meningkatkan keamanan organisasi dengan bertukar informasi keamanan siber menggunakan layanan penyimpanan tersentralisasi. Namun pada praktiknya, penggunaan layanan tersentralisasi memiliki ancaman terhadap serangan *distributed denial-of-service* (DDoS) yang dapat mengakibatkan kegagalan pada sistem dan menyebabkan *single point of failure* serta serangan *man-in-the-middle* (MITM) yang dapat mengakibatkan modifikasi informasi dan pencurian informasi yang dipertukarkan. Ancaman ini mengakibatkan kurangnya kepercayaan pengguna terhadap kerahasiaan, keutuhan, dan ketersediaan informasi. Penelitian ini mengusulkan rancangan sistem *secure cybersecurity information sharing* (CyberShare) menggunakan jaringan pribadi *interplanetary file system* (IPFS) sebagai penyimpanan informasi secara terdesentralisasi. Tidak seperti penyimpanan tersentralisasi yang hanya memiliki *single-node*, sistem CyberShare menggunakan IPFS *four-node* yang saling terhubung dengan *swarm key* sebagai kunci autentikasi. Sistem ini memungkinkan pengguna untuk menyimpan dan berbagi informasi dari pengirim ke penerima informasi, menghindari ketergantungan pada server pusat dan mengurangi beban server. Hasil analisis menunjukkan bahwa sistem CyberShare yang diusulkan dapat menjamin kerahasiaan, keutuhan, dan ketersediaan informasi keamanan siber. Sistem CyberShare dapat meningkatkan keamanan informasi yang dipertukarkan sehingga organisasi dapat berbagi dan memanfaatkan informasi keamanan siber dengan aman.

***Kata Kunci* – cybersecurity, information sharing, ipfs**

## I. PENDAHULUAN

Setelah pandemi COVID-19 melanda dunia internasional, jumlah serangan siber semakin meningkat[1]. Hal tersebut menjelaskan bahwa penerapan teknik keamanan siber yang hanya mengandalkan teknologi saja tidak cukup untuk melindungi organisasi dari serangan siber yang canggih [2]. Oleh karena itu, dibutuhkan teknik *proactive security*, yang merupakan teknik pengamanan yang bertujuan untuk mencegah serangan siber dan mendeteksinya sejak dini. Teknik ini menggunakan teknologi dan proses keamanan yang lebih canggih dan berorientasi pada pencegahan dan deteksi dini serangan siber, bukan hanya merespons setelah serangan terjadi [3]. Salah satu cara yang dapat digunakan adalah dengan berbagi informasi keamanan siber atau *cybersecurity information sharing* yang berasal dari dalam organisasi maupun dari luar organisasi [4]. Berbagi informasi keamanan siber dalam organisasi dapat membantu pemangku kepentingan dalam organisasi untuk memanfaatkan sumber daya keamanan siber dengan membuat keputusan yang tepat dalam merumuskan teknik pertahanan, deteksi, strategi, dan mitigasi ancaman siber [5]. Para pemangku kepentingan yang menerima informasi keamanan siber kemudian menggunakannya untuk meningkatkan keamanan organiasinya dan dapat memberikan perlindungan kepada pemangku kepentingan lainnya dengan berbagi informasi untuk mencegah penyebaran ancaman siber tersebut [6].

Penerapan berbagi informasi keamanan siber memanfaatkan penyimpanan tersentralisasi yang merupakan model penyimpanan informasi yang paling umum digunakan di berbagai organisasi [7]. Penyimpanan tersentralisasi memberikan manfaat dalam hal efisiensi dan pengelolaan informasi, karena memudahkan proses penyimpanan dan pengambilan informasi yang cepat [8]. Namun, model ini juga memiliki kelemahan, salah satunya adalah risiko keamanan terhadap serangan terdistribusi *denial-of-service* (DDoS) yang mengakibatkan kegagalan pada sistem dan menyebabkan *single point of failure* atau bencana alam. Serangan berikutnya adalah serangan *Man in The Middle* (MITM) [9] pada transmisi informasi keamanan siber yang menyebabkan entitas yang tidak berwenang menerima informasi keamanan siber dan menyebabkan kebocoran informasi. Entitas ini dapat merusak keutuhan dan mengubah informasi, yang kemudian diteruskan kembali ke penerima sehingga penerima memperoleh informasi yang dimodifikasi tersebut. Oleh

*) **penulis korespondensi**: Tony Haryanto
Email: tony.haryanto@ui.ac.id

karena itu diperlukan teknologi penyimpanan terdistribusi dan terdesentralisasi yang dapat menjamin kerahasiaan, keutuhan dan ketersedian infomasi.

