ECTI Transactions on Computer and Information Technology
Journal homepage: https://ph01.tci-thaijo.org/index.php/ecticit/
Published by the ECTI Association, Thailand, ISSN: 2286-9131

Secure Supply Chain Information Interchange using Distributed Trust Backbone

Potchara Pruksasri[1] and Suchart Khummanee[2]

ABSTRACT

International trade requires transparent visibility of the goods transportation. High-quality data related to containers is essential for container movement across the border speed. However, customs and port authorities face information incorrectness and inconsistency, which are significant determinants that decrease the performance of container clearance in supply chain activities. The Seamless Integrated Data Pipeline principle has been proposed to overcome the mentioned data quality shortcomings and enhance supply chain visibility. Based on the Data Pipeline idea, we proposed the Distributed Trust Backbone (DTB) as a model of secure information exchange between parties within the supply chain activity. However, the supply chain data is highly dynamic. Access control on dynamic resources is the key to enabling secure data exchange and clear visibility. We take this challenge up in this paper. We propose an access control mechanism based on the supply chain Data Pipeline concept and apply it to the DTB model. The elaboration on the concrete detail of the system is presented in this paper. The prototype has been developed and performed in the simulation tests. It reduces 58% of requesting data for supply chain activities. The results of the experiments show that our proposed method performs 100% access control to data with BigO(1) accessing the Access Control List. It can ensure that the information for decision-making in the supply chain is of high quality. The supply chain visibility is clearer and speeds up a modern information exchange system of supply chains.

Article information:

Keywords: Access Control, Data Pipeline, PKI, Digital Certificate, Supply Chains

Article history:
Received: July 8, 2024
Revised: October 24, 2024
Accepted: November 13, 2024
Published: November 30, 2024
(Online)

DOI: 10.37936/ecti-cit.2025191.257456

1. INTRODUCTION

Recently, international transportation has complicated processes from start to end. Each method includes relevant organizations, constantly changing depending on activities and transportation regulations. The dynamic change of relevant participants creates a complex channel of data exchange. However, the data exchange in the supply chain needs to be completed. For example, the exporter sends the export data to the transporter, which is then saved in the system before being forwarded to other relevant participants, such as sea carriers or authorities. This flow revealed data states that consist of send, save, and forward. Questions regarding the accuracy and completion of duplicate sending data, called second-handed data, contain a gap and error that would negatively affect the system and are then put on the table.

The form of data sent from the sender to the receiver in the supply chain is called data push and causes several problems related to data security. The concept of data exchange with the contrary form using data as requested or data pull gained more interest. Hence, the possibility of using the data pull instead of the former data exchange scheme was studied [1]. The data pull scheme focused on accessing data from the origin or the owner through a computer network system based on the hypothesis that the data received from the owner was more accurate and reliable than other sources. In addition, the data recorded in the source needs to be completed. Additional data might be added later in each process of transporting goods. The dynamically added data provided a complicated process of gaining complete data for further steps of transportation processing.

[1,2] The authors are with the Department of Computer Science, Faculty of Informatics, Mahasarakham University, Maha Sarakham, Thailand, E-mail: potchara.p@msu.ac.th and suchart.k@msu.ac.th
[2] Corresponding author: suchart.k@msu.ac.th

Thus, the control of data accuracy exchanged in the system is impressive.

The study of the data-pull model and data access indicated more challenges to developing an effective data communication system that could replace the existing one. Regarding data efficiency within the new system, qualified data is also required as the basis of the essential key to smoothly driving the data exchange mechanism. The competent data will enable greater visibility of the supply chain system. Control, consideration, and decision-making can be performed effectively and instantaneously because there are no doubts regarding the received data. At the outset, the design of data communication emphasizes the security of data. This paper proposes a data communication system with greater security through data pull to provide adequate supply chain systems.

The development of the Seamless Integrated Data pipeline principle, which uses data pull exchange, is studied [2] [3]. We adopt its concept into this work and divide it into two parts. Firstly, we design core components that allow accurate and secure data transfer from the source to the destination. Secondly, we create control protocols that indicate the operating method and process of secure data exchange. The Distributed Trust Backbone or DTB prototype system is implemented by setting up computer systems and software for each Data pipeline component. Six servers in Europe, Indonesia, and Thailand simulate data communication closest to the actual data communication. The data access control mechanism is created based on the type of supply chain components and security protocols; this led to the demonstration of the functional prototype.

This paper presents the design and model of data exchange based on the latest data pipeline concept, the DTB, which changes the current direction of data exchange from data pushes to data pulls. The basic design of core components and their roles are described together with the secure communication protocols that support the process for each element accurately and effectively. The prototype system is set up to simulate the data exchange based on the example supply chain activity.

2. BACKGROUND

2.1 Information Exchanging in Supply Chains

Importing and exporting goods in Thailand involves several steps and is relatively expensive compared to countries in the European Union (EU). An analysis has identified the main reasons for this. The Thai Customs Department takes 14 days for each process to coordinate between customs and importers and exporters for exporting containers, which is longer than in many countries in the European Union [4]. To address this issue, a proposal has been made to implement a Single Window System (SWS) in Thailand. This system would facilitate the exchange of electronic documents between government agencies (G2G) and between businesses and government organizations (B2G) under the supervision of the United Nations (UN) [5][6]. The SWS system is currently in use. Research has also examined data security responsibilities in the import and export process under SWS guidelines. It has identified potential problems in data exchange, along with suggestions and solutions to address these issues [4].

