symmetry

MDPI

Article

PURA-SCIS Protocol: A Novel Solution for Cloud-Based Information Sharing Protection for Sectoral Organizations

Fandi Aditya Putra [1], Kalamullah Ramli [1,*], Nur Hayati [1] and Teddy Surya Gunawan [2]

[1] Department of Electrical Engineering, Universitas Indonesia, Depok 10430, Indonesia; fandi.aditya@ui.ac.id (F.A.P.); nur.hayati81@ui.ac.id (N.H.)

[2] Department of Electrical and Computer Engineering, International Islamic University Malaysia, Kuala Lumpur 53100, Malaysia; tsgunawan@iium.edu.my

* Correspondence: kalamullah.ramli@ui.ac.id

Abstract: Over recent years, the incidence of data breaches and cyberattacks has increased significantly. This has highlighted the need for sectoral organizations to share information about such events so that lessons can be learned to mitigate the prevalence and severity of cyber incidents against other organizations. Sectoral organizations embody a governance relationship between cross-sector public and private entities, called public-private partnerships (PPPs). However, organizations are hesitant to share such information due to a lack of trust and business-critical confidentially issues. This problem occurs because of the absence of any protocols that guarantee privacy protection and protect sensitive information. To address this issue, this paper proposes a novel protocol, Putra-Ramli Secure Cyber-incident Information Sharing (PURA-SCIS), to secure cyber incident information sharing. PURA-SCIS has been designed to offer exceptional data and privacy protection and run on the cloud services of sectoral organizations. The relationship between organizations in PURA-SCIS is symmetrical, where the entities must collectively maintain the security of classified cyber incident information. Furthermore, the organizations must be legitimate entities in the PURA-SCIS protocol. The Scyther tool was used for protocol verification in PURA-SCIS. The experimental results showed that the proposed PURA-SCIS protocol provided good security properties, including public verifiability for all entities, blockless verification, data privacy preservation, identity privacy preservation and traceability, and private information sharing. PURA-SCIS also provided a high degree of confidentiality to protect the security and integrity of cyber-incident-related information exchanged among sectoral organizations via cloud services.

Keywords: cyber incident information sharing; secure protocol; sectoral organizations; classified information; privacy preservation; data protection

check for updates

Citation: Putra, F.A.; Ramli, K.; Hayati, N.; Gunawan, T.S. PURA-SCIS Protocol: A Novel Solution for Cloud-Based Information Sharing Protection for Sectoral Organizations. *Symmetry* **2021**, *13*, 2347. https://doi.org/10.3390/sym13122347

Academic Editor: Yu-Chi Chen

Received: 10 November 2021
Accepted: 29 November 2021
Published: 7 December 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Copyright: © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

Sharing cybersecurity information between private sectors is an essential strategy for protecting against the recent increase in data breaches and cyberattacks [1,2]. Sectoral organizations are divided into sectors with similar business processes (e.g., energy, transportation, health, infrastructure, information technology, finance, banking, and government); therefore, sharing cybersecurity information can be done through cloud services because it has flexibility and simplicity for the sectoral organizations involved [3]. In addition, cloud services have various services for exchanging information, including cloud storage.

To enable cyberattack information exchange between organizations, the Information Sharing and Analysis Center (ISAC) platform, which contains classified information, must be adequately secured [4,5]. Therefore, cyber-incident information sharing technology needs to identify the information type and how it is collected, stored, and processed [6]. However, the problem is that various organizations are reluctant to share their cyber-incident information and trust those who have it [7–9].

Recent research on privacy-preserving schemes in data sharing has been carried out by masking the participants' identity or sensitive information [10,11]. The PRivacypreserving and Aggregatable Cybersecurity Information Sharing (PRACIS) technique guarantees private data forwarding and aggregation by privacy preservation into the Structured Threat Information eXpression (STIX) data format as proposed in [12]. In [10], the authors presented a survey related to privacy issues and solutions regarding sharing services. The privacy attribute of data sharing in cloud computing with an efficient Ciphertext-Policy Attribute-Based Encryption (CP-ABE) solution was proposed in [11] and maintains privacy through authority verification. A public auditing scheme to provide privacy in data storage was utilized in [13]. The data exchange protocol, such as keys between entities with accountable optimistic fair exchange protocol, was also utilized in [14]. Data exchange protocols (e.g., cryptographic keys) are protected by other methods, including Non-Commuting Group based on an NP-complete decisional problem as described in [15] and Multi-Stage Quantum in [16]. However, the previous studies do not validate the security requirements of their research by utilizing the formal security validation tools (e.g., Scyther, AVISPA, Tamarin Proofer).

Protecting the identity of data owners during public information sharing was the main focus in [11,13]. In addition, STIX has been used in cyber threat intelligence sharing [12]. Efficient privacy preservation with a certificateless provable data possession scheme in cloud computing solutions was proposed in [17]. Data sharing is carried out on public entities that third parties can audit without downloading the entirety of the information or data. However, that research was not focused on sectoral or private entities. Secure, anonymous authentication and key agreement protocol are also used in the design of multi-server environments as utilized in [18]. However, this research focused on multi-server environments whose utilization is specific to the Internet of Things scheme.

Issues related to data leakage have been discussed in previous studies, where the solution was to provide secure and trusted data protection. Data protection can be achieved using cryptographic techniques to maintain the security and confidentiality of data sharing [11–13,17,19]. Data protection with a novel CP-ABE technique that utilizes a security model and access policy and gate and bilinear maps has been described in [11]. Similarly, the CP-ABE technique for cybersecurity information sharing related to Cyber Threat Intelligence with STIX has been used in [20]. A data integrity auditing scheme with sensitive information hiding, which functions as signatures, has also been presented [19]. In this case, other parties can use the information, but sensitive information on the data owner remains hidden through the encryption feature. The previous research focused on cryptographic techniques but did not utilize secure protocols with claims of security validation.

Securing information storage media, including cloud storage, is another primary concern in information sharing. The studies in [21,22] utilized a fully homomorphic encryption scheme with elliptic curve cryptography to secure private clouds. That previous research focused on the role of fully homomorphic encryption used to protect data stored in cloud storage. However, information stored in cloud storage also needs proof of data ownership. The stored data needs to be verified that it is the original data belonging to the data owner [17,19]. The secure relationship between the host or provider and the user has been proposed in [10]. The provable data possession by public users has also been presented in [17]. Secure remote access of data ownership was proposed in [19]. All previous research focused on generic entities that can access information storage media.

1.1. Contribution

The above-mentioned previous research fails to explicitly address the protection of information-sharing schemes between sectoral organizations for classified information via private cloud services. This paper proposes the novel PURA-SCIS protocol to address this problem, which focuses on providing security and privacy protection by incorporating secure protocols to ensure data confidentiality. Each entity in PURA-SCIS has a symmetrical relationship to maintain the confidentiality of classified cyber incident information exchanged together.

The proposed solution also established proof of data ownership scheme by utilizing certificateless provable data possession, as in [17], which focused on classified information using the Traffic Light Protocol (TLP), such as red or amber [23]. Therefore, the PURA-SCIS protocol focuses on protecting classified information shared via the cloud among sectoral organizations. The entities in PURA-SCIS are considered equal based on the concept of symmetry, including the request and response process between two entities in the protocol.

Several related studies have addressed the issue of information sharing. However, some shortcomings remain. For example, the existing scheme has not considered the privacy protection of the entity's identity (i.e., the sectoral organization). Another is that few studies have discussed information changes and interception that cause data leakage of classified information in information-sharing schemes. Most research also focuses on protecting information in the cloud service of non-sectoral organizations (i.e., the public cloud) without considering the classified information in the private cloud belonging to sectoral organizations. Therefore, the key contributions of this paper are the following:

1. The novel PURA-SCIS protocol is proposed to implement information sharing in both public and private sectoral organizations. In addition, to provide a secure data-sharing scheme, the verifiable data possession of PURA-SCIS is focused on sectoral organizations and considers both privacy preservation and data encryption.
2. A secure protocol audit is designed to guarantee the confidentiality of the cyber incident information-sharing process between entities. Confidentiality is an essential aspect of the PURA-SCIS protocol because classified information in the information-sharing process must be secure from intrusion by unauthorized parties. The code implementation of the PURA-SCIS protocol can be verified on the Github repository.
3. The PURA-SCIS protocol guarantees privacy protection with secure classified information-sharing in the private cloud environment. PURA-SCIS also defines entities that have the authorization to share information in the private cloud. In addition, cryptographic public keys are utilized to protect information exchanged by entities on the network.
4. The PURA-SCIS protocol is designed to address seven security properties, including the cybersecurity ecosystem of cloud-based information storage, communication protocols, and security techniques via secure protocols and security analysis. Information security, especially protecting cyber incident information sharing on cloud networks, was comprehensively analyzed.

1.2. Organization

Section 2 presents secure cyber incident information sharing. The proposed PURA-SCIS protocol is elaborated in Section 3. Section 4 discusses the assessment results for the proposed PURA-SCIS protocol. Finally, Section 5 concludes the paper.

2. Secure Cyber Incident Information Sharing

2.1. Information Sharing and Analysis Center and Sectoral Organizations

Cybersecurity information sharing plays a crucial role in countering cyber-attacks, especially information sharing related to incidents and threats [12]. Cybersecurity information sharing is carried out by Information Sharing and Analysis Centers (ISAC), which are divided into various sectors [23]. The benefits of implementing ISAC are situational awareness, legal protections, trust and strong partnerships with entities, automation, reciprocity, governance flexibility of sharing organizations, membership accessibility (expertise, knowledge, expanded professional networks), reduced cost, improved public reputation, low-risk organizational network, reliable and relevant information, and senior management [24]. ISAC can share information on cyber incidents, such as vulnerabilities, best practices, threats, and cyber risks, with their own organization as well as those at risk of such incidents [25].

ISAC is widely recognized as playing a crucial role in the relationships among entities in sectoral organizations. Sectoral organizations embody a governance relationship between cross-sector public and private entities, called public-private partnerships (PPPs) [26]. Cybersecurity PPPs emphasize continuous and ongoing information sharing related to national security policy analysis [26]. These private sectors include energy supply and infrastructure, drinking water supply and distribution, healthcare, financial market infrastructures, banking, rail transport, air transport, maritime, road transport, and food distribution, among others [23]. Public sector organizations comprise government bodies, both at the ministry and country-state levels [23]. Public sector organizations require information sharing from the private sector to provide added value to the planning and disseminating of public services [27]. Effective information sharing in sectoral organizations can promote national public cybersecurity goals [25].

In-organization IT departments such as computer security incident response teams or cybersecurity agencies provide cyber incident information sharing. Information sharing is implemented into ISAC based on established sector-based business processes. Countries that implement sector-based ISAC include the United States of America and Japan. Examples of U.S. ISAC are the Financial Services ISAC (FS-ISAC) and the Research and Education ISAC (REN-ISAC) [26]. At the state level, California, USA, has its own ISAC: the California Cybersecurity Integration Center (CAL-CSIC) [28]. Japan operates its own Financial ISAC, ICT-ISAC Japan, and the Japan Electricity ISAC (JE-ISAC) [29].

2.2. Cyber Incident Information Sharing in Sectoral Organizations

Information sharing can improve cybersecurity awareness and response culture [6]. However, cyber incident information-sharing collaboration is limited to information sharing platforms and includes incident analysis centers, regular meetings, working groups, conferences and side events, web portals/platforms, and teleconferences [23]. These collaborations increase organizational capabilities in a sectoral community regarding cyber incident information sharing.

Cyber incident information is useful for increasing organizations' cybersecurity capabilities, especially among organizations within the same sector. Cyber incident information has been classified into the four categories of the Traffic Light Protocol (TLP): red, amber, green, and white. The red category is information that can be used only by a member or Person in Charge in certain sectoral organizations. The amber category is information that can be used for the benefit of members of sectoral organizations. The green category is information that can be accessed by members of sectoral organizations and their partners. The white category is information that the public can freely use with an observation of the standard copyright rules.

Cyber incident information classified as red or amber by sectoral organizations must be kept confidential, but classified information owned by sectoral organizations can be stored in private cloud storage [17]. By contrast, the authors stated that the information with a white category classification is stored in the public cloud. Information stored in the public cloud must validate data ownership to show legal ownership through a certificateless provable data possession scheme. Revocable storage applied in the cloud with Identity-Based Encryption has been presented in [3], which focused on storing encrypted user identities. Finally, a survey on data security and privacy protection stored in the cloud was conducted in [30], which concluded that cloud security is a rather challenging task.