*InterPlanetary File System* (IPFS) adalah protokol jaringan *peer-to-peer* (P2P) yang memungkinkan pengguna untuk menyimpan informasi secara terdesentralisasi dan mengambil file dari jaringan yang didistribusikan dengan menghindari ketergantungan pada server pusat dan mengurangi beban server [10]. IPFS menggunakan sistem distribusi terdesentralisasi yang memungkinkan file disimpan pada banyak node dan dapat diakses secara aman dan cepat. Setiap file diidentifikasi oleh hashnya dan tersedia untuk diambil dari node mana saja di jaringan. Dalam IPFS, setiap node dianggap sama pentingnya dan memiliki kapasitas untuk menyimpan dan mengambil data [11]. Keuntungan menggunakan IPFS antara lain adalah keamanan yang lebih baik, karena file tidak disimpan pada satu lokasi pusat dan tidak dapat dihapus oleh pihak tertentu [12]. Selain itu, IPFS juga menawarkan kecepatan transfer file yang lebih cepat karena file dapat diambil dari node yang paling dekat dengan pengguna. IPFS juga mendukung versi berbeda dari suatu file, sehingga memungkinkan pengguna untuk mengakses versi lama dan baru dari file yang sama [13].

Oleh karena itu, penelitian ini mengusulkan rancangan sistem *secure cybersecurity information sharing* (CyberShare) atau berbagi informasi keamanan siber secara aman yang memanfaatkan jaringan pribadi IPFS empat node sebagai penyimpanan file secara terdesentralisasi. Hasil analisis menunjukkan bahwa sistem CyberShare mampu menjamin ketersediaan, keutuhan dan kerahasiaan informasi keamanan siber sehingga organisasi dapat berbagi informasi dengan aman dan memanfaatkan informasi keamanan siber.

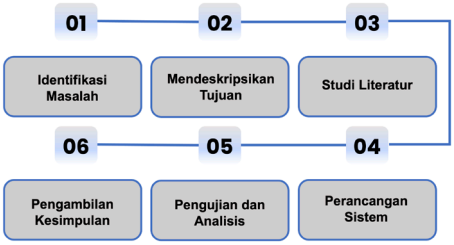
## II. PENELITIAN YANG TERKAIT

Penelitian sebelumnya membahas mengenai usulan protokol berbagi informasi insiden siber yang berfokus pada perlindungan informasi rahasia yang dibagikan melalui penyimpanan tersentralisasi diantara organisasi sektoral [14]. Penelitian sebelumnya juga membahas mengenai usulan skema berbagi informasi pemerintah untuk kerjasama lintas departemen dengan menggunakan teknologi blockchain [15]. Terdapat penelitian sebelumnya juga yang membahas model berbagi informasi antar pemerintah dengan menggunakan teknologi blockchain [16]. Selain itu, terdapat penelitian yang berfokus pada kolaborasi keamanan siber dengan model aktivitas operasi keamanan siber dan model kematangan berbagi informasi intelijen ancaman siber antar organisasi sectoral [17]. Berbagi informasi keamanan siber pada penelitian sebelumnya dilakukan menggunakan model komunikasi *peer to peer* (P2P) melalui layanan penyimpanan tersentralisasi karena memiliki fleksibilitas dan kemudahan bagi pemerintah yang terlibat [18]. Layanan tersentralisasi memiliki beberapa layanan, termasuk penyimpanan *cloud* [19]. Namun, dalam praktiknya, penyimpanan tersentralisasi pada penerapan berbagi informasi keamanan siber memiliki berbagai ancaman yang dapat memengaruhi komponen yang membentuk infrastruktur organisasi seperti jaringan dan komunikasi [20]. Sistem manajemen penyimpanan tersentralisasi melibatkan otoritas pusat untuk mengontrol sejumlah besar informasi. Hal tersebut mengakibatkan kurangnya kepercayaan pengguna terhadap kerahasiaan, keutuhan, dan ketersediaan informasi [21].