Business procedures are an essential factor in international trade. International trading generally uses a “Buy-Ship-Pay” model [7], similar to regular trade. The difference from regular trade is that it uses containers to transport goods across countries to their destinations, the primary method of transporting goods across countries today. Many containers arrive at the port daily, and inspecting every container of goods is impossible. Before importing into the destination country, selecting suspicious containers is a mechanism to reduce the number of containers required to be inspected. The “Green Lane concept” [8] clears containers into the country. The green lane procedure relies on information related to the transport of goods to assess the risk. Data is, therefore, critical in this process.

In practice, however, information related to containerized products often contains many errors, for example, due to the passing of incorrect information between two or more supply chain actors [1]. Incorrect information makes decision-making ineffective. Product information transmitted electronically through various systems may only sometimes be accurate or up-to-date upon reaching its destination. This error is mainly because product data is entered multiple times into the systems of different stakeholders (exporters, shippers, carriers, and customs). Each may have its own internal systems, and there may be intentional or unintentional errors in data entry. Incorrect information affects tax evasion attempts. Illegal transport of goods directly impacts the overall supply chain efficiency. The government may lose tax revenue and cause damage to the business. Therefore, developing a central system that connects product information in real-time is necessary. Measures to control data entry and edit and check data regularly must be accelerated. Therefore, the concept of a “Seamless Integrated Data Pipeline” [9] or simply “Data Pipeline” has been proposed. This efficient data exchange system is designed to support the exchange of information in international supply chains. A vital feature of this system is its reliance on the principle of acquiring quality information from the source of information [10], emphasizing the importance of data accuracy. The conceptual idea of the Data Pipeline can be seen from Fig. 1.

Dutch Customs proposes a new solution to address flawed supply chain data: the Seamless Integrated Data Pipeline or Data Pipeline. The main idea of the Data Pipeline system is that product data will be available to authorized partners as soon as it is sourced. Data will be accurate and reliable because it comes directly from the owner, reducing the need to duplicate potentially inaccurate data [12]. Real-time updates on product status will be provided, and all systems will be connected to a single pipeline. Stakeholders in the supply chain can share information conveniently. Based on this concept, the Data Pipeline system will result in accurate, up-to-date, and reliable data. To increase supply chain efficiency, reduce costs, prevent illegal transportation of goods, and increase transparency. However, the Data Pipeline concept is currently under development. Customs in the EU work together with other agencies to put this concept into practice today.

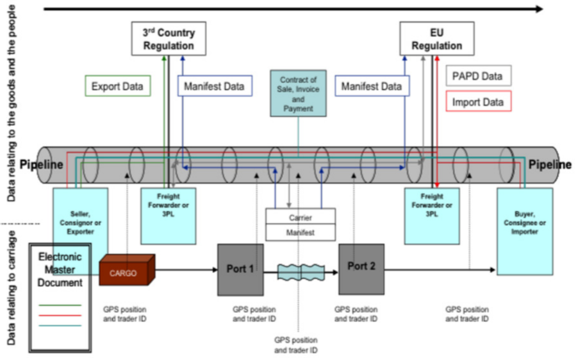

Data relating to the goods and the people
Data relating to carriage
3rd Country Regulation
EU Regulation
Export Data
Manifest Data
Contract of Sale, Invoice and Payment
Manifest Data
PAPD Data
Import Data
Pipeline
Pipeline
Seller, Consignor or Exporter
Freight Forwarder or 3PL
Carrier
Manifest
Freight Forwarder or 3PL
Buyer, Consignee or Importer
Electronic Master Document
CARGO
Port 1
Port 2
GPS position and trader ID
GPS position and trader ID
GPS position and trader ID
GPS position and trader ID
GPS position and trader ID

Fig.1: *Information flows of the supply chain Data Pipeline.*

The Data Pipeline is continuously being developed. Government agencies and business organizations collaborate to create effective data pipelines [13][14]. This research focuses on designing a secure data-sharing method under the Data Pipeline exchange system. It proposes a new model for a more secure Data Pipeline called the Distributed Trust Backbone (DTB). The DTB system aims to create a secure data exchange within the Data Pipeline based on principles. "Chain of Trust". The main idea of DTB is to allow only trusted actors to exchange information within the same community to create a secure and efficient Data Pipeline system. It facilitates reliable information exchange, reduces costs, and increases supply chain efficiency.

2.2 Information Security and Chain of Trust

Information security principles in information exchange systems, especially for new concepts like the Data Pipeline, focus on information security based on CIA principles [15]. It consists of three groups: Confidentiality, Integrity, and Availability. Confidentiality means keeping data private and inaccessible to unauthorized users. Data integrity means maintaining the integrity and accuracy of data throughout its lifecycle. Availability means ensuring that authorized users can access data whenever they need it. However, an additional principle is vital for modern multi-user data exchange systems: responsibility for the data itself. Data responsibility is identifying and tracking the actions of users who create, edit, or access data. This research uses these principles as the foundation for designing a secure data exchange system for the Data Pipeline, where the Data Pipeline must prevent unauthorized access to confidential data. This issue involves user authentication and data access control.