2.3. Data Security: Privacy-Preservation and Protection

Organizational identity is sensitive data that must be secured. Various techniques can achieve data security. One of them is the application of privacy preservation for sensitive organizational data in the information sharing process.

Sensitive information protection can be implemented through secure information hiding techniques using identity-based auditing in cloud storage [31]. A bilinear map system model and computational Diffie-Hellman with a discrete logarithm assumption have been used. Therefore, efficient identity-based auditing in a shared cloud has been proposed for sensitive Electronic Health Record data.

Data privacy protection can be carried out with an anonymity scheme but accompanied by proof of data ownership to avoid false information. One solution is to propose a privacy-preserving certificateless provable data possession scheme on cloud storage [17] that utilizes Elliptic Curve Cryptography and certificateless cryptography. Certificateless provable data possession techniques can prove the ownership of the data without knowledge of the owner's original identity. A third party can then validate the proof of ownership or refer to a Trusted Third Party agent in a public data-sharing scheme.

Another issue in data privacy protection is ensuring access control in securing valuable and sensitive information. Computational issues also become essential to ensure data confidentiality and guarantee privacy for entities. In [11], the authors used data privacy preservation with a novel CP-ABE scheme. However, no role was provided for the data integrity and verification process.

The audit process carried out by third parties should not disclose user privacy data on the network. For example, privacy preservation of the public auditing process in cloud storage was presented in [13]. However, the audit process carried out by the Third-Party Auditor could not determine the information corresponding to the user's privacy data. A novel algorithm for cybersecurity information sharing has been presented in [12], in which the sharing mechanism on STIX objects was supported in the context of situational awareness of cyber threats. Data privacy preservation with anonymous communication technique clustering was utilized in [10] and included a *k*-anonymity scheme, *p*-anticonspiration privacy model, zero-knowledge proof, anonymous mutual authentication, Bayesian security game, and *k*-anonymity with the e-differential scheme. These techniques can be used to provide privacy-preserving user data privacy in cloud storage.

Data in the cloud needs to be audited and protected. In addition to data privacy, data protection is another critical aspect requiring enforcement. Data confidentiality techniques can protect data through a public auditing scheme with a pseudonym user hash [13]. In addition, secure and safe data sharing between users in the cloud can be realized using various cryptographic techniques [3], such as Identity-Based Encryption (IBE) with user revocation functions and ciphertext updates simultaneously through revocable storage. Using CP-ABE, secure data sharing can also be realized [10], as an efficient CP-ABE scheme can maintain privacy by verifying authorities and ensuring data confidentiality. Therefore, the privacy-preserving CP-ABE with a novel scheme can provide efficient results and increase security.

The integration of CP-ABE and STIX in cybersecurity information sharing was proposed in [20], focusing on Cyber Threat Intelligence. Cybersecurity Information Exchange protects sensitive organization information by providing encryption and access control when carrying out proactive protection. As a result, the user could only decrypt sensitive information with appropriate attributes.

The current research project proposes a secure-protocol solution for securing cyber incident information sharing in the cloud services of sectoral organizations. The proposed scheme was developed by improving the scheme proposed in [17] involving the utilization of certificateless provable data possession.

3. The Proposed PURA-SCIS Protocol

This section may be divided into subheadings that provide a concise and precise description of the experimental results, their interpretation, and the experimental conclusions that can be drawn.

The Putra-Ramli Secure Cyber-incident Information Sharing (PURA-SCIS) protocol is a communication protocol that focuses on cyber incident information sharing and allows secure exchange of classified information between sectoral organizations. The PURA-SCIS protocol utilizes public-key cryptography on cryptographic protocols as one of the security measures in cyber incident information sharing. The protocol design process is divided into two stages (i.e., design and testing), as illustrated in Figure 1.

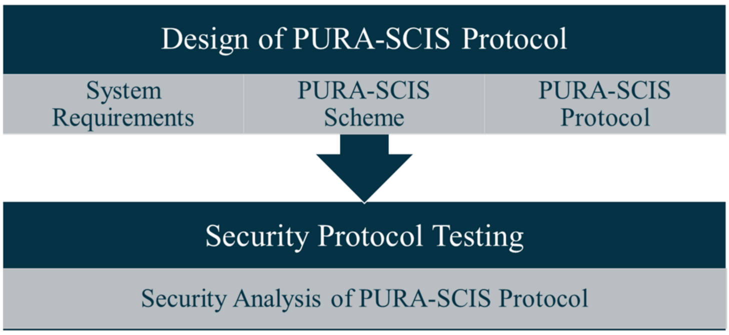

Design of PURA-SCIS Protocol
System Requirements
PURA-SCIS Scheme
PURA-SCIS Protocol
Security Protocol Testing
Security Analysis of PURA-SCIS Protocol

Figure 1. Research Stages.

The first stage is the design of the PURA-SCIS protocol, which considers three attributes: the system requirements, PURA-SCIS scheme, and PURA-SCIS protocol. The second stage is security protocol testing, in which the security of the information exchange communication protocol is tested using a cryptographic protocol. This section discusses the design of the PURA-SCIS protocol.

3.1. System Requirements of the PURA-SCIS Protocol

PURA-SCIS protocol required a system involving entities and their roles. Accordingly, five entities were defined in the PURA-SCIS protocol, as listed in Table 1.

Table 1. Entities of PURA-SCIS Protocol.

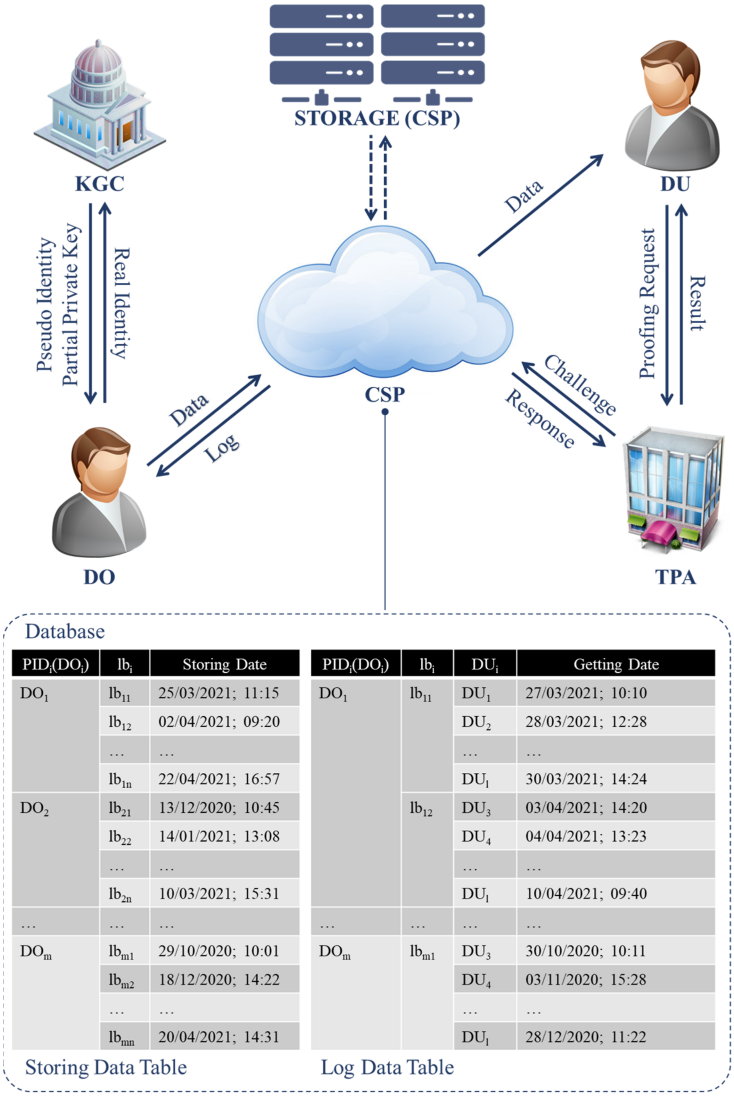
Entity	Definition
KGC	Key Generation Center
CSP	Cloud Service Provider
DO	Data Owner (the i-th DO)
TPA	Third Party Auditor
DU	Data User

Each entity has a specific role and function:

1. The Key Generation Center (KGC) is a fully trusted entity that partially generates key pairs to prove the Data Owner's cyber incident information ownership.
2. The Cloud Service Provider (CSP) is a semi-trusted entity that stores all entity public key information and the Data Owner's cyber incident information. The Cloud Service Provider also secures all the stored information using various cryptographic techniques.
3. The Data Owner is an entity that stores cyber incident information in the Cloud Service Provider of sectoral organizations.
4. The Third Party Auditor is a semi-trusted entity serving as a third-party auditor to prove Data Owner data possession through a challenge-response process with the Cloud Service Provider.
5. The Data User is an entity consuming the Data Owner's cyber incident information on the network.

3.2. PURA-SCIS Scheme

The PURA-SCIS scheme is a process of cyber incident information sharing between sectoral organizations privately on a cloud service. As shown in Figure 2, the PURA-SCIS scheme is an information network and communication relationship between entities.



$PID_i(DO_i)$	lb_i	Storing Date
DO_1	lb_{11}	25/03/2021; 11:15
	lb_{12}	02/04/2021; 09:20
	…	…
	lb_{1n}	22/04/2021; 16:57
DO_2	lb_{21}	13/12/2020; 10:45
	lb_{22}	14/01/2021; 13:08
	…	…
	lb_{2n}	10/03/2021; 15:31
…	…	…
DO_m	lb_{m1}	29/10/2020; 10:01
	lb_{m2}	18/12/2020; 14:22
	…	…
	lb_{mn}	20/04/2021; 14:31

Storing Data Table

$PID_i(DO_i)$	lb_i	DU_i	Getting Date
DO_1	lb_{11}	DU_1	27/03/2021; 10:10
		DU_2	28/03/2021; 12:28
		…	…
		DU_l	30/03/2021; 14:24
	lb_{12}	DU_3	03/04/2021; 14:20
		DU_4	04/04/2021; 13:23
		…	…
		DU_l	10/04/2021; 09:40
…	…	…	…
DO_m	lb_{m1}	DU_3	30/10/2020; 10:11
		DU_4	03/11/2020; 15:28
		…	…
		DU_l	28/12/2020; 11:22

Log Data Table

Figure 2. PURA-SCIS Scheme.

Figure 2 describes the proposed cyber incident information-sharing scheme. The Cloud Service Provider has storage that entities on the information-sharing network can only access to store data. The Cloud Service Provider also keeps all logs of information about the data storage process by the Data Owner. The Cloud Service Provider stores information, such as entity identity, stored information labels, and the timestamps of the data exchange processes. Note that the timestamp includes both the data storage time and the data retrieval time by the entity.

The Cloud Service Provider can be referred to as a cloud provider or vendor that provides private cloud storage services for sectoral organizations. More details about the private cloud can be found in [30,32]. The Cloud Service Provider can act in knowing all the information in its storage. However, if the cyber incident information has a secret classification (TLP: red/amber), that specific information can only be sent via encrypted information or information with passwords. As a semi-trusted third party, the Cloud Service Provider cannot read the confidential information in the data exchange but can only help prove data ownership through the available metadata.

The Third Party Auditor helps Data Users to validate the data stored on the network and the data stored by the Cloud Service Provider. A trusted independent cybersecurity organization or government organization authorized in the cybersecurity area can be utilized as the Third Party Auditor. Data users can also entrust the Third Party Auditor's information as a data requester without worrying about data breaches or leaks.

The Data Owner and Data Users have very different roles; however, the implementation of these two entities can be handled by the same organization in the network. For example, one organization in the cyber incident information-sharing network can act as either the Data Owner or a Data User. Organizations in the network can provide their information or request their information securely. The organizations can be organizations in particular sectors, such as public or private sectors.

The purpose of cyber incident information sharing is to serve as a forum or platform by which organizations in the same sector can share cyber incident information. The result is a beneficial increase in cybersecurity capabilities between organizations and a strengthening of cybersecurity defenses for every organization involved in the cyber incident information-sharing network.