Berdasarkan penelitian sebelumnya yang terkait dengan adanya ancaman keamanan informasi terhadap berbagi informasi keamanan siber yang menggunakan layanan tersentralisasi, maka menjadi penting untuk melanjutkan pengembangan penelitian terhadap berbagi informasi keamanan siber dengan menggunakan layanan terdesentralisasi yang aman. Layanan terdesentralisasi tersebut harus dapat menjamin ketersediaan, keutuhan, dan kerahasiaan informasi. Dalam konteks ini, diperlukan upaya untuk menganalisis faktor keamanan sistem berbagi informasi yang terdesentralisasi. Dengan demikian, penelitian selanjutnya diharapkan dapat menghasilkan solusi yang dapat memenuhi kebutuhan keamanan pada penerapan berbagi informasi keamanan siber.

## III. METODE PENELITIAN

Tahapan yang digunakan dalam penelitian ini antara lain: identifikasi permasalahan, mendeskripsikan tujuan, studi literatur, perancangan sistem, pengujian dan analisis serta pengambilan kesimpulan [22]. Tahapan penelitian diilustrasikan pada Gambar 1 dengan rincian sebagai berikut:




Gbr 1. Tahapan Penelitian

1. Identifikasi Permasalahan

   Pada tahap ini dilakukan identifikasi terhadap permasalahan yang melatarbelakangi penelitian ini. Permasalahan tersebut yaitu terkait dengan penerapan *Cybersecurity Information Sharing* (CIS) yang memanfaatkan penyimpanan tersentralisasi pada organisasi. Namun, dalam praktiknya, penyimpanan tersentralisasi pada penerapan CIS memiliki kerawanan terhadap serangan *distributed denial-of-service (DDoS)* yang dapat mengakibatkan *single point of failure* dan *Man in The Middle* (MITM) yang dapat mengakibatkan modifikasi informasi. Serangan tersebut mengakibatkan kurangnya kepercayaan pengguna terhadap kerahasiaan, keutuhan, dan ketersedian informasi.
2. Mendeskripsikan Tujuan

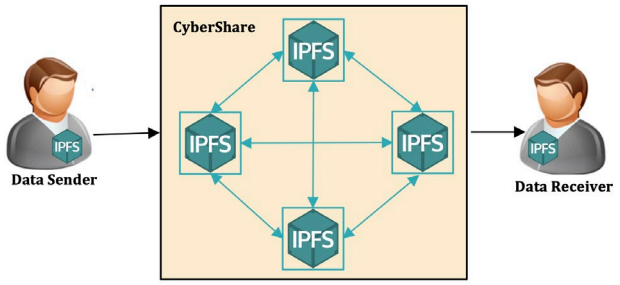
   Dalam penelitian ini, peneliti mengembangkan sebuah rancangan berbagi informasi keamanan siber yang aman untuk menjamin kerahasiaan, keutuhan dan ketersediaan informasi. Sistem ini dirancang dengan menerapkan jaringan pribadi *interplanetary file system* (IPFS) yang dapat menjamin kerahasiaan, keutuhan dan ketersediaan informasi keamanan siber. Hasil penelitian ini diharapkan dapat dimanfaatkan oleh analis keamanan siber untuk berbagi informasi keamanan siber.
3. Studi Literatur

   Pada tahap ini dilakukan studi literatur berkaitan dengan penelitian yang terdahulu terkait berbagi informasi

keamanan siber di berbagai organisasi, pemanfaatan *interplanetary file system* sebagai solusi *single point of failure.*

4. Perancangan Arsitektur Sistem

Perancangan dilakukan berdasarkan rekomendasi yang didapatkan pada studi literatur, agar penelitian ini dapat menjadi solusi dari permasalahan yang telah didefinisikan. Tujuan dari rancangan sistem ini adalah untuk menghasilkan sistem penyimpanan dan berbagi informasi keamanan siber yang mampu menjamin ketersediaan, keutuhan dan kerahasiaan informasi kemanan siber yang disimpan dan dipertukarkan antar organisasi. Untuk mendukung tujuan tersebut, dilakukan perancangan sistem dengan menggunakan *Interplanetary File System* (IPFS). IPFS adalah sebuah protokol jaringan *peer to peer* untuk menyimpan data di sebuah sistem terdistribusi. Tidak seperti penyimpanan file di *server*, IPFS mendistribusikan file tersebut ke berbagai *node* di IPFS. Sementara sistem file lain menggunakan alamat berbasis lokasi untuk mencari file, IPFS menggunakan alamat berbasis konten di mana alamat file didasarkan pada hash konten file [23]. IPFS juga menggunakan tabel hash terdistribusi untuk mengetahui di mana menemukan data atau jalurnya yang mengarah lebih dekat ke data [24]. Pada arsitektur sistem ini, IPFS digunakan sebagai penyimpanan file yang terdesentralisasi yang memungkinkan file tersebar kedalam beberapa *node* yang berada dalam jaringan IPFS. Teknologi-teknologi tersebut dikombinasikan kedalam sebuah arsitektur sistem CyberShare seperti yang dirancang pada gambar 2 sebagai berikut:




Gbr 2. Desain Arsitektur Sistem CyberShare

Gambar diatas mengilustrasikan arsitektur sistem CyberShare. Untuk berinteraksi dengan sistem ini, setiap pengguna harus terhubung ke jaringan pribadi IPFS. Pengguna CyberShare terdiri dari *data sender* dan *data receiver*, Setiap pengguna memiliki identitas khusus yaitu *peer identity* (PeerID). PeerID merupakan identitas unik dari suatu *node* dalam jaringan *peer-to-peer.* PeerID berfungsi sebagai pengidentifikasi antar sesama pengguna dalam satu jaringan. Dalam arsitektur sistem ini, PeerID digunakan agar pengguna dapat berinteraksi dengan pengguna lain dalam jaringan pribadi IPFS. CyberShare memiliki perintah untuk mengunduh informasi keamanan siber dan menggunggah nilai hash dari informasi keamanan siber kedalam jaringan pribadi IPFS. Informasi keamanan siber dan nilai hash hasil dari transaksi hanya didistribusikan antar pengguna melalui jaringan pribadi IPFS. Rancangan Arsitektur ini, membutuhkan beberapa entitas dan teknologi. Berikut adalah entitas dan fungsi yang digunakan dalam membangun arsitektur sistem CyberShare, seperti tercantum dalam Tabel 1.

TABEL 1. ENTITIAS DAN FUNGSINYA

| Entitas | Fungsi |
|---|---|
| *Data Sender* | Entitas yang dapat menyimpan informasi di dalam jaringan IPFS. *Data Sender* juga dapat mengirim dan berbagi informasi yang disimpan di dalam jaringan IPFS dengan *Data Receiver* menggunakan Cybershare |
| *Data Receiver* | Entitas yang menerima dan memanfaatkan informasi yang telah dibagikan oleh *Data Sender* kepada menggunakan Cybershare |
| CyberShare | Platform simulasi penyimpanan dan berbagi informasi keamanan siber yang terhubung kedalam jaringan pribadi 4 node IPFS. Entitas yang ingin bergabung kedalam jaringan IPFS harus membangkitkan *swarmkey* yang sama |

5. Pengujian dan Analisis

Pengujian sistem dilakukan dengan membuat lingkungan virtual yang mirip dengan lingkungan nyata, dimana sistem atau aplikasi dapat diuji secara terisolasi atau tanpa mempengaruhi lingkungan nyata yang sebenarnya. Simulasi sistem CyberShare dijalankan dengan menggunakan perangkat lunak virtualisasi VMware 12.2.4, dimana VMware dibuat dan dijalankan di atas sistem operasi utama. Dalam simulasi sistem CyberShare, VMware dibuat untuk menjalankan empat sistem operasi Linux yang mewakili empat *node* yang berbeda dengan spesifikasi sistem operasi seperti tabel 2, sehingga memungkinkan pengujian dan pengembangan aplikasi yang lebih aman dan terisolasi. Selain itu, simulasi sistem CyberShare juga dapat digunakan untuk menguji keamanan informasi tanpa mengganggu sistem operasi utama atau lingkungan sebenarnya.

TABEL 2. SPESIFIKASI *NODE*

| Node | Spesifikasi | |
|---|---|---|
| Ipfs1 | Processor | 2 Processor Core |
| | Memory | 4096 MB |
| | OS | Linux 5.15.0-52-generic ubuntu 20.04.5 LTS |
| | Storage | 66.2 GB |
| Ipfs2 | Processor | 2 Processor Core |
| | Memory | 4096 MB |
| | OS | Linux 5.15.0-52-generic ubuntu 20.04.5 LTS |
| | Storage | 78.8 GB |
| Ipfs3 | Processor | 2 Processor Core |
| | Memory | 4096 MB |
| | OS | Linux 4.15.0-196-generic ubuntu 18.04.06 LTS |
| | Storage | 43.2 GB |
| Ipfs4 | Processor | 2 Processor Core |
| | Memory | 4096 MB |
| | OS | Linux 4.15.0-196-generic ubuntu 18.04.06 LTS |
| | Storage | 13.1 GB |