When addressing data integrity, the system must guarantee that data stays whole, consistent, and accurate during transmission. Crucial measures such as data validation and error checking should be implemented. Additionally, the system should be able to track user actions and identify the individuals responsible for creating, modifying, or accessing data. This concept is called "Accountability". It represents the final "A" in the CIA-A principles. By adhering to these principles, Data Pipelines ensures that data exchange is secure, reliable, and accountable. This is essential for efficient and dependable supply chain management.

The Chain of Trust results from applying CIA-A principles to information exchange because reliable information exchange between organizations requires a person to certify the reliability of each organization. The format of exchanged information is dynamic, necessitating the system's ability to adapt to changing data formats used by different user groups and support the increasing number of users [16]. The Chain of Trust principle, as referred to in Fig. 2, addresses this by introducing a Trusted Third Party (TTP). The TTP acts as an intermediary between the sender and receiver of information [17], verifying the identity of both parties and confirming the exchange's existence and integrity. Through these checks, the TTP builds trust between the sender and receiver, even if they do not know each other directly. This approach ensures secure communication, regardless of whether the parties are individuals, organizations, or computer systems, and clarifies the role of the TTP in establishing trust in information exchange.

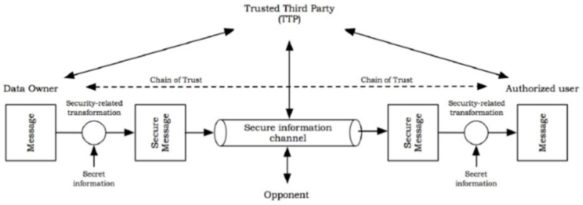


Fig.2: *The Chain of Trust.*

The advantage of a chain of trust is that it increases confidence and credibility in exchanging information through secure data communication channels. The system is more robust because a trusted middleman verifies it.

Applying a Chain of Trust to the Data Pipeline principles can create a secure and reliable foundation for exchanging data within an ever-changing supply chain system.

3. THE PROPOSED DTB CORE COMPONENTS

This Distributed Trusted Backbone (DTB) emphasizes the security of information systems within supply chains. It will create high-quality data in supply chain systems and speed up the process for an effective outcome. The data communication process in the DTB has to be redesigned and changed. The DTB architecture is designed based on stakeholders' data exchange on their activities in a supply chain, the so-called supply chain community, the group of stakeholders relevant to each situation or activity that will materialize dynamically depending on the activity of the supply chain. Indeed, it is found that each trade lane of transportation consists of many communities, which different stakeholders continually process. According to the study and data collection [9], DTB is designed based on widely acceptable security technology, i.e., PKI, to create a chain of trust among stakeholders in different supply chain activities. DTB can be revealed as a conceptual figure in Fig. 3.

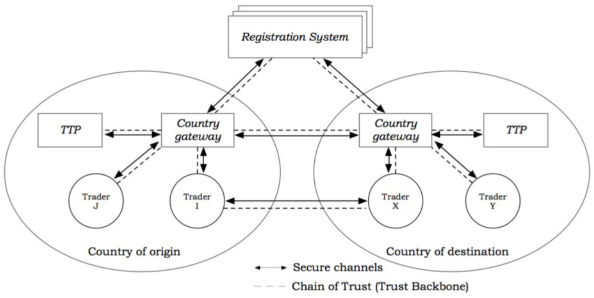


Fig.3: *Distributed Trust Backbone Architecture - DTB.*

DTB information exchange is used in a supply chain community when an actor requires information from another. The core components of DTB coordinate to affirm the individual actor's reliability and create a chain of trust between actors. Based on the analysis, we propose that the DTB consists of four main system elements: DTB Central (Registration), Gateway, Trusted Third Party, and Data Source systems [18].

3.1 DTB Central (Registration)

In DTB, the central system is designed to be the core system for administration related to the Data Pipeline. This system covers the registration of the Data Pipeline member, discovery of relevant members, and internal verification between the core components of the DTB in the data exchange process. This component stores the recorded collaboration of all members along with their relevant processes. The members of DTB can be divided into two groups: actors and system components.

Actors are the organizational computer systems related to the activities of the supply chain or any organization in the community. They consist of business partners, transporters, and authorities who require data exchange with different actors, for example, exporter or importer business partners, local truck services, freight forwarders or sea carriers in transporters, and customs or ministries of commerce in authorities. These actors exchange data throughout the transportation lanes, from the origin to the destination. The diversity of actors depends on an individual country's transportation and governance process. Consequently, actors must register as DTB members to exchange data via each organization's computer system.

System components are coordinated computer systems aiming to support the data exchange of international actors in DTB, depending on the country's context. These include the Registration, the Gateway, and Trust Third Parties systems. In theory, the registration system's design is considered the single central system that contains the data source of all members operating supply chain activities. It is simple and convenient to access and is called a single virtual registration system. In practice, a registration system is a set of connecting and processing registration systems in the form of cloud computing and can be located anywhere. Presently, the connection between sites is linked by high-speed networking worldwide. Therefore, the site's location is not a barrier to establishing a registration system for operators in different locations.