The other entity is the Key Generation Center, which can act as an entity or an application platform that generates cryptographic keys according to the needs of entities on the network. This Center can play a role with specific schemes or secure channels and be implemented as an integrated platform for each entity. The Key Generation Center can also be implemented as a fully trusted party for providing cryptographic key pairs for users on the network. This situation can only be achieved if the Key Generation Center is a fully trusted party because the Center keeps all the entity's original identities, especially of the Data Owner as the owner of the information.

Figure 2 explains the five phases and the entities involved. These phases are shown in Table 2 and described in the process, as in the subsequent sections.

Table 2. PURA-SCIS Components.

Component	Definition
ID_i	Real Identity DO-*i*
DO_i	Pseudo-Identity DO-*i* (Identity on the CIS network) as a public key of DO-*i* (in the proposed protocol equals *DO*)
DU_i	Pseudo-Identity DU-*i* (Identity on the CIS network) as a public key of DU-*i* (in the proposed protocol equals *user*)
(D_i, y_i)	Partial Public Key DO-*i* for provable data possession algorithm
m	The shared data (in the proposed protocol equals $m1$)
σ	The shared data component of provable data possession (in the proposed protocol equals $m2$)
$R_l,\ S_l$	The component of σ data
lb_i	The label of the shared data
log	The log of the shared data
$na,\ nb,\ \dots, nk$	N once
j	The random number, $j \in Q$ (with c elements, $c \leq n$) of set $\{1, 2, \dots, n\}, \lvert Q \rvert = c$
V_j	The challenge component of provable data possession, $V_j \in Z_q^*$
$a,\ b$	Proof of response to the challenge
res	The result of provable data possession
pk	The public key symbol
$\{\ \}pk(\ )$	The process of encrypted data with the public key

3.2.1. Key Generation Phase

This phase is the crucial establishment process for entities joined in the network. The generated key is the user's key pair and does not reveal the user's real identity for proof of data ownership. After the possession of the partial key pair of provable data is completed, the entity that encrypts the exchanged cyber incident information generates a public key pair. The technical detail of the Key Generation phase applied in PURA-SCIS protocol is that Data Owner gives its identity to the Key Generation Center. The Key Generation Center then uses a pseudo-identity algorithm to generate a pseudo-identity $\{DO_i\}$ and key pairs $\{D_i, y_i\}$. This cryptographic key pair can be used for the provable data possession process for the Data Owner. The Data Owner then generates σ, which contains R_l and S_l that act as provable data possession components. All public key identities of the Data Owner, Cloud Service Provider, Third Party Auditor, and Data User are known to each other; therefore, the sender requests the cryptographic protocol without first proving data possession of the identity.

3.2.2. Data Storing Phase

Cyber incident information is stored in the cloud storage of sectoral organizations with the public key encryption method. Data stored in a private cloud belongs to the entities in the system. In this phase, the Data Owner stores data on the Cloud Service Provider by sending $\{m, \sigma, na, DO_i\}$, encrypted by public key Data Owner $\{X_i\}$. The Cloud Service Provider confirms Data Owner delivery by resending na, accompanied by $\{lb, na, nb, CSP\}pk(DO_i)$. The label is given to the Data Owner and stored with the code lb. If the Data Owner succeeds in sending back the nb, then the Data Owner is confirmed to store data in the Cloud Service Provider. The Cloud Service Provider then stores the Data Owner data in its storage by classifying records PID, lb, and timestamp information. Finally, the Data Owner sends $\{nb\}pk(CSP)$ to the Cloud Service Provider to close the communication. This process is the first Information Sharing and Analysis Center (ISAC) protocol (i.e., the ISAC1 protocol).

3.2.3. Data Retrieval and Log Reporting Phase

Data retrieval in the cloud service of sectoral organizations for data requesters is accompanied by log reporting to data owned by the cloud provider. The Data User initializes the detailed process, which selects and requests a Data Owner via the Cloud Service Provider by sending the desired data label. Entities within the system can only access data retrieval in the private cloud belonging to the Cloud Service Provider. The Data User sends $\{lb_i, nc, DU_i\}pk(CSP)$ to the Cloud Service Provider, and the Cloud Service Provider confirms the Data User request by providing $\{m, \sigma, lb_i, nd, CSP\}pk(DU_i)$; the Data User then replies with $\{nd\}pk(DU_i)$. After data sent from the Cloud Service Provider to the Data User is successful, the Cloud Service Provider sends the log to the Data Owner, who is confirmed as the Data Owner by sending $\{log, DU_i, CSP\}pk(DO_i)$. The process is continued with confirmation of data transmission between the Data Owner and the Cloud Service Provider. The Data Owner sends $\{log, ne, DO_i\}pk(CSP)$ as confirmation to the Cloud Service Provider. Finally, the Cloud Service Provider sends $\{ne\}pk(DO_i)$ to the Data Owner as a communication closure. This process of the protocol is referred to as the second protocol, i.e., the ISAC2 protocol.

3.2.4. Challenge-Response Phase

This phase is a process of provable data possession by data requesters through a third-party auditor, with partial proof of data ownership between a third-party auditor and a cloud provider for the sectoral organizations. The received data must prove ownership through a trusted third party as an auditor (i.e., a Third Party Auditor). After the Data User receives data from the Cloud Service Provider, the Data User forwards the data $\{m, \sigma, lb_i, DO_i, nf, DU_i\}pk(TPA)$ to the Third Party Auditor, which then confirms the Data User by sending $\{nf, ng, TPA\}pk(DU_i)$. The final process of the request for provable data possession is the sending of $\{ng\}pk(TPA)$ from the Data User to the Third Party Auditor.

The Third Party Auditor determines $j \in Q$ and randomly determines $V_j \in Z_q^*$ and sends challenge data $\{j, V_j, lb_i, DO_i, nh, TPA\}pk(CSP)$ to the Cloud Service Provider. The Cloud Service Provider receives the Third Party Auditor challenge data and then generates response data. Before processing the response data, the Cloud Service Provider selects the stored Data Owner information, according to DO_i and lb_i. The Cloud Service Provider counts a and b as response data and sends $\{a, b, lb_i, lb_i, DO_i, nh, ni, CSP\}pk(TPA)$ to the Third Party Auditor. Finally, communication between the Cloud Service Provider and the

Third Party Auditor is closed by the Third Party Auditor by sending $\{ni\}pk(CSP)$ to the Cloud Service Provider.

The Third Party Auditor receives the Cloud Service Provider data and matches the values of a and b obtained with the provable data possession algorithm through the hash function scheme. Upon completion of the calculation, a is set to 1 to represent the validated Data Owner, whereas a is set to 0 if the Data Owner cannot be validated. The final process of this phase is sending $\{ni\}pk(CSP)$ from the Third Party Auditor to the Cloud Service Provider. This process is referred to as the third ISAC protocol (ISAC3).

3.2.5. Results Phase

The Third Party Auditor sends the data possession results to the data requester. The result of the challenge-response process by the Third Party Auditor produces a value that is sent as final information on proving data ownership of the Data Owner to the Data User. The Third Party Auditor sends $\{res, lb_i, DO_i, TPA\}pk(DU_i)$ to the Data User. The result obtained by the Data User is a *res* that shows Data Owner provable data possession. Next, the Data User confirms receipt of the Third Party Auditor message by sending $\{lb_i, nk, DU_i\}pk(TPA)$. Finally, the Third Party Auditor closes communication with $\{nk\}pk(DU_i)$ to the Data User. This process is referred to as the fourth ISAC protocol (ISAC4).

The challenge-response process is carried out between the Third Party Auditor and the Cloud Service Provider to prove possession by the Data Owner (i.e., m). The process involves a calculation algorithm that generates a challenge value from the Third Party Auditor to the Cloud Service Provider. The challenge data are used as the input to the response calculation algorithm that produces a and b. The calculation of provable data possession is detailed in [13].

All of these cryptographic function components include elliptic curve cryptography, certificateless cryptography, and hash functions. The security of the information storage process in the Cloud Service Provider is related to the role of cloud service in the sectoral organizations. The Cloud Service Provider stores the Data Owner's information securely in its storage and database. Therefore, in the challenge-response process carried out between the Cloud Service Provider and the Third Party Auditor, the Cloud Service Provider has the authority to access cyber incident information stored by the Data Owner.

First, the Cloud Service Provider checks the lb_i and DO_i sent by the Third Party Auditor. Then, the Cloud Service Provider looks for the data in its database and accesses the information through its storage. Finally, the Cloud Service Provider securely stores all cyber incident information with an encryption process to prevent arbitrary access to the stored data by unauthorized users. The Cloud Service Provider plays an important role as a data controller for data privacy issues. The secure access to stored cyber incident information can be processed automatically through an integrated computer system. The automation process reduces the chance of human error or threats caused by insider threats within the Cloud Service Provider. However, the Cloud Service Provider communicates with the private cloud services provided to entities in the system.

3.3. The PURA-SCIS Protocol

The PURA-SCIS scheme in Figure 2 implements a secure communication protocol between its entities. The PURA-SCIS protocol is proposed based on the cyber incident information sharing process, with additional security properties. This protocol is focused on securing confidential data in private clouds for sectoral organizations. The PURA-SCIS scheme has five phases that classify confidential data into secure data and other data. Each phase has a different component of data, as described in Table 3.

Table 3. Data Component Relationship with The Phases.

Phases	Data Component	
	Secure Data	**Other Data**
Key Generation Phase	$ID_i,\ DO_i,\ (D_i, y_i)$	–
Data Storing Phase	$m,\ \sigma,\ lb_i$	$na,\ nb,\ DO_i,\ CSP$
Getting Data and Reporting Log Phase	$m,\ \sigma,\ lb_i,\ log,\ DU_i$	$nc,\ nd,\ ne, DO_i,\ CSP$
Challenge-Response Phase	$m,\ \sigma,\ lb_i,\ log,\ j,\ V_j,\ a,\ b,\ DO_i$	$nf,\ ng,\ nh,\ ni,\ DU_i,\ CSP,\ TPA$
Result Phase	$res,\ lb_i,\ DO_i$	$nk,\ DU_i,\ TPA$

Figure 3 shows a sequence diagram that illustrates the process of the PURA-SCIS scheme. The PURA-SCIS protocol consists of 4 ISAC protocols (defined in Section 3.2 earlier). The entities involved in the PURA-SCIS protocol are the Data Owner, Data User, Cloud Service Provider, and Third Party Auditor. The PURA-SCIS protocol focuses on using the public key of each entity to maintain the confidentiality of data transmission among the entities in a cyber incident information-sharing network.

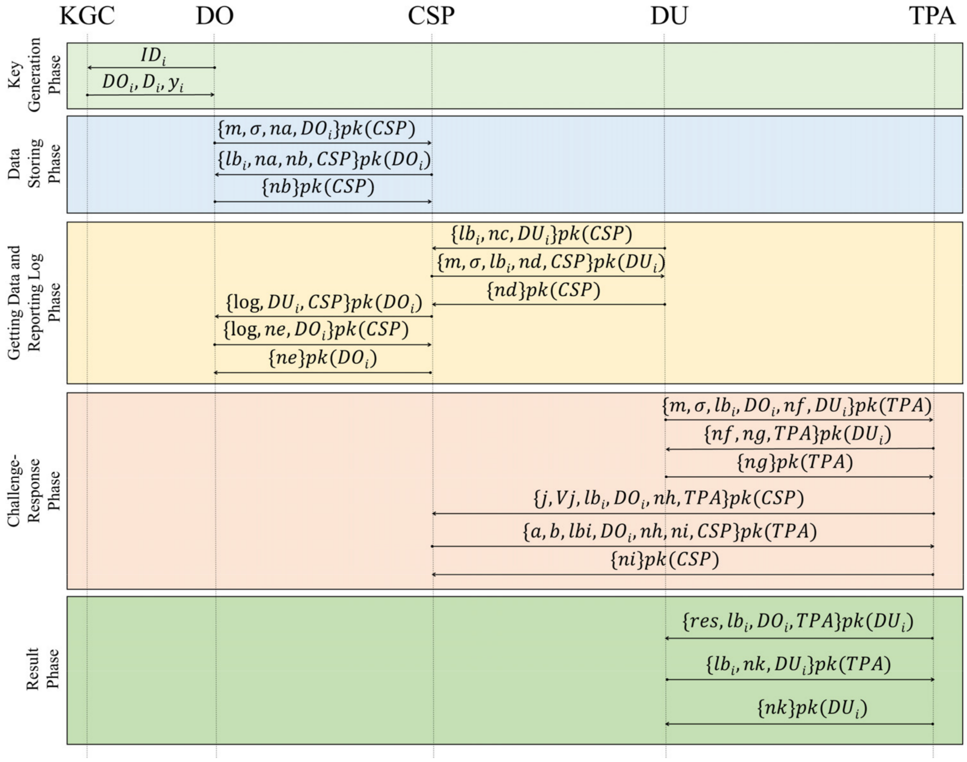

KGC
DO
CSP
DU
TPA
Key Generation Phase
ID_i
DO_i, D_i, y_i
Data Storing Phase
$\{m, \sigma, na, DO_i\}pk(CSP)$
$\{lb_i, na, nb, CSP\}pk(DO_i)$
$\{nb\}pk(CSP)$
Getting Data and Reporting Log Phase
$\{lb_i, nc, DU_i\}pk(CSP)$
$\{m, \sigma, lb_i, nd, CSP\}pk(DU_i)$
$\{nd\}pk(CSP)$
$\{\log, DU_i, CSP\}pk(DO_i)$
$\{\log, ne, DO_i\}pk(CSP)$
$\{ne\}pk(DO_i)$
Challenge-Response Phase
$\{m, \sigma, lb_i, DO_i, nf, DU_i\}pk(TPA)$
$\{nf, ng, TPA\}pk(DU_i)$
$\{ng\}pk(TPA)$
$\{j, Vj, lb_i, DO_i, nh, TPA\}pk(CSP)$
$\{a, b, lbi, DO_i, nh, ni, CSP\}pk(TPA)$
$\{ni\}pk(CSP)$
Result Phase
$\{res, lb_i, DO_i, TPA\}pk(DU_i)$
$\{lb_i, nk, DU_i\}pk(TPA)$
$\{nk\}pk(DU_i)$

Figure 3. The Proposed PURA-SCIS Protocol.