Pada tahap ini dilakukan simulasi pengujian sistem secara virtual dengan membuat sistem Cybershare menggunakan empat node IPFS yang saling terhubung dengan menggunakan *swarm key* yang identik untuk setiap node. Simulasi pengujian dilakukan dengan menggunakan metode pengujian non-fungsional meliputi pengujian keamanan informasi yaitu uji kerahasiaan, keutuhan dan ketersediaan informasi keamanan siber pada hasil

rancangan arsitektur sistem dengan memanfaatkan IPFS. Tujuan utama dari pengujian keamanan informasi adalah untuk mengidentifikasi kerentanan atau celah keamanan dalam sistem dan melindungi data dan informasi sensitif dari akses yang tidak sah. Simulasi pengujian dilakukan pada *virtual machine* berdasarkan skenario yang ditentukan. Selanjutnya, dilakukan analisis dari hasil pengujian sistem tersebut sebagai dasar pengambilan kesimpulan dan rekomendasi penelitan selanjutnya.

6. Pengambilan Kesimpulan

Tahap akhir adalah melakukan pengambilan kesimpulan dari hasil penelitian dan menentukan rekomendasi serta saran untuk pengembangan penelitian selanjutnya.

## IV. HASIL DAN PEMBAHASAN

Bab ini berisikan hasil pengujian dan pembahasan berupa analisis keamanan informasi meliputi ketersediaan, keutuhan dan kerahasiaan informasi keamanan siber yang diperoleh dan disajikan sebagai berikut:

1. Hasil Pengujian

Dalam rangka menguji ketersediaan file, dilakukan percobaan yang dirancang untuk menguji kemampuan sistem dalam menghadapi situasi yang tidak terduga, yaitu saat salah satu *node* mengalami kegagalan atau nonaktif. Dalam pengujian ketersediaan file dengan satu node nonaktif, penulis mencoba mengunggah file dari *node* Ipfs1 kedalam jaringan pribadi IPFS. Kemudian penulis mencoba untuk mengunduh file tersebut dari semua *node* termasuk *node* Ipfs1. Namun pada percobaan ini, dikondisikan salah satu *node* yaitu *node* Ipfs4 dalam keadaan nonaktif sedangkan *node* yang lain dalam keadaan aktif. Hasil pengujian ketersediaan file dengan satu dari empat *node* nonaktif terlihat pada tabel 3.

TABEL 3. HASIL PENGUJIAN KETERSEDIAAN FILE

| Node | IP Address | Status | Percobaan | Hasil |
|---|---|---|---|---|
| Ipfs1 | 172.16.55.140 | Aktif | Download | Berhasil |
| Ipfs2 | 172.16.55.141 | Aktif | Download | Berhasil |
| Ipfs3 | 172.16.55.142 | Aktif | Download | Berhasil |
| Ipfs4 | 172.16.55.143 | Nonaktif | Download | Gagal |

Pengujian keutuhan file selanjutnya yaitu dengan mengunggah dua file ke dalam CyberShare. Kedua file tersebut mempunyai nama dan ukuran yang mirip (berbeda 5.510 byte) namun sedikit mengalami perubahan pada kontennya. Sesuai dengan prinsip fungsi hash, maka CyberShare dapat dengan mudah mengidentifikasi kedua file tersebut dengan keluaran hash yang berbeda, karena terdapat perbedaan konten pada file tersebut. Dalam CyberShare, pengguna dapat memverifikasi integritas setiap file dengan menggunakan nilai hash yang dihasilkan oleh fungsi hash. Hasil dari pengujian dapat dilihat pada Tabel 4.