The infrastructure design of a DTB registration system was based on the technology of cloud computing and the Internet between the user and system or system and system instead of a closed system and private network. Moreover, data communication is gradually increasing, which influences the number of user-generated content (UGC) or the information created by the user. Similar to a supply chain system, each transportation consists of new operators; therefore, the DTB data of different operators must be collected in a secure location with easy accessibility, which can be fulfilled by cloud computing.

3.2 Gateway Systems

An international supply chain system is relevant to stakeholders spread worldwide. The product information must always be sent to the operators for consideration before the product arrives. The stakeholders who live in different countries are to exchange product information continuously. The data exchange between stakeholders, but not all data to all stakeholders, can be exchanged freely since the transportation policy differs in other countries. Some countries' policies promote electronic data exchange to hasten transportation, e.g., countries in Europe, the USA, or Canada. Conversely, some countries may not allow free data access or exchange due to political concerns or country instability. The Gateway system would support the data exchange of related information, enabling the international connection of members in other countries.

The Gateway system was designed to control and exchange data between countries following regulations related to electronic data exchange. All countries that coordinate data exchange processing using a Data Pipeline are to set up their Gateway system as an entry point of data exchange related to import transportation. The Gateway system will approve the request or transaction at an international level as the first point of consideration by the data exchange policy between the countries. Some requests are only accepted if they are relevant to the signed policy. Therefore, Gateway's role is to extract the data requested from other countries, especially countries with an exchange policy and bilateral agreement.

The architecture of the Gateway system is similar to that of the Registration system. It is a single virtual system with an interface that links DTB members who request to exchange data with overseas members. The system must also be continually able to extend its capabilities. Thus, forming a Gateway system in cloud computing is suitable because it is qualified to support both scalability and availability. Set up their Gateway system as an entry point of data exchange related to import transportation. The Gateway system will approve the request or transaction at an international level as the first point of consideration in the data exchange policy between countries.

3.3 Trust Third Party Systems

The main feature of DTB data communication is that it can effectively affirm the system's members' reliability. Also, it has to be able to create a chain of trust between members for data exchange. The process of DTB, through a medium system, will confirm who is responsible as a supporter and can approve the reliability of a member in the system. In DTB, this is called a Trusted Third Party or TTP.

The Trusted Third Party supports the approval process and confirmation of members in the system. TTP generally refers to the Certificate Authority based on PKI technology. Actors such as traders and authorities must register for identification to the Certificate Authority or CA to obtain a digital certificate and communicate with others in the secure channel using a digital certificate. The CA plays the role of the country's TTP. However, when the actors in the country used a different CA, problems with the system with a digital certificate were found. The DTB should use the trust model system as Root CA since it is simple and suitable to the country's environment. Many countries, such as The Netherlands and Thailand, offer the National Root CA for their member [4]. Overseas traders can check and assure traders under the confirmation of the Root CA within those countries. For example, the EU operates an electronic identity (eID) management backbone across Europe under the name of the STORK-eID Framework [13]. This project is responsible for confirming electronic service accessibility, including supply chain systems using central systems or TTP for identification. The system of eID guarantees that the individual or organization in the EU is required to exchange electronic data across the country. Member countries accept STORK-eID and reduce the problem of user identification. Nowadays, more than 550 organizations have become members of STORK-eID.

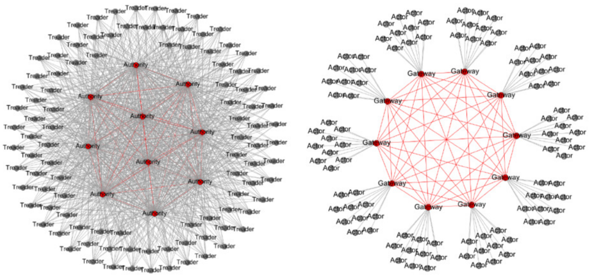
Based on a recent study, the design of DTB highlights the advantages of identity verification before data exchange as the main element in affirming the members' reliability, emphasizing the application of PKI technology and digital certificates. These are the critical elements in creating a chain of trust. DTB members must register for national TTP to gain a digital certificate. When registered, the TTP of the individual's country will record the member's information, which has been approved and is reliable. Consequently, at the start of the DTB data exchange, TTP will check the member's status in collaboration with Gateway and request the information from the partner country. Suppose the TTP of the partner country verifies the member's reliability.

3.4 Data Source Systems

The final core component of DTB is the data source system related to transportation activities. As stated, the data communication in a Data Pipeline was designed as a data pull, which is entirely different from this current system. Especially the data on transportation collected at the origin was only accessed and retrieved from the authorized person. The data source is the computer system that always supports the data retrieved from the operators. The transportation operators in each trade lane included business partners, transporters, and authorities to provide the system for data service. It reveals that the product data will be recorded at the origin and will not be duplicated or saved elsewhere. The data will be a unique and up-to-date data source.

Moreover, the data in the source has to interface to allow other operators to access the data. The person wishing to access data has to link through each data source's specified secure channel, such as Secure Web Services. This web service includes RESTful API protocols, which consist of an access code using the digital certificate from registration to verify the identity with the country's TTP. Since data is diverse within supply chains in each country, the data exchanged in DTB will be formed into the same pattern or standard, and the duplicated data will be merged to facilitate a similar data source method. Data harmonization to reach the standards of data sets exchanged in DTB is essential to exchange data between data sources. As a result, at each step of data exchange, the data source's format should relate to the standard of data format, which may be XML, JSON, or any programming language agreed upon by the DTB user.