4. Evaluation of the Proposed PURA-SCIS Protocol

Security assessment on the communication patterns of the PURA-SCIS protocol is achieved via a cryptographic protocol approach using formal analysis tools [33,34]. In this research, the Scyther tool with Security Protocol Description Language (SPDL) is used to assess the security properties of the proposed protocol to verify security. The Scyther tool was chosen because this tool is easy to use, is the fastest protocol verification tool that does not use approximation methods, and has been successfully used and implemented by many researchers; see [33–40]. Scyther is used to prove and verify that PURA-SCIS has met the security requirements, namely confidentiality. The tool is installed on a machine running Ubuntu OS 16.04 with 4 GB memory. The source code for PURA-SCIS is available on Github Repository.

4.1. Security Analysis of the Provable Data Possession Scheme

The provable data possession scheme provides several security services listed in [17] as follows:

4.1.1. Public Verifiability

The provable data possession algorithm can provide verification services by either the user or the Data User. In addition, data possession can be verified using the challenge-response algorithm between the Cloud Service Provider and the Third Party Auditor.

4.1.2. Blockless Verification

Provable data possession does not need to use all the data from the information to be proven. Instead, the process can use partial data for verification.

4.1.3. Data Privacy Preservation

Data possession proven through the challenge-response process does not involve the disclosure of all information. Instead, data privacy preservation is provided through the process of provable data possession with partial information that cannot be traced to reconstruct the original information completely.

4.1.4. Identity Privacy Preservation and Traceability

The provable data possession process should not be used to reveal the true identity of the Data Owner. However, the Data Owner can still be known by the Data User through the identity used in the network. The identity can be a specific identity that is known between entities in the network. Every stored data item can also be traced to its origin (i.e., traceability).

The PURA-SCIS protocol focused on improving the previous design [17] with an additional security protocol and ensuring secure cyber incident information sharing in the network. This security guarantee is provided by public-key cryptography, which secures information exchange through security protocols on the network.

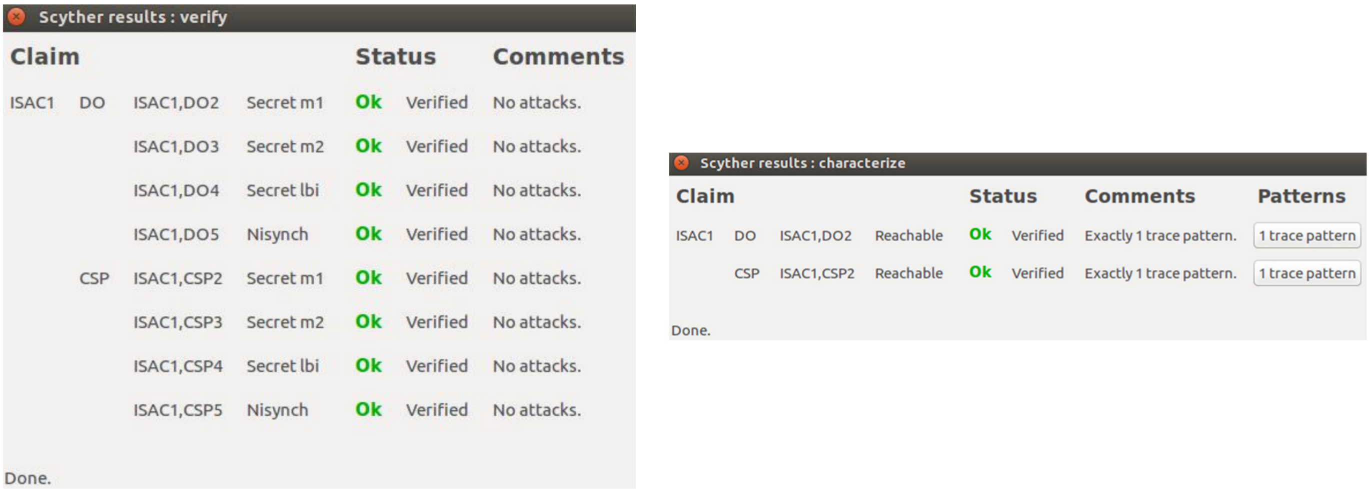
4.2. Security Analysis of The PURA-SCIS Protocol

The Scyther tool is used to perform security validation on the proposed protocol using formal analysis with cryptographic protocols. The security evaluation was performed on the four protocols: ISAC1, ISAC2, ISAC3, and ISAC4 (defined in Section 3.2).

4.2.1. ISAC1 Security Verification

Figure 4a shows the ISAC1 verification result with the communication protocol between the Data Owner and the Cloud Service Provider. Again, the results showed no possible loophole for cybercriminals to attack the communication protocol between the Data Owner and the Cloud Service Provider. As shown in Figure 4a, the ISAC1 protocol guarantees confidentiality on $m1$, $m2$, and lb_i. In the Data Owner role, the system obtained four claims with OK status and no attacks. In the Cloud Service Provider role, the system obtained four claims with OK status and no attacks. These results found no attacks on the Data Owner role and the Cloud Service Provider role.

The Data Owner and Cloud Service Provider can guarantee security if the communication process is authentic. The additional secure protocol can guarantee data confidentiality in the communication protocol. ISAC1 has been designed to comply with Nisynch, (i.e., non-injective synchronization). This means that every communication in the protocol runs according to the protocol specifications, with the appropriate data exchange, and in the correct order.



Scyther results : verify

Claim				Status		Comments
ISAC1	DO	ISAC1,DO2	Secret m1	Ok	Verified	No attacks.
		ISAC1,DO3	Secret m2	Ok	Verified	No attacks.
		ISAC1,DO4	Secret lbi	Ok	Verified	No attacks.
		ISAC1,DO5	Nisynch	Ok	Verified	No attacks.
	CSP	ISAC1,CSP2	Secret m1	Ok	Verified	No attacks.
		ISAC1,CSP3	Secret m2	Ok	Verified	No attacks.
		ISAC1,CSP4	Secret lbi	Ok	Verified	No attacks.
		ISAC1,CSP5	Nisynch	Ok	Verified	No attacks.

Done.

(**a**)

Scyther results : characterize

Claim				Status		Comments	Patterns
ISAC1	DO	ISAC1,DO2	Reachable	Ok	Verified	Exactly 1 trace pattern.	1 trace pattern
	CSP	ISAC1,CSP2	Reachable	Ok	Verified	Exactly 1 trace pattern.	1 trace pattern

Done.

(**b**)

Figure 4. (**a**) ISAC1 Verification Result; (**b**) ISAC1 Pattern Result.

Figure 4b shows the ISAC1 pattern result with only one trace pattern with the OK status. This result indicates that the security protocol in ISAC1 established only one communication process with the Data Owner and Cloud Service Provider entities in the network. Therefore, the role of the Data Owner and Cloud Service Provider on ISAC1 confirmed that only one trace pattern is obtained and is reachable.

Figure 5 is an example of a suitable pattern for ISAC1. There are two related entities in ISAC1: the role DO and the role CSP. Figure 5a shows the claim to DO in the ISAC1 protocol. Figure 5b shows the claim CSP on the ISAC1 protocol.

4.2.2. ISAC2 Security Verification

ISAC2 found that the communication protocol guarantees the security or the secrecy of m ($m1$), σ ($m2$), lb_i, log, and user (DU_i). ISAC2 extracted three guarantee properties on the Data User role: alive CSP, Nisynch, and Niagree (non-injective agreement). The Cloud Service Provider role also guarantees alive DU, alive DO, Nisynch, and Niagree. Finally, the Data Owner role also guarantees alive CSP, Nisynch, and Niagree.

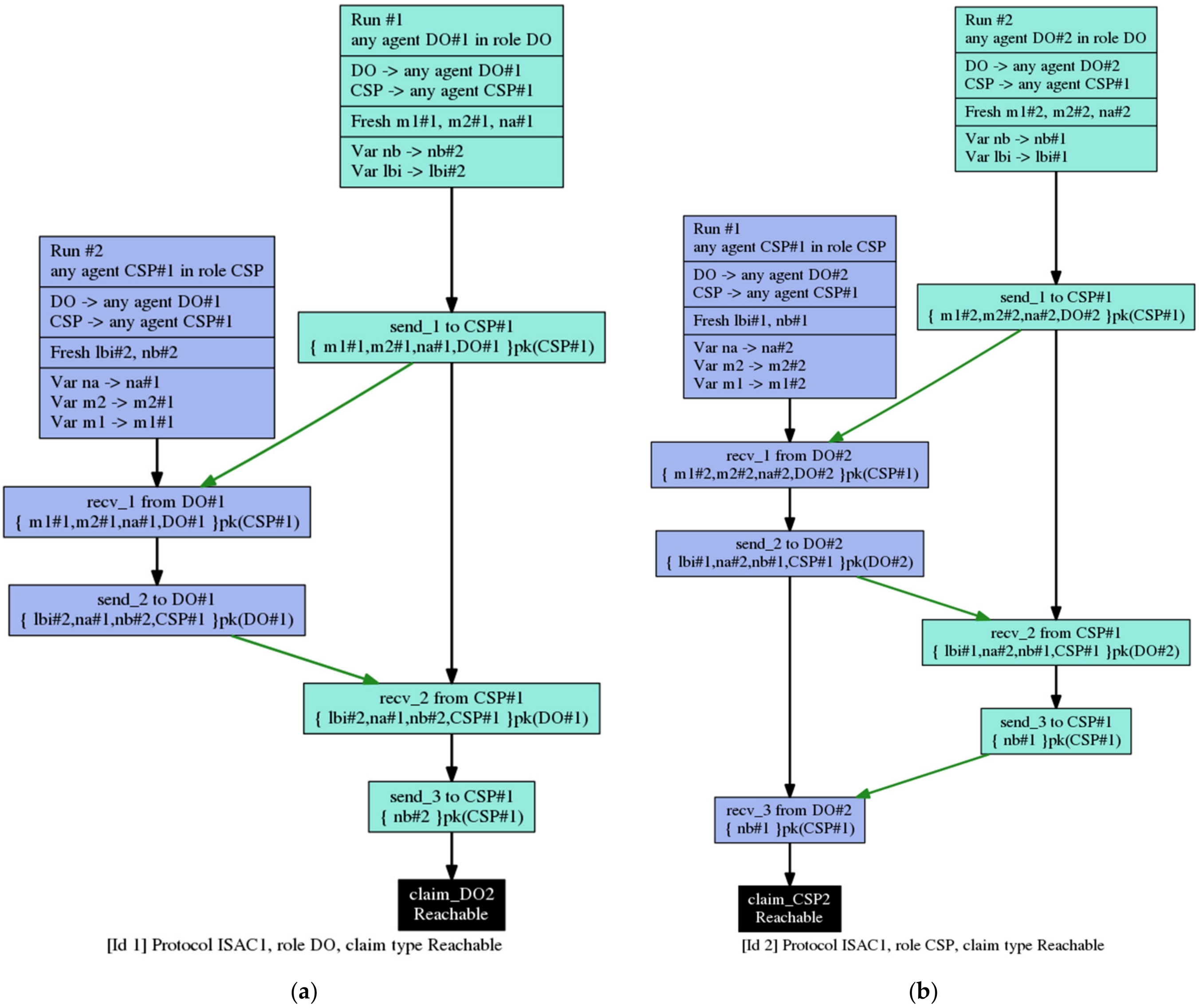
The aliveness indicates that the entities in the communication network trust that the protocol can guarantee the existence of other communicating entities. Nisynch is also provided in this ISAC2 protocol, similar to ISAC1. The Niagree defines this as a term of a messaging agreement between various parties. The Niagree states that all parties to the protocol run the protocol and communicate with each other. These claims are examples of certainty and security provided by the proposed cyber incident information-sharing scheme protocol.