TABEL 4. HASIL PENGUJIAN KEUTUHAN FILE

| Name File | Volume | Hash File |
|---|---|---|
| CI_lockbit.pdf | 1.711.649 bytes | QmccehyfhaQmpP35D91a7G25i3yKfdzro6RH9mhGnWvA3n |
| CI_lockbitx.pdf | 1.717.159 bytes | QmZuCsUJAcvcijgkWasrKwGbcnPYM5WgCjiSAtcTLTRRC8 |

Dalam pengujian kerahasiaan, terdapat kemungkinan untuk mengunduh file dari *node* klien IPFS lain di luar jaringan pribadi atau bahkan dari pengguna yang belum terdaftar dalam jaringan pribadi IPFS. Dalam hal ini, IPFS yang digunakan dari luar jaringan pribadi memiliki *swarm key* yang berbeda dari *swarm key* yang digunakan dalam jaringan pribadi IPFS. Meskipun demikian, pengguna dari luar jaringan pribadi IPFS mempunyai nilai hash yang valid dari file yang akan diunduh di jaringan pribadi IPFS. Berdasarkan hasil pengujian kerahasiaan yang ditunjukkan pada Tabel 5.

TABEL 5. HASIL PENGUJIAN KERAHASIAN FILE

| Jaringan | Valid Hash | Percobaan | Hasil |
|---|---|---|---|
| Pengguna dalam Jaringan Pribadi IPFS | QmV4asVwV9owLkNJe8o7ZPLAiZhfetonxngc4X96TFQ7Db | Download | Berhasil |
| Pengguna dalam Jaringan Publik IPFS | QmV4asVwV9owLkNJe8o7ZPLAiZhfetonxngc4X96TFQ7Db | Download | Gagal |

2. Analisis

Dalam rangka untuk mengevaluasi ketersediaan, keutuhan, dan kerahasiaan file dalam sistem CyberShare, dilakukan beberapa pengujian dengan berbagai skenario yang mungkin terjadi. pengujian ketersediaan file dilakukan dengan cara menonaktifkan salah satu node dalam jaringan pribadi IPFS yang digunakan oleh sistem. Hal ini dilakukan untuk mensimulasikan kegagalan sistem atau serangan siber. Dalam hasil pengujian, ditemukan bahwa data masih dapat diakses melalui *node* yang masih aktif di dalam jaringan pribadi IPFS. Hal ini menunjukkan bahwa sistem penyimpanan CyberShare yang menggunakan teknologi IPFS dapat memberikan tingkat redundansi yang tinggi dan tidak tergantung pada satu titik pusat yang rentan terhadap serangan atau kegagalan sistem serta memastikan ketersediaan data dalam situasi yang sulit.

Selanjutnya, pengujian keutuhan file dilakukan dengan cara mengunggah file asli dan file modifikasi dengan konten serta ukuran yang hampir sama ke dalam sistem CyberShare. Hasil pengujian menunjukkan bahwa sistem CyberShare dapat mendeteksi perubahan yang dilakukan dalam file, bahkan hanya beberapa byte saja. Hal ini terjadi karena IPFS yang berada dalam sistem CyberShare menggunakan teknologi hash yang dapat memastikan keutuhan informasi dengan membuat hash dari file tersebut dan menyimpan hash tersebut ke dalam jaringan pribadi IPFS. Dengan menggunakan hash ini, IPFS dapat memastikan bahwa data yang disimpan di dalam jaringan tidak dapat dimodifikasi tanpa sepengetahuan pengguna dalam jaringan.

Terakhir, pengujian kerahasiaan file dilakukan dengan cara mensimulasikan akses yang tidak sah dari entitas yang berbahaya dari luar sistem CyberShare. Dalam pengujian ini, dilakukan pengunduhan dari entitas yang belum melakukan pendaftaran sebagai anggota dari jaringan pribadi IPFS dalam sistem CyberShare, serta entitas yang berada pada jaringan yang berbeda dengan jaringan pribadi IPFS namun memiliki nilai hash yang valid atau sesuai dengan file yang diinginkan. Namun,

hasil pengujian menunjukkan bahwa pengunduhan dari entitas yang tidak terdaftar dan entitas diluar jaringan pribadi IPFS tidak dapat dilakukan atau gagal. Hal ini disebabkan oleh fakta bahwa entitas di luar jaringan pribadi IPFS tidak memiliki *swarm key* yang sama dengan anggota jaringan privat IPFS sehingga akses unduh atau unggah file kedalam sistem tidak dapat dilakukan. Oleh karena itu, pengujian tersebut membuktikan bahwa sistem CyberShare dapat memberikan tingkat kerahasiaan yang tinggi bagi data yang disimpan di dalamnya.