The Distributed Trust Backbone (DTB) is the infrastructure presented for data exchange security with the Seamless Integrated Data Pipeline concept based on Public Key Infrastructure Technology. Core components have been designed based on data communication in a supply chain community studied from actual trade lanes. It approves the reliability of DTB members and develops a chain of trust between data source systems. The DTB represents a data exchange model within a new supply chain, which will enhance the reliability and quality of transportation information. Moreover, the structure of DTB can resolve the complexity of global data exchange. Fig. 4 shows that if stakeholders of the supply chain system currently contain the amount of n where they directly exchange the data, the number of communication links will be at n2. However, when the data is exchanged through the DTB structure using the Gateway system, the amount of m where m is much lower than n. Then, the number of communication links will decrease to m2n. It implies that the complexity of data communication decreases, which is one factor that improves the smooth running of a supply chain.



(a) Current supply chain system (b) The Data Pipeline with DTB

Fig.4: *The complexity of members in the DTB.*

The complexity has been significantly reduced by transitioning from a mesh network to a star network topology. In a mesh network, each node is connected to every other node, resulting in a complex web of interconnections. This complexity can lead to increased data traffic, higher energy consumption, and slower data transmission speeds. On the other hand, a star network topology simplifies the system by connecting all nodes to a central hub, reducing the overall complexity of the network. This complexity reduction directly impacts the system's cost, energy consumption, data transmission speed, and routing to data sources. Additionally, the network's scalability is improved by segmenting network groups into subgroups, making it easier, safer, and smoother to increase the number of communication nodes.

4. THE PROPOSED SECURE COMMUNICATION PROTOCOLS

The data communication protocol is designed to connect the members of a DTB system. The previous section discussed the DTB system with the registration system (RS), which collects the data of all members. RS uses the cloud computing system as it can cope with flexible sizing and can support processes with more excellent proficiency. We suggest establishing gateway systems to bridge connections between members from different countries. Moreover, each country has to provide an identification system to verify members' reliability as a trusted third party related to the old and new systems. Therefore, a computer system of core components has been designed with a protocol to control and coordinate data communication [10], which is designed into three subprotocols as follows:

4.1 Registration Protocol

The initial protocol registers all actors in a supply chain as members of the DTB system. For identification and reliability, all members must comply with the registration process shown in Fig. 5.

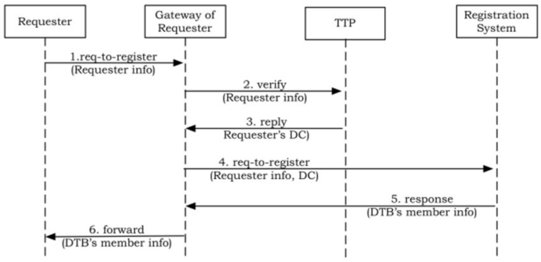

Requester
Gateway of Requester
TTP
Registration System
1.req-to-register (Requester info)
2. verify (Requester info)
3. reply Requester's DC)
4. req-to-register (Requester info, DC)
5. response (DTB's member info)
6. forward (DTB's member info)

Fig.5: *Registration Protocol.*

The protocol design shows the registration process and verifies the actor's reliability to gain credible membership within the DTB system.

Protocol description:

Step 1: The initial stage starts with the requester, an actor applying to become a member and submitting an electronic registration request through their country's Gateway system. The request includes essential information, such as the organization's name, network address, contact person, and the Trusted Third Party (TTP) who can certify the actor.

Step 2: Upon receiving this request, the Gateway, a trusted entity, contacts the TTP specified by the applicant to request confirmation and verification of reliability. This step underscores the Gateway's crucial role in ensuring the integrity of the DTB system.

Step 3: TTP accepts the request and approves the applicant's information. Any TTP may be chosen as long as the TTP serves in the applicant's country. However, the selected TTP has to provide the channel for Gateway requests. For instance, TTP receives the request through a web service. When the registration at TTP has been approved, TTP will send the result and identification of the actor to Gateway along with the digital certificate.

Step 4: Gateway receives the identification result from TTP through various channels, such as a web service. The requester is verified as reliable enough to become a member of DTB. Gateway then sends all registered information and the requester's digital certificate to the registration system, where the data is saved. The process of actor verification enables new credible members to exchange data. The registration system saves the connection data of the specific actor for future use.

Step 5: The registration system prepares the recorded information of members, especially the ID of the DTB, which will then be sent back to the Gateway system of the specific actor.

Step 6: This final step concludes with the actor who initiated the registration receiving confirmation of their DTB membership. This marks the successful culmination of the registration protocol, with the actor now a credible member of the DTB system.

4.2 Discovery Protocol

After the registration process, members can exchange data with others. However, a member (requester) most likely needs another member's digital certificate or contact details (data owner). Equally, the data owner would need more information regarding this requester. Solving the mentioned situation, we proposed the Discovery protocol that supports discovering members' information. The search members' data has been collected in the registration system. However, some essential information, such as the member's digital certificate, is collected by the individual organization or TTP rather than RS. It is easy to find general information regarding members because all the data will already be saved in RS. However, it is not easy to obtain a member's digital certificate. The process of discovery protocol is shown in Fig. 6.