The results obtained from ISAC2 in Figure 6a showed no attacks and no attacks within bounds. In its implementation, the process is carried out only once by the entity. This parameter is used to detect replay attacks that send data repeatedly to gain information access in the protocol. This result showed that the proposed protocol is secure with anonymity and two-way authentication because all claims can be fulfilled.

In ISAC2, 3 entities are involved in the protocol: DU, CSP, and DO. DU and CSP are the protocol roles for requesting and retrieving information through the Cloud Service Provider of sectoral organizations. The process is automatically followed by a notification of the data retrieval process to the Data Owner with the log from the Cloud Service Provider to the Data Owner. These two processes are interrelated, so they become the same protocol.

Figure 6b shows that the pattern generated from the Data User and Cloud Service Provider roles has 1 trace pattern. This pattern indicated that no other processing gaps resulted from the protocol proposed in ISAC2. However, the Data Owner role showed that two trace patterns were generated. This result found one pattern that produced a possible pattern of security attacks in the ISAC2 protocol.

Figure 7 is an example of a suitable pattern for ISAC2. There are three related entities in ISAC2: role DU, role CSP and role DO. Figure 7a shows the claim DU on the ISAC2 protocol. Figure 7b shows the claim CSP on the ISAC2 protocol. Figure 7c shows the claim DO on the ISAC2 protocol.

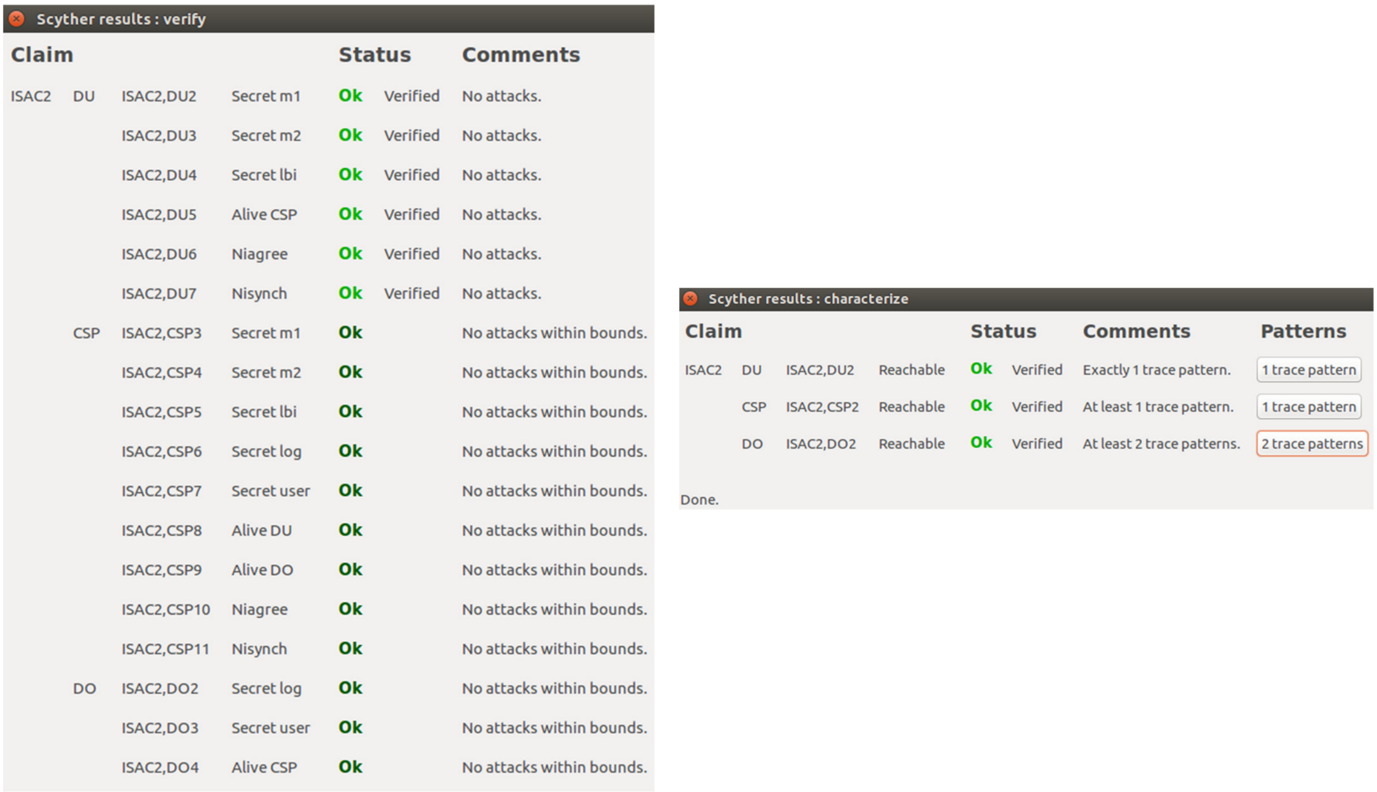


(**a**) (**b**)

Figure 5. (**a**) ISAC1 Pattern Scheme—role DO; (**b**) ISAC1 Pattern Scheme—role CSP.

Figure 8 shows the pattern of attack loopholes that occurred in the ISAC2 protocol. The attack can occur with initial intruder knowledge capability on the attacker. Figure 6 explains that the attacker performs the data request process because of the public key of the Cloud Service Provider. Therefore, the attacker only needs the protocol process as usual to identify it.

The attack scheme in Figure 8 is projected from the proposed scheme. The network's entities are private networks formed by the public key distribution process between entities before information-sharing of cyber incidents. Each entity can verify the sender's public key first by viewing the list of authorized entities' public keys on the network. The attack in Figure 6 can be anticipated with the Cloud Service Provider by the available public key list of entities in the cyber incident information-sharing network. However, Eve (initials of the attacker) cannot reply to the data sent by the Cloud Service Provider with the information. Therefore, the protocol attack in Figure 8 cannot be recognized with the initial check and distribution of the entity's public key.



Scyther results : verify

Claim				Status		Comments
ISAC2	DU	ISAC2,DU2	Secret m1	Ok	Verified	No attacks.
		ISAC2,DU3	Secret m2	Ok	Verified	No attacks.
		ISAC2,DU4	Secret lbi	Ok	Verified	No attacks.
		ISAC2,DU5	Alive CSP	Ok	Verified	No attacks.
		ISAC2,DU6	Niagree	Ok	Verified	No attacks.
		ISAC2,DU7	Nisynch	Ok	Verified	No attacks.
	CSP	ISAC2,CSP3	Secret m1	Ok		No attacks within bounds.
		ISAC2,CSP4	Secret m2	Ok		No attacks within bounds.
		ISAC2,CSP5	Secret lbi	Ok		No attacks within bounds.
		ISAC2,CSP6	Secret log	Ok		No attacks within bounds.
		ISAC2,CSP7	Secret user	Ok		No attacks within bounds.
		ISAC2,CSP8	Alive DU	Ok		No attacks within bounds.
		ISAC2,CSP9	Alive DO	Ok		No attacks within bounds.
		ISAC2,CSP10	Niagree	Ok		No attacks within bounds.
		ISAC2,CSP11	Nisynch	Ok		No attacks within bounds.
	DO	ISAC2,DO2	Secret log	Ok		No attacks within bounds.
		ISAC2,DO3	Secret user	Ok		No attacks within bounds.
		ISAC2,DO4	Alive CSP	Ok		No attacks within bounds.

(**a**)

Scyther results : characterize

Claim				Status		Comments	Patterns
ISAC2	DU	ISAC2,DU2	Reachable	Ok	Verified	Exactly 1 trace pattern.	1 trace pattern
	CSP	ISAC2,CSP2	Reachable	Ok	Verified	At least 1 trace pattern.	1 trace pattern
	DO	ISAC2,DO2	Reachable	Ok	Verified	At least 2 trace patterns.	2 trace patterns

Done.

(**b**)

Figure 6. (**a**) ISAC2 Verification Result; (**b**) ISAC2 Pattern Result.

4.2.3. ISAC3 Security Verification

Figure 9a shows that the ISAC3 protocol guarantees the security of m, σ, lb_i, log, j, V_j, a, b, and DO_i. The three entities in ISAC3 can provide secret claims on the data exchanged. The verification result showed that the Data User role has no attacks, and the Third Party Auditor and Cloud Service Provider roles have no attacks within bounds. These results showed that the data exchanged are safe within the constraints.

The results of the ISAC3 pattern are shown in Figure 9a,b, which identify one trace pattern in the Data User and Third Party Auditor roles. No other pattern is reachable other than the pattern proposed in the protocol. However, the result of the Cloud Service Provider role indicated the generation of another pattern, indicating the possibility of an attack resulting from the ISAC3 protocol.

The attack found in Figure 10 is similar to the protocol attack in Figure 8. This attack occurred by Eve, the attacker, being able to send a request message to the Third Party Auditor. Eve can have the ability in the form of initial intruder knowledge to perform this protocol action. The attacker only needs the protocol process to carry out the attack.

The attack on the ISAC3 protocol can be anticipated with each entity by identifying the entity's public key in the network. The protocol flow process in Figure 8 does not continue when the attacker sends data to the Third Party Auditor. Therefore, the Third Party Auditor should already know the public key of the authorized entity, so the Auditor can determine which entity's public key has not been registered.

The checking process is performed when the Third Party Auditor wants to reply to the data transmission process by the attacker to the Third Party Auditor. For example, the Third Party Auditor requires the entity's public key to reply to the attacker's message. If the public key is not registered, the Third Party Auditor does not reply to the attacker's message, and the protocol does not continue.

4.2.4. ISAC4 Security Verification

The last part of the protocol in the proposed scheme is ISAC4. Figure 11a shows that the verification result for ISAC4 produced a guarantee of confidentiality for res, lb_i, and DO_i by the ISAC4 protocol. Claims generated from the Third Party Auditor and the Data User roles were verified as having no attacks. This result indicated the data confidentiality in the communication process could be guaranteed in ISAC4.