## V. KESIMPULAN

Berdasarkan analisis hasil pengujian pada penelitian ini, dapat disimpulkan bahwa:

1. Perancangan dan analisis keamanan informasi sistem *secure cybersecurity information sharing* (CyberShare) dengan menggunakan jaringan pribadi *interplanetary file system* (IPFS) empat node sebagai penyimpanan informasi keamanan siber yang terdesentralisasi dapat menjadi solusi untuk meningkatkan keamanan siber dan kepercayaan pengguna terhadap kerahasiaan, keutuhan, dan ketersediaan informasi. Sehingga organisasi dapat berbagi dan memanfaatkan informasi keamanan siber dengan aman.
2. Penerapan CyberShare yang menggunakan penyimpanan terdesentralisasi dapat dijadikan sebagai solusi masalah privasi yang muncul akibat dari adanya otoritas tunggal penyedia layanan pada penyimpanan tersentralisasi. pada penyimpanan tersentralisasi, informasi dapat dimodifikasi, dibagikan atau dimanfaatkan oleh otoritas tunggal tanpa sepengetahuan atau persetujuan dari pemilik informasi. Sebaliknya, pada penyimpanan terdesentralisasi, informasi tidak dapat dimodifikasi dan dibagikan tanpa sepengetahuan pemilik informasi.
3. Sistem CyberShare masih mempunyai kekurangan antara lain, data transaksi antara *data sender* dan *data receiver* tidak dicatat dalam sistem, sehingga rawan penyangkalan terhadap data yang dikirim ataupun yang diterima, maka perlu dilakukan pengembangan dengan menggunakan teknologi blockchain sebagai sistem pencatatan transaksi yang *immutable* antara *data sender* dan *data receiver*, sehingga terdapat bukti otentik anti-penyangkalan terhadap transaksi yang dilaksanakan antara kedua belah pihak.

## UCAPAN TERIMA KASIH

Ucapan terima kasih penulis kepada Kementerian Komunikasi dan Informatika yang telah membantu dan memberikan dukungan finansial pada penelitian ini.

## DAFTAR PUSTAKA

[1] A. Lamssaggad, N. Benamar, A. S. Hafid, and M. Msahli, "A Survey on the Current Security Landscape of Intelligent Transportation Systems," *IEEE Access*, vol. 9, no. Vlc, pp. 9180–9208, 2021, doi: 10.1109/ACCESS.2021.3050038.

[2] D. P. Fidler, "Cybersecurity in the Time of COVID-19," *Counc. Foreign Relations*, no. 2020, pp. 7–9, 2020, [Online]. Available: https://www.cfr.org/blog/cybersecurity-time-covid-19.

[3] D. Y. Perwej, S. Qamar Abbas, J. Pratap Dixit, D. N. Akhtar, and A. Kumar Jaiswal, "A Systematic Literature Review on the Cyber Security," *Int. J. Sci. Res. Manag.*, vol. 9, no. 12, pp. 669–710, 2021, doi: 10.18535/ijsrm/v9i12.ec04.

[4] A. B. Ajmal, M. A. Shah, C. Maple, M. N. Asghar, and S. U. Islam, "Offensive Security: Towards Proactive Threat Hunting via Adversary Emulation," *IEEE Access*, vol. 9, pp. 126023–126033, 2021, doi: 10.1109/ACCESS.2021.3104260.

[5] A. O. David and A. E. Akinrayo, "Summary of Cyber Threat Intelligence," no. February 2023, doi: 10.2015/IJIRMF/202203006.

[6] F. Cremer *et al.*, "Cyber risk and cybersecurity: a systematic review of data availability," *Geneva Pap. Risk Insur. Issues Pract.*, vol. 47, no. 3, pp. 698–736, 2022, doi: 10.1057/s41288-022-00266-6.

[7] Y. Li and Q. Liu, "A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments," *Energy Reports*, vol. 7, no. xxxx, pp. 8176–8186, 2021, doi: 10.1016/j.egyr.2021.08.126.

[8] H. Dandan, Z. Yajuan, L. Junfeng, L. Chen, X. Mo, and S. Zhihai, "Research on centralized data-sharing model based on master data management," *MATEC Web Conf.*, vol. 139, 2017, doi: 10.1051/matecconf/201713900195.

[9] A. Mallik, A. Ahsan, M. M. Z. Shahadat, and J. C. Tsou, "Man-in-the-middle-attack: Understanding in simple words," *Int. J. Data Netw. Sci.*, vol. 3, no. 2, pp. 77–92, 2019, doi: 10.5267/j.ijdns.2019.1.001.