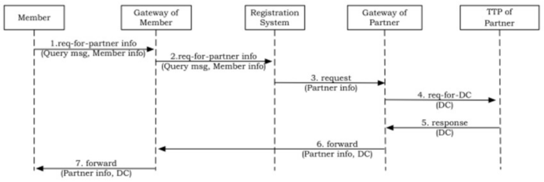


Fig.6: *Discovery Protocol.*

Protocol description:

Step 1: The protocol starts when members request data, or requesters create a request-for-partner-info, known as query messages. Alternatively, the message is sent to the Gateway system in the requester's country since the gateway system acts as the medium for connecting members to other core components.

Step 2: Gateway will start proving the requester's reliability by checking the requester and TTP where the member has been registered. If the results reveal the requester is reliable, the Gateway system will forward the request to the registration system (RS).

Step 3: The RS will request up-to-date information regarding the member, especially the searching organization's digital certificate with their country's Gateway system. Since RS does not have updated digital certificates, this data is requested of the member's TTP via the Gateway system.

Step 4: When the Gateway system receives the request, it will ask the member's TTP for an updated digital certificate.

Step 5: The member's TTP relays the digital certificate to the Gateway system. The TTP will notify the requester if a problem is found with the certificate, such as an expired one.

Step 6: Similar to step 4, the Gateway system acts as a medium to connect different core components and will forward the data to the requester's Gateway system.

Step 7: Finally, the requested information and the member's digital certificate will be sent to the requester; this can be relied on as accurate and up-to-date.

4.3 Identification and Authentication Protocol

To connect with partners, related data and security must be checked, especially the identification and authentication of members before data exchange, to create a chain of trust. The member must verify the reliability of both sides. The identification and authentication protocol is shown in Fig. 7.

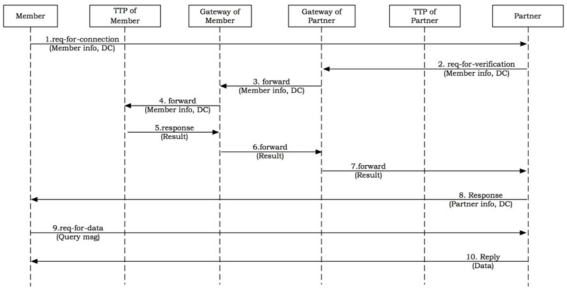


Fig.7: *Identification and Authentication Protocol.*

Protocol description:

Step 1: When the partner's data is needed to establish the identification and authentication of members in DTB, the process is initiated. Requesters (members) send a connection request message to the partner's network address. This message contains the requester's details, including their network address, name, contact number, and digital certificate. The partner needs these details to conduct the verification process.

Step 2: The partner receiving the request must prove the requesting member's reliability, which DTB's core components will verify. The partner's request will be sent to their country's Gateway system for reliable verification. The member's request for information will also be attached to the request for reliable verification.

Step 3: The Gateway system acts as a bridge between countries. The Gateway system of the partner country sends the request to the requester's gateway to check for TTP reliability in the requester's country.

Step 4: The requester's Gateway system will ask the country's TTP to prove the requester's reliability. According to the registration protocol, all members must provide an approved TTP. The TTP also checks and confirms the requester's reliability in this case.

Step 5: The result will be sent to the Gateway system.

Step 6: The Gateway system will forward this to the partner's gateway since it only transfers the data.

Step 7: The Gateway system will forward this to the partner's gateway since it only transfers the data.

Step 8: If the requester is proven reliable, the information is sent directly to the requester and the partner's digital certificate. This state shows that the identification and authentication are complete. This indicates that the identification and authentication are complete. After that, data can be processed for data exchange between members for information unrelated to the system's core component. The exchanged data will be directed through a secure web service with an access code for security throughout the data exchange session.

5. THE PROPOSED DATA ACCESS CONTROL MECHANISM

5.1 Supply chain community and relations

The data access control mechanism operates on the computer system of the data source, whether there is a trader, a transporter, or a responsible government agency. The exchanged information is always stored in the data source. Accessing information in the form of data pulled from the data source obtains the correct and up-to-date information. Applying for a tax privilege using the certificate of origin product information, a case study of the research, we consider the actors involved in the exchange of information. It can be shown as a relevant data exchange community (Community), as shown in Fig. 8.

Four organizations are involved in the information exchange: the exporter, the certification authority, the customs, and the importer. This community exchanges information using data pull, storing data at the data source. As a result, access control mechanisms are utilized to store those data.

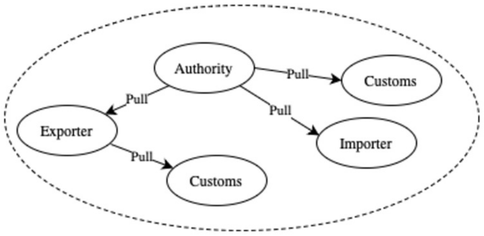


Fig.8: *Data exchange community.*

The data exchange operations with other organizations in the Community and ongoing transport activity determine data access control. For each request, the data source must assign access rights to whoever is involved, and the request is called a Transaction [19].