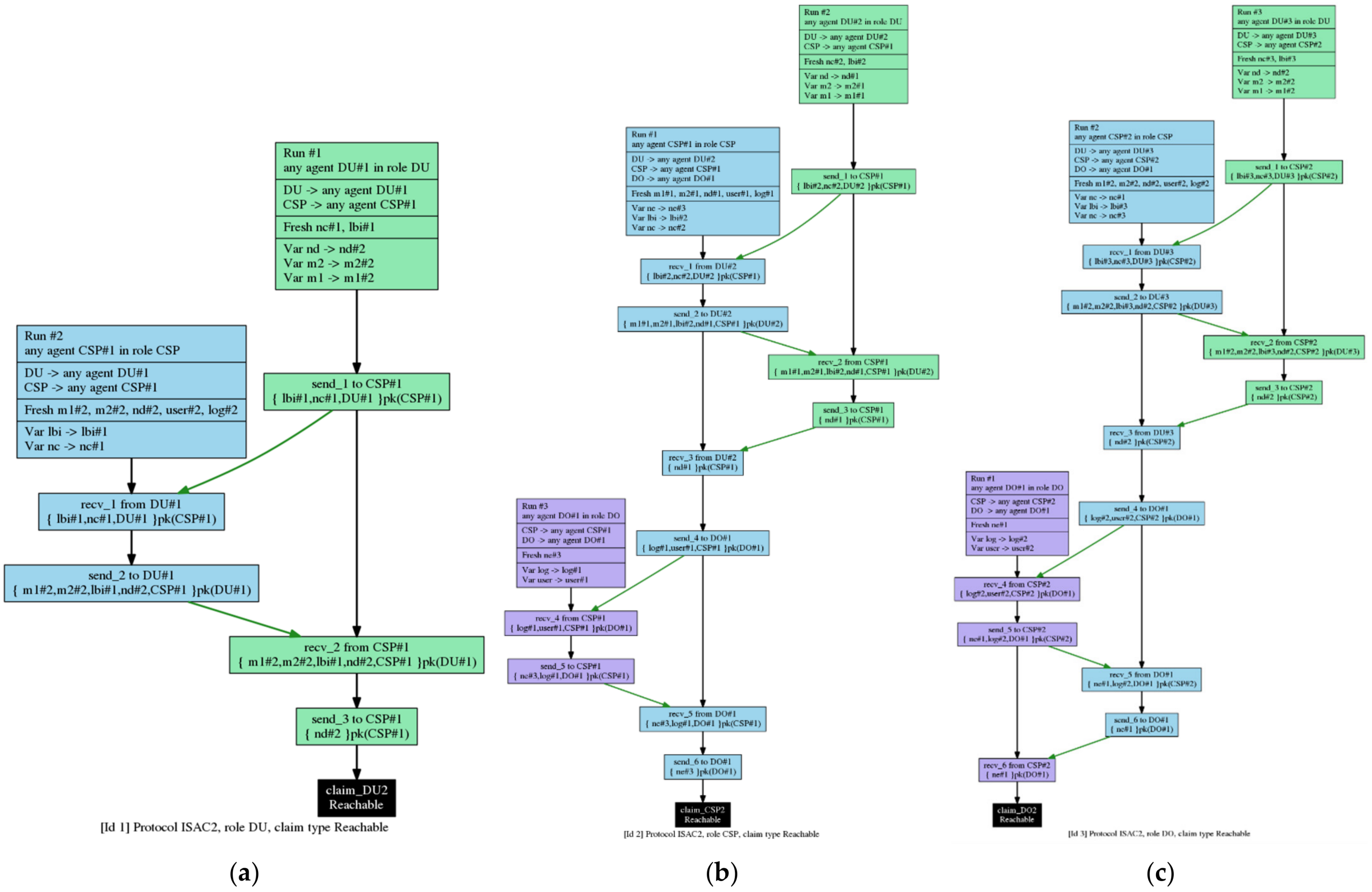


Figure 7. (**a**) ISAC2 Pattern Scheme—role DU; (**b**) ISAC2 Pattern Scheme—role CSP; (**c**) ISAC2 Pattern Scheme—role DO.

Figure 11b shows exactly one trace pattern and a reachable result in the results phase of the Third Party Auditor and the Data User roles. Therefore, this result protocol has only one pattern. The certainty of this pattern has been confirmed by the Third Party Auditor and Data User roles. This ISAC4 protocol result is only communicated between the Third Party Auditor and the Data User. Thus, there is no possibility of an attack on the ISAC4 protocol.

Based on the proposed PURA-SCIS protocol, various security services can be obtained. Security is focused on providing confidentiality for cyber incident information in cyber incident information-sharing networks. The security comparison is described in Table 4. The security properties comparison is based on the data-sharing security process proposed by PURA-SCIS protocol with the previous research.

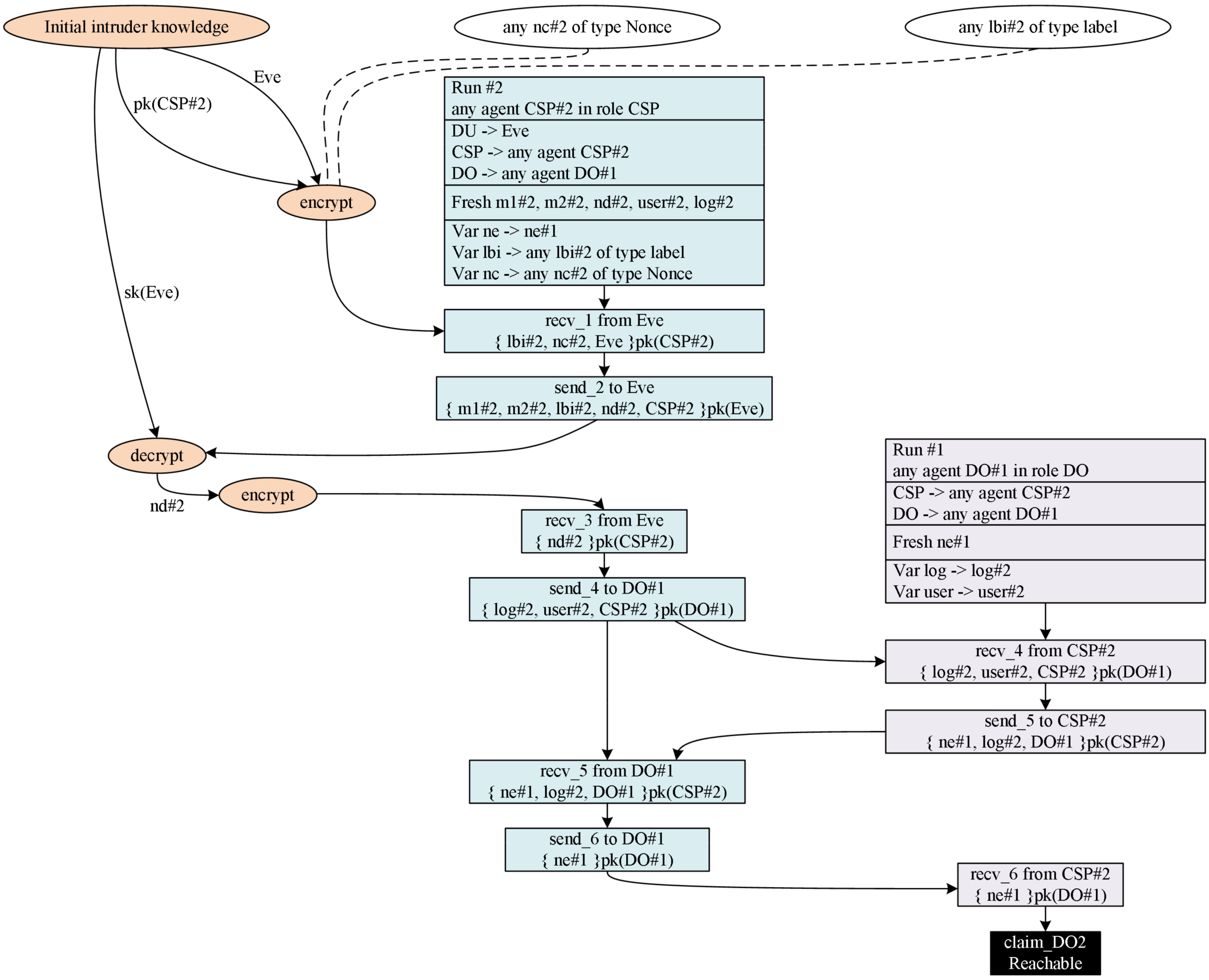
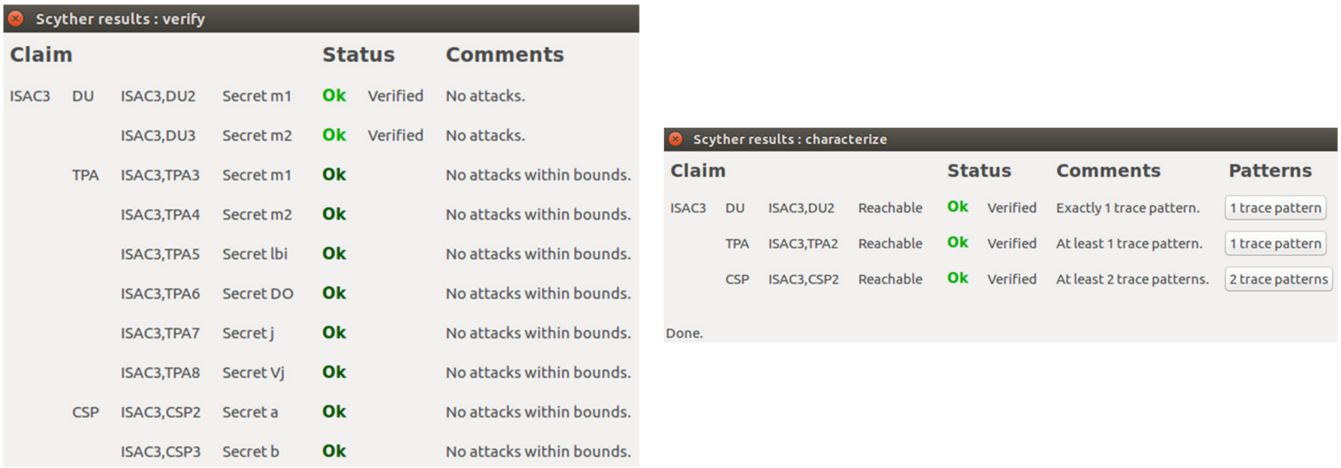


Figure 8. ISAC2 Pattern Scheme Attack.



Claim				Status		Comments
ISAC3	DU	ISAC3,DU2	Secret m1	Ok	Verified	No attacks.
		ISAC3,DU3	Secret m2	Ok	Verified	No attacks.
	TPA	ISAC3,TPA3	Secret m1	Ok		No attacks within bounds.
		ISAC3,TPA4	Secret m2	Ok		No attacks within bounds.
		ISAC3,TPA5	Secret lbi	Ok		No attacks within bounds.
		ISAC3,TPA6	Secret DO	Ok		No attacks within bounds.
		ISAC3,TPA7	Secret j	Ok		No attacks within bounds.
		ISAC3,TPA8	Secret Vj	Ok		No attacks within bounds.
	CSP	ISAC3,CSP2	Secret a	Ok		No attacks within bounds.
		ISAC3,CSP3	Secret b	Ok		No attacks within bounds.

(**a**)

Claim				Status		Comments	Patterns
ISAC3	DU	ISAC3,DU2	Reachable	Ok	Verified	Exactly 1 trace pattern.	1 trace pattern
	TPA	ISAC3,TPA2	Reachable	Ok	Verified	At least 1 trace pattern.	1 trace pattern
	CSP	ISAC3,CSP2	Reachable	Ok	Verified	At least 2 trace patterns.	2 trace patterns

Done.

(**b**)

Figure 9. (**a**) ISAC3 Verification Result; (**b**) ISAC3 Pattern Result.