[10] A. Manoj Athreya *et al.*, "Peer-to-Peer Distributed Storage Using InterPlanetary File System," *Adv. Intell. Syst. Comput.*, vol. 1133, no. January, pp. 711–721, 2021, doi: 10.1007/978-981-15-3514-7_54.

[11] H. Gao, Z. Ma, S. Luo, Y. Xu, and Z. Wu, "BSSPD: A Blockchain-Based Security Sharing Scheme for Personal Data with Fine-Grained Access Control," *Wirel. Commun. Mob. Comput.*, vol. 2021, 2021, doi: 10.1155/2021/6658920.

[12] N. Sangeeta and S. Y. Nam, "Blockchain and Interplanetary File System (IPFS)-Based Data Storage System for Vehicular Networks with Keyword Search Capability," *Electron.*, vol. 12, no. 7, 2023, doi: 10.3390/electronics12071545.

[13] R. Zeng, J. You, Y. Li, and R. Han, "An ICN-Based IPFS High-Availability Architecture," 2022.

[14] F. A. Putra, K. Ramli, N. Hayati, and T. S. Gunawan, "Pura-scis protocol: A novel solution for cloud-based information sharing protection for sectoral organizations," *Symmetry (Basel).*, vol. 13, no. 12, pp. 1–22, 2021, doi: 10.3390/sym13122347.

[15] M. Changjun and L. Yi, "Government information sharing scheme for cross-departmental collaboration," *Proc. - 2020 Int. Signal Process. Commun. Eng. Manag. Conf. ISPCEM 2020*, pp. 169–172, 2020, doi: 10.1109/ISPCEM52197.2020.00040.

[16] Y. Zhang, S. Deng, Y. Zhang, and J. Kong, "Research on government information sharing model using blockchain technology," *Proc. - 10th Int. Conf. Inf. Technol. Med. Educ. ITME 2019*, pp. 726–729, 2019, doi: 10.1109/ITME.2019.00166.

[17] M. Hajizadeh, N. Afraz, M. Ruffini, and T. Bauschert, "Collaborative cyber attack defense in SDN networks using blockchain technology," *Proc. 2020 IEEE Conf. Netw. Softwarization Bridg. Gap Between AI Netw. Softwarization, NetSoft 2020*, no. June, pp. 487–492, 2020, doi: 10.1109/NetSoft48620.2020.9165396.

[18] K. Lee, "Comments on 'Secure Data Sharing in Cloud Computing Using Revocable-Storage Identity-Based Encryption,'" *IEEE Trans. Cloud Comput.*, vol. 8, no. 4, pp. 1299–1300, 2020, doi: 10.1109/TCC.2020.2973623.

[19] S. Ghernaouti, L. Cellier, and B. Wanner, "Information sharing in cybersecurity : Enhancing security, trust and privacy by capacity building," *2019 3rd Cyber Secur. Netw. Conf. CSNet 2019*, pp. 58–62, 2019, doi: 10.1109/CSNet47905.2019.9108944.

[20] S. Pal, M. Hitchens, T. Rabehaja, and S. Mukhopadhyay, "Security requirements for the internet of things: A systematic approach," *Sensors (Switzerland)*, vol. 20, no. 20, pp. 1–34, 2020, doi: 10.3390/s20205897.

[21] L. K. V. S. M. A. P. P. Rajalakshmi A, "A Blockchain and IPFS basedframework for secure Research record keeping," *Int. J. Pure Appl. Math.*, vol. 119, no. 15, pp. 1437–1442, 2018.

[22] M. Patel and N. Patel, "Exploring Research Methodology," *Int. J. Res. Rev.*, vol. 6, no. 3, pp. 48–55, 2019.

[23] C. Rahalkar and D. Gujar, "Content Addressed P2P File System for the Web with Blockchain-Based Meta-Data Integrity," *2019 6th IEEE Int. Conf. Adv. Comput. Commun. Control. ICAC3 2019*, pp. 3–6, 2019, doi: 10.1109/ICAC347590.2019.9036792.

[24] M. M. Arer, P. M. Dhulavvagol, and S. G. Totad, "Efficient Big Data Storage and Retrieval in Distributed Architecture using Blockchain and IPFS," *2022 IEEE 7th Int. Conf. Converg. Technol. I2CT 2022*, no. April, 2022, doi: 10.1109/I2CT54291.2022.9824566.