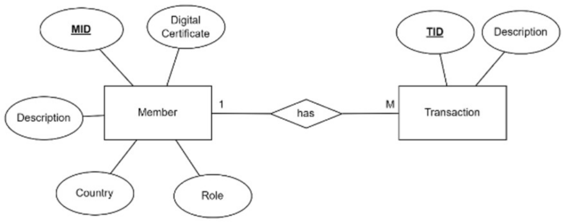


Fig.9: *The relationship between organizational data and data operations.*

The Member entity in the Community deals with information such as the unique agency number, digital certificate, and details of organizations, countries, and roles in the Community. They are correlated with data operations (Transactions) prepared for requests from relevant. One entity has a relationship with N data items (Transactions).

5.2 Access rights and data processing

Transaction data stored in the system consists of data fields and operations. These data fields are standard data that are analyzed, designed, and accepted for information exchange in the supply chain. They vary depending on each supply chain's activities. This research uses data based on the ATIGA Form D, established standards for ASEAN countries.

Let f_1, f_2, f_3, ..., be the data fields of the Transaction item, which refers to Certificate of Origin information (ATIGA Form D) shared within the organization, which can be written as a function as

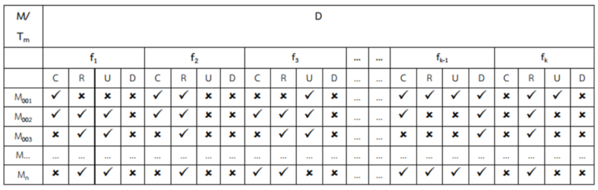
$$M_{n,Tm} \rightarrow D(f_1, f_2, f_3, \ldots, f_k) \qquad (1)$$

Where D is the domain of f_1, f_2, f_3, ..., f_k

he above functions can be expressed as the relationship of M_n, T_m, and D, called the Permission

Policy Mapping table, as shown in Table 1.

Table 1: *The permission policy mapping table.*



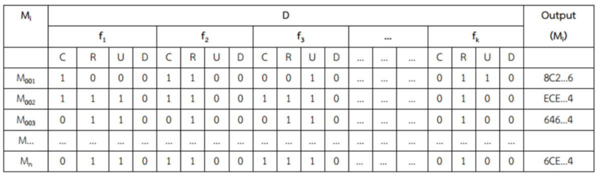
M/ T_m	D																					
	f_1				f_2				f_3				...	...	f_{k-1}				f_k			
	C	R	U	D	C	R	U	D	C	R	U	D	...	...	C	R	U	D	C	R	U	D
M_{001}	✓	×	×	×	✓	✓	×	×	×	×	✓	×	...	...	✓	✓	✓	✓	×	✓	✓	×
M_{002}	✓	✓	✓	×	✓	✓	×	×	✓	✓	✓	×	...	...	✓	×	×	✓	×	✓	×	×
M_{003}	×	✓	✓	×	×	✓	×	×	×	✓	✓	×	...	...	×	×	×	✓	×	✓	×	×
M...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...
M_n	×	✓	✓	×	×	✓	×	×	✓	✓	×	×	...	...	✓	✓	✓	✓	×	✓	×	×

The permission policy mapping table describes the data action permissions as follows.

C = the right to create data (Create).
R = the right to read data (Read).
U = the right to correct information (Update).
D = the right to delete the data (Delete).

M_i, T_m refers to the memberi, who has the privilege to commit on the item in the transaction m. Each member has the data action permission of × (not eligible), replacing the value with 0, and ✓ (eligible), replacing the value with 1. Therefore, the data action permissions were replaced with 0 and 1 (Binary) and converted to hexadecimal. It will provide the permission policy of the member associated with that transaction, as depicted in Table 2.

Table 2: *The binary permission policy mapping table.*



M_i	D																			Output (M_i)
	f_1				f_2				f_3				...			f_k				
	C	R	U	D	C	R	U	D	C	R	U	D	...	...	...	C	R	U	D	
M_{001}	1	0	0	0	1	1	0	0	0	0	1	0	...	...	...	0	1	1	0	8C2...6
M_{002}	1	1	1	0	1	1	0	0	1	1	1	0	...	...	...	0	1	0	0	ECE...4
M_{003}	0	1	1	0	0	1	0	0	0	1	1	0	...	...	...	0	1	0	0	646...4
M...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	
M_n	0	1	1	0	1	1	0	0	1	1	1	0	...	...	...	0	1	0	0	6CE...4

The sample data access rights of $M_{001,T001}$ can be calculated as Permission Policy as follows.

$$\begin{array}{rl} M_{001,T001} = & 1000|1100|0010|....|0110| \\ & \quad\downarrow \quad\;\; \downarrow \quad\;\; \downarrow \qquad\quad \downarrow \\ = & \quad 8 \quad\;\; C \quad\;\; 2 \;..... \quad 6 \end{array}$$

5.3 Memory managing

Information exchange in various activities creates diverse information exchanges, which requires a fast access control mechanism that supports every activity and meets massive requests. Therefore, authorization must be processed in the organization's memory system—one consideration when processing in memory is the size of the storage space that must be efficiently stored. The memory space can be calculated to illustrate the memory space efficiency of the permission policy napping designed as follows.

$$Memoryspace \;= \textit{number of relevant members x number of data fields x number of data access rights}$$

As an example, the memory space for the authorization of Certificates of Origin data exchange can be calculated as follows: 4 (organizations) × 190 (fields) × 1 (CRUD gives 1 byte) = 760 bytes, and further experimentally hypothesized that if the data has an average number of 190 fields (as an example), and the computer system has 1 gigabyte (1 GB) of memory space to store these access rights, then 1,000,000,000 / 760 = 1,315,789 permission policies can be stored.