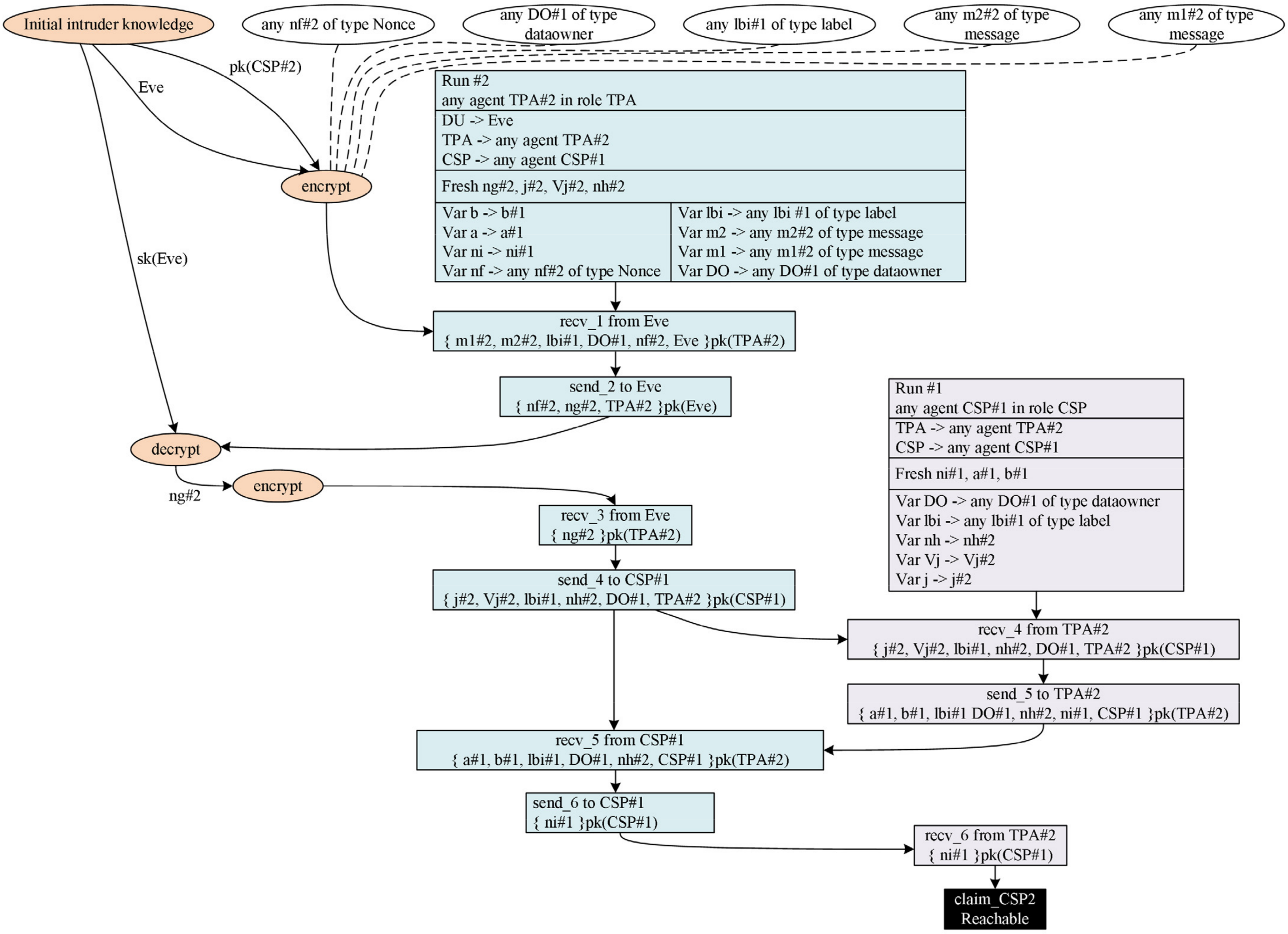
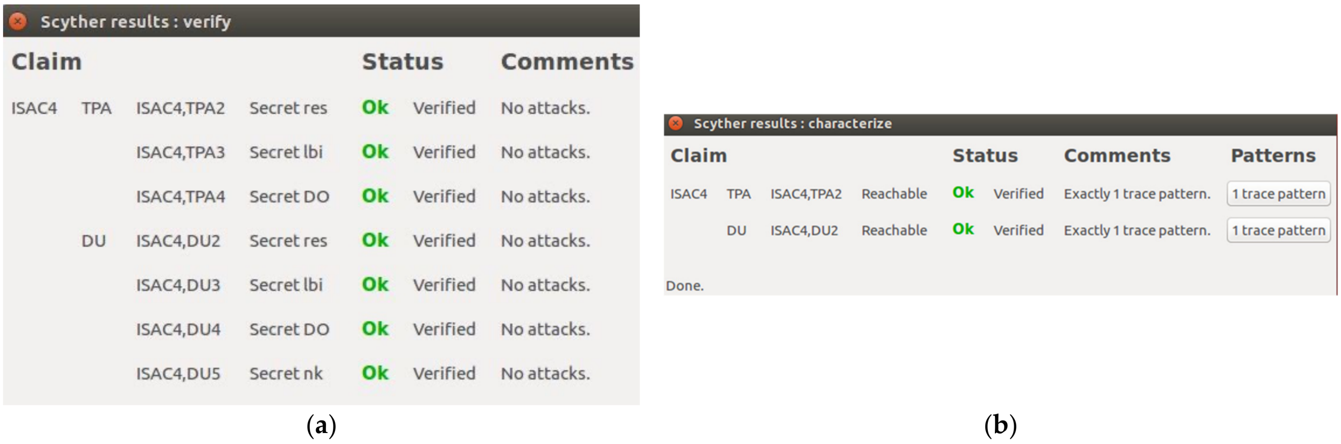

Initial intruder knowledge
any nf#2 of type Nonce
any DO#1 of type dataowner
any lbi#1 of type label
any m2#2 of type message
any m1#2 of type message
pk(CSP#2)
Eve
encrypt
sk(Eve)
Run #2
any agent TPA#2 in role TPA
DU -> Eve
TPA -> any agent TPA#2
CSP -> any agent CSP#1
Fresh ng#2, j#2, Vj#2, nh#2
Var b -> b#1
Var a -> a#1
Var ni -> ni#1
Var nf -> any nf#2 of type Nonce
Var lbi -> any lbi #1 of type label
Var m2 -> any m2#2 of type message
Var m1 -> any m1#2 of type message
Var DO -> any DO#1 of type dataowner
recv_1 from Eve
{ m1#2, m2#2, lbi#1, DO#1, nf#2, Eve }pk(TPA#2)
send_2 to Eve
{ nf#2, ng#2, TPA#2 }pk(Eve)
decrypt
ng#2
encrypt
recv_3 from Eve
{ ng#2 }pk(TPA#2)
send_4 to CSP#1
{ j#2, Vj#2, lbi#1, nh#2, DO#1, TPA#2 }pk(CSP#1)
Run #1
any agent CSP#1 in role CSP
TPA -> any agent TPA#2
CSP -> any agent CSP#1
Fresh ni#1, a#1, b#1
Var DO -> any DO#1 of type dataowner
Var lbi -> any lbi#1 of type label
Var nh -> nh#2
Var Vj -> Vj#2
Var j -> j#2
recv_4 from TPA#2
{ j#2, Vj#2, lbi#1, nh#2, DO#1, TPA#2 }pk(CSP#1)
send_5 to TPA#2
{ a#1, b#1, lbi#1 DO#1, nh#2, ni#1, CSP#1 }pk(TPA#2)
recv_5 from CSP#1
{ a#1, b#1, lbi#1, DO#1, nh#2, CSP#1 }pk(TPA#2)
send_6 to CSP#1
{ ni#1 }pk(CSP#1)
recv_6 from TPA#2
{ ni#1 }pk(CSP#1)
claim_CSP2
Reachable

Figure 10. ISAC3 Pattern Scheme Attack.



Scyther results : verify

Claim				Status		Comments
ISAC4	TPA	ISAC4,TPA2	Secret res	Ok	Verified	No attacks.
		ISAC4,TPA3	Secret lbi	Ok	Verified	No attacks.
		ISAC4,TPA4	Secret DO	Ok	Verified	No attacks.
	DU	ISAC4,DU2	Secret res	Ok	Verified	No attacks.
		ISAC4,DU3	Secret lbi	Ok	Verified	No attacks.
		ISAC4,DU4	Secret DO	Ok	Verified	No attacks.
		ISAC4,DU5	Secret nk	Ok	Verified	No attacks.

(**a**)

Scyther results : characterize

Claim				Status		Comments	Patterns
ISAC4	TPA	ISAC4,TPA2	Reachable	Ok	Verified	Exactly 1 trace pattern.	1 trace pattern
	DU	ISAC4,DU2	Reachable	Ok	Verified	Exactly 1 trace pattern.	1 trace pattern

Done.

(**b**)

Figure 11. (**a**) ISAC4 Verification Result; (**b**) ISAC4 Pattern Result.

The proposed protocol exploits the security properties shown in Table 4. The advantage of the PURA-SCIS protocol is providing private information sharing with data confidentiality via a secure protocol by basing security on mathematical calculations proposed by Ming and Shi in [17]. The PURA-SCIS protocol has the advantage of private information sharing where the cloud-based storage used is a specific private cloud for organizations in the sector that join the system. In addition, certificateless provable data possession provides data privacy for organizations that join the network.

Table 4. Comparison of Various Data Sharing Research.

Schemes	Security Properties					
	Public Verifiability for All Entity	Blockless Verification	Data Privacy Preservation	Identity Privacy Preservation and Traceability	Private Information Sharing	Data Confidentiality
Fan et al. [31]	√	X	√	√	√	X
Ming & Shi [17]	√	√	√	√	X	X
Zhang et al. [11]	√	X	√	X	√	√
Zhen et al. [13]	√	X	√	√	X	√
Shen et al. [19]	√	X	√	√	√	X
Wei et al. [3]	√	X	√	X	√	√
Proposed PURA-SCIS Protocol	√	√	√	√	√	√

The PURA-SCIS protocol has also been limited so that only private information sharing can be made available. Conversely, the cyber incident information can be verified publicly, albeit with the limited entities that connect to the same network. All entities can perform the verification process, but only for entities in the cyber incident information sharing private cloud.

4.3. The Challenges of PURA-SCIS Protocol Implementation

The PURA-SCIS protocol can increase security for the information sharing process between entities in sectoral organizations. Cyber incident information sharing can be realized in a technology platform as a communication system between entities. This technology platform requires a set of information technology devices that are connected through a common network. Security of private cloud access also needs to be considered for legitimate entities. Private clouds' availability in providing sectoral organizations' cyber incident information services is also important outside the confidentiality context of the exchanged cyber incident information.

Implementation of information sharing such as ISAC in each sector in public or private organizations can have different information network models. The information network model is the flow of exchanged information between the entities. Information sharing protocols can be customized based on unclassified information, such as public information. Information sharing protocols should also be adaptable based on unclassified information such as public information. Unclassified cyber incident information has more important integrity issues than information confidentiality. Examples of unclassified information (TLP: white) are sectoral organizations' annual cyber incident reports, sectoral organizations' cyber threat intelligence term reports, and cyber security awareness documents for stakeholders and the public.

Public sectors such as the government have a unique and different bureaucracy compared to the private sector. The bureaucracy mechanism of information disclosure is a special issue for the government. The existence of government bureaucracies can be an ISAC special issue sector in performing an effective and efficient information-sharing business process. Therefore, the cyber incident information network model in the public sector, such as government, is an interesting issue for implementing the PURA-SCIS protocol, especially for local or country-state governments.

The implementation of the PURA-SCIS Protocol can be embedded into other information-sharing platforms. System automation can also be implemented without requiring additional resources or increasing information leakage vulnerability or human error. The cyber incident information sharing platform can be adapted to provide provable data possession to the owner. In addition, the application of the entity's public key can be provided in the cyber incident information-sharing business process. The public key is also important in the cyber incident information sharing process with public key infrastructure policies.

The utilization of entities' public keys cannot be separated from cryptographic key management. The public key has a key validity period, so a process is instigated for destroying and updating the public key. Therefore, public key management in the network also needs further regulation. Public key management also has a cryptographic key lifecycle organized into key management. In addition, the provision of incentives to motivate sectors to share information also needs consideration [24,41]. Distributing and storing public keys is an important part of the cyber incident information-sharing business process; therefore, the entity's public key management process can be integrated into cyber incident information-sharing platforms.

Cyber incident information sharing is also related to the role of sectoral organizations incorporated into private networks. The PURA-SCIS protocol describes the information sharing protocol with the entity's public key without revealing the organization's real identity. The relationship of the original organization's identity included in the information-sharing business process also needs to be kept private. Privacy becomes very important because the Key Generation Center stores the organization's real identity as a trusted third party.

Information classification in information sharing becomes important based on TLP classification. The entities' policy that is directly involved in information becomes a crucial aspect in exchanging sensitive cyber incident information by organizations. Information storage by the Cloud Service Provider is important for sensitive cyber incident information that is exchanged. The Cloud Service Provider is expected to protect the information stored in cloud storage by sectoral organizations. The security policy and mechanisms on the cloud service of the sectoral organizations should be regulated without harming the entities in the network. Cloud security must be managed and reviewed in the information store by the Cloud Service Provider and must include the implementation of the provable data possession between the Cloud Service Provider and the Third Party Auditor.

Organizations that are reluctant to share their information and tend to work alone for their reputation are a challenge for sectoral organizations. Information exchanged confidentiality can increase sharing information trust for organizations in certain sectors. Cybersecurity information sharing can be an important element in a country's cyber resilience. The approach of a government cybersecurity organization in a country becomes an important issue of the organization's willingness to participate in information sharing in each sector. Confidentiality of classified information should be an important trust issue for sectoral organizations. Conversely, other challenges can also come from the information shared by sectoral organizations that have low-quality information.

5. Conclusions

This paper proposed the novel PURA-SCIS protocol for cyber incident information sharing. PURA-SCIS links various entities among sectoral organizations, including data owners, data requesters, third-party auditors, cloud service providers, and key generation centers. PURA-SCIS facilitates the exchange of information with public-key security encryption between entities. The communication process can be adjusted for secure communication between entities in a network. The proposed protocol provides several security properties, including public verifiability for all entities, blockless verification, data privacy preservation, identity privacy preservation and traceability, private information sharing, and data confidentiality. Finally, the protocol can be implemented in selected private clouds in the cyber incident information-sharing process for sectoral organizations.

The main limitation of this research project is that the proposed protocol only focused on classified information (TLP: red or amber). Information classification also includes public information that does not require confidentiality guarantees but does require data integrity guarantees. The information network model can also differ according to the entity's role according to the respective business processes needed in each sectoral organization's ISAC. In future work, a cyber incident information-sharing model appropriate for private networks (sectoral-ISAC) or public networks (such as government-ISAC) will be created. The model will be adjusted based on the needs of the relevant public or private sector and the classification of information involved. Key establishment, distribution, and public-key management will be developed in cyber incident information-sharing. Cyber incident information can be further classified to determine policies on network information level handling.

Author Contributions: Conceptualization, F.A.P. and K.R.; methodology, F.A.P. and K.R.; software, F.A.P.; validation, K.R., T.S.G. and F.A.P.; formal analysis, F.A.P.; resources, F.A.P.; data curation, K.R. and T.S.G.; writing—original draft preparation, F.A.P. and N.H.; writing—review and editing, K.R., T.S.G. and N.H.; visualization, F.A.P. and T.S.G.; supervision, K.R. and T.S.G.; project administration, K.R. and N.H.; funding acquisition, K.R. and N.H. All authors have read and agreed to the published version of the manuscript.

Funding: This research is supported by Universitas Indonesia through Hibah PUTI Kolaborasi Internasional (2Q2) Scheme under contract number NKB-788/UN2.RST/HKP.05.00/2020, in which Prof. Dr-Ing. Kalamullah Ramli is the corresponding author. Ms Hayati is in PhD study supported by Beasiswa Unggulan Dosen Indonesia Dalam Negeri (BUDI-DN), Lembaga Pengelola Dana Pendidikan (LPDP), and a cooperation of the Ministry of Research and Higher Education and the Ministry of Finance of the Republic of Indonesia.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The protocol coded is openly available at the Github Repocitory: https://github.com/fandiputra/isacprotocol (accessed on 1 December 2021).

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results.

References

1. Zrahia, A. Threat intelligence sharing between cybersecurity vendors: Network, dyadic, and agent views. *J. Cybersecur.* **2018**, *4*, 1–16. [CrossRef]
2. Vakilinia, I.; Sengupta, S. Fair and private rewarding in a coalitional game of cybersecurity information sharing. *IET Inf. Secur.* **2019**, *13*, 530–540. [CrossRef]
3. Wei, J.; Liu, W.; Hu, X. Secure data sharing in cloud computing using revocable-storage identity-based encryption. *IEEE Trans. Cloud Comput.* **2016**, *6*, 1136–1148. [CrossRef]
4. Shen, J.; Zhou, T.; He, D.; Zhang, Y.; Sun, X.; Xiang, Y. Block Design-Based Key Agreement for Group Data Sharing in Cloud Computing. *IEEE Trans. Dependable Secur. Comput.* **2019**, *16*, 996–1010. [CrossRef]
5. Wang, N.; Cai, Y.; Fu, J.; Chen, X. Information privacy protection based on verifiable (t, n)-Threshold multi-secret sharing scheme. *IEEE Access* **2020**, *8*, 20799–20804. [CrossRef]
6. Ghernaouti, S.; Cellier, L.; Wanner, B. Information sharing in cybersecurity: Enhancing security, trust and privacy by capacity building. In Proceedings of the 2019 3rd Cyber Security in Networking Conference, CSNet, Quito, Ecuador, 23–25 October 2019; pp. 58–62. [CrossRef]
7. Wagner, T.D.; Mahbub, K.; Palomar, E.; Abdallah, A.E. Cyber threat intelligence sharing: Survey and research directions. *Comput. Secur.* **2019**, *87*, 101589. [CrossRef]
8. Guo, B.; Deng, X.; Tian, J.; Guan, Q.; Zheng, X. A Secure Incentive Mechanism for Competitive Organization Data Sharing: A Contract Theoretic Approach. *IEEE Access* **2019**, *7*, 60067–60078. [CrossRef]
9. Mermoud, A.; Keupp, M.M.; Huguenin, K.; Palmié, M.; David, D.P. To share or not to share: A behavioral perspective on human participation in security information sharing. *J. Cybersecur.* **2019**, *5*, 1–13. [CrossRef]
10. Yan, K.; Shen, W.; Jin, Q.; Lu, H. Emerging Privacy Issues and Solutions in Cyber-Enabled Sharing Services: From Multiple Perspectives. *IEEE Access* **2019**, *7*, 26031–26059. [CrossRef]
11. Zhang, L.; Cui, Y.; Mu, Y. Improving Security and Privacy Attribute Based Data Sharing in Cloud Computing. *IEEE Syst. J.* **2020**, *14*, 387–397. [CrossRef]
12. de Fuentes, J.M.; González-Manzano, L.; Tapiador, J.; Peris-Lopez, P. PRACIS: Privacy-preserving and aggregatable cybersecurity information sharing. *Comput. Secur.* **2017**, *69*, 127–141. [CrossRef]
13. Yang, Z.; Wang, W.; Huang, Y.; Li, X. Privacy-preserving public auditing scheme for data confidentiality and accountability in cloud storage. *Chin. J. Electron.* **2019**, *28*, 179–187. [CrossRef]
14. Loh, J.-C.n.; Heng, S.-H.; Tan, S.-Y. A Generic Framework for Accountable Optimistic Fair Exchange Protocol Fair Exchange Protocol. *Symmetry* **2019**, *11*, 285. [CrossRef]
15. Mihalkovich, A.; Sakalauskas, E.; Luksys, K. Key Exchange Protocol Defined over a Non-Commuting Group Based on an NP-Complete Decisional Problem. *Symmetry* **2020**, *12*, 1389. [CrossRef]

16. Harun, N.Z.; Zukarnain, Z.A.; Hanapi, Z.M.; Ahmad, I. Multi-Stage Quantum Secure Direct Communication Using Secure Shared Authentication Key. *Symmetry* **2020**, *12*, 1481. [CrossRef]
17. Ming, Y.; Shi, W. Efficient Privacy-Preserving Certificateless Provable Data Possession Scheme for Cloud Storage. *IEEE Access* **2019**, *7*, 122091–122105. [CrossRef]
18. Chuang, Y.-H.; Lei, C.-L.; Shiu, H.-J. How to Design a Secure Anonymous Authentication and Key Agreement Protocol for Multi-Server Environments and Prove Its Security. *Symmetry* **2021**, *13*, 1629. [CrossRef]
19. Shen, W.; Qin, J.; Yu, J.; Hao, R.; Hu, J. Enabling Identity-Based Integrity Auditing and Data Sharing with Sensitive Information Hiding for Secure Cloud Storage. *IEEE Trans. Inf. Forensics Secur.* **2018**, *14*, 331–346. [CrossRef]
20. Vakilinia, I.; Tosh, D.K.; Sengupta, S. Attribute based sharing in cybersecurity information exchange framework. *Simul. Ser.* **2017**, *49*, 68–73. [CrossRef]
21. Hong, M.Q.; Wang, P.Y.; Zhao, W.B. Homomorphic Encryption Scheme Based on Elliptic Curve Cryptography for Privacy Protection of Cloud Computing. In Proceedings of the 2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS), New York, NY, USA, 9–10 April 2016; pp. 152–157. [CrossRef]
22. Chaudhary, P.; Gupta, R.; Singh, A.; Majumder, P. Analysis and Comparison of Various Fully Homomorphic Encryption Techniques. In Proceedings of the 2019 International Conference on Computing, Power and Communication Technologies, GUCON, New Delhi, India, 27–28 September 2019; pp. 58–62.
23. European Union Agency for Cybersecurity. *Information Sharing and Analysis Centres (ISACs) Cooperative Models*; ENISA: Athens, Greece, 2018.
24. Koepke, P. Cybersecurity Information Sharing Incentives and Barriers. In *Working Paper CISL #2017-13*; MIT Management Sloan School: Cambridge, MA, USA, 2017.
25. Sedenberg, E.M.; Mulligan, D.K. Public Health as a Model for Cybersecurity Information Sharing. *Berkeley Technol. Law J.* **2015**, *30*, 1687.
26. Kollars, N.A.; Sellers, A. Trust and information sharing: ISACs and U.S. Policy. *J. Cyber Policy* **2016**, *1*, 265–277. [CrossRef]
27. Gil-Garcia, J.R.; Pardo, T.A.; De Tuya, M. Information Sharing as a Dimension of Smartness: Understanding Benefits and Challenges in Two Megacities. *Urban Aff. Rev.* **2019**, *57*, 8–34. [CrossRef]
28. Tresh, K.; Kovalsky, M. Toward Automated Information Sharing California: Cybersecurity Integration Center's approach to improve on the traditional information sharing models. *Cyber Def. Rev. JSTOR* **2018**, *3*, 23–32.
29. II, L.W.; Tsuchiya, M.; Repko, R. *Improving Cybersecurity Cooperation between the Governments of the United States and Japan*; SASAKAWA USA: Washington, DC, USA, 2020.
30. Yang, P.; Xiong, N.; Ren, J. Data Security and Privacy Protection for Cloud Storage: A Survey. *IEEE Access* **2020**, *8*, 131723–131740. [CrossRef]
31. Fan, Y.; Liao, Y.; Li, F.; Zhou, S.; Zhang, G. Identity-Based Auditing for Shared Cloud Data with Efficient and Secure Sensitive Information Hiding. *IEEE Access* **2019**, *7*, 114246–114260. [CrossRef]
32. Jin, H.; Luo, Y.; Li, P.; Mathew, J. A Review of Secure and Privacy-Preserving Medical Data Sharing. *IEEE Access* **2019**, *7*, 61656–61669. [CrossRef]
33. Cremers, C.J.F. The Scyther tool: Automatic verification of security protocols. *Comput. Aided Verif.* **2008**, *5423*, 414–418.
34. Cremers, C.; Mauw, S. *Operational Semantics and Verification of Security Protocols*; Springer: Berlin/Heidelberg, Germany, 2012.
35. Kahya, N.; Ghoualmi, N.; Lafourcade, P. Formal analysis of PKM using scyther tool. In Proceedings of the International Conference on Information Technology and e-Services (ICITeS), Sousse, Tunisia, 24–26 March 2012. [CrossRef]
36. Navas, R.E.; Toutain, L. LATe: A Lightweight Authenticated Time Synchronization Protocol for IoT. In Proceedings of the Global Internet of Things Summit (GIoTS), Bilbao, Spain, 4–7 June 2018.
37. Thammara, C. Efficient and Secure NFC Authentication for Mobile Payment Ensuring Fair Exchange Protocol. *Symmetry* **2020**, *12*, 1649. [CrossRef]
38. Madhoun, N.E.; Guenane, F.A.; Pujolle, G. A Cloud-Based Secure Authentication Protocol for Contactless-NFC Payment. In Proceedings of the IEEE International Conference on Cloud Networking (CLOUDNET), Niagara Falls, ON, Canada, 5–7 October 2015.
39. Shehada, D.; Yeun, C.Y.; Zemerly, M.J.; Qutayri, M.A.; Hammadi, Y.; Damiani, E.; Hu, J. BROSMAP: A Novel Broadcast Based Secure Mobile Agent Protocol for Distributed Service Applications. *Secur. Commun. Netw.* **2017**, *2017*. [CrossRef]
40. Palombo, H.M. A Comparative Study of Formal Verification Techniques for Authentication Protocols. Master's Thesis, University of South Florida, Hillsborough, CA, USA, 2015.
41. Naghizadeh, P.; Liu, M. Using Private and Public Assessments in Security Information Sharing Agreements. *IEEE Trans. Inf. Forensics Secur.* **2019**, *15*, 1801–1814. [CrossRef]