The next step is to access those permissions to verify the requesting member after much access rights information has been successfully stored in memory. Accessing data in the worst case is accessed via sequential search, where access speeds based on processing values are equal to BigO(n). As the number of new members increases, the efficiency of access to permissions decreases over time. Therefore, a more efficient authorization is needed so that permissions access speeds are still possible rather than sequential.

Using efficient hashed storage can speed up access to the same amount of data as BigO(1). Perfect hashing is a possible hashing process. It guarantees that access to the hashed data is collision-free because the key to a hash must be constant. The critical value does not change while running, knowing all data to hash.

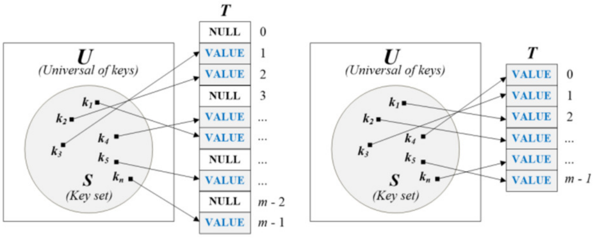


Fig.10: *Perfect hashing.*

Where S is the set of all keys to be hashed, say that the function 1} is the perfect hashing function for S when h injection on S and There are no critical collisions in S if (Fig. 10, left-hand side). Usually, the size of T (|T|) should be greater than the number of keys in S because it reduces the number of calculations made by the h function and the processing of duplicate keys. Because when a key passes the h function, the resulting value is duplicated. A new function from the provided group of functions must be selected to replace the original function h that processes any two keys and repeats. However, if the hash table size equals the number of keys in S (|T| = |S|), the hash becomes Minimal complete hashing, Shown in Fig. 10 (right). The data access speed in the slowest case of perfect hashing is BigO(1). After the hashing process, the access rights information is saved to the computer system's memory with the characteristics shown in Fig. 11.

M_{001} data is a unique member alias, such as a UUID. After the hash process, it obtains a memory location that will link to the memory member's permission policy repository.

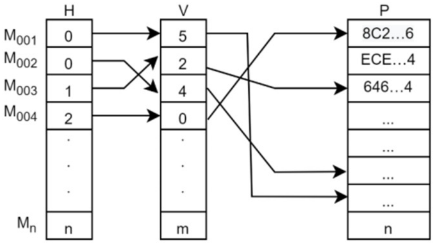


Fig.11: *Permission policies in memory space.*

5.4 Access Rights Verification

The requesting member submits the request via the Data Pipeline to the data source system, where the data is stored with the member's UUID, a unique key. The authorization process has the following steps.

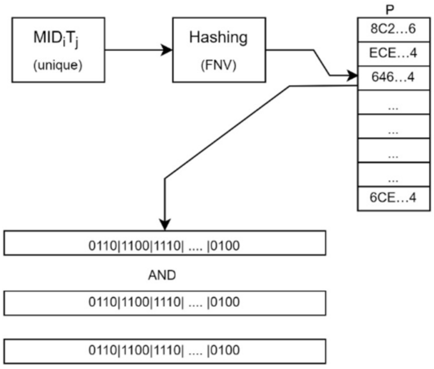


Fig.12: *Data access authorization procedures.*

Step 1: The requested member information, combined with the Transaction ID (Request for a Certificate of Origin), creates a unique key stored in the hash table that sets the rights of the owner of that information, such as the Department of Foreign Trade. Further, permissions are assigned once the certificate is issued electronically. Therefore, when using the perfect hashing process, this unique information is immediately accessible.

Step 2: After the hashing process, it obtains a memory location pointing to the requesting entity's permission policy index. If found, the requested member information is in the same community as the owner. The information has already been added, and the permission policy will be called out for use in the next authorization step.

Step 3: The permission policy is then converted to binary and mapped to the right of action (CRUD) with the respective data fields in every data field.

Step 4: The information requested by the requesting member is verified in the individual data fields. It uses the AND process, a high-speed verification process that grants access rights, as shown in the figure. If the result is 0, the requested action cannot be performed, but 1, the requested action, is allowed.

Finally, the request for that data is processed through access authorization. All the transaction data and the member's credentials are hashed. The hash data can be used to verify the data's integrity when it reaches its destination. It confirms the accuracy of the information that matches the data's origin.

6. PROTOTYPE AND EVALUATION

6.1 System Prototype

Creating prototype systems to simulate functionality is widely favored to prove the design concept. The solid model system simulates work under specified conditions. By creating this prototype system, it is divided into three parts:

Hardware and Infrastructure:

The DTB system infrastructure is set up using Amazon's cloud system, which has three main components: Registration System (RS), Gateway Systems (GW), and Data Source Systems (DS - Trader/Authority). The Registration System is a Virtual Private Server (VPS) system that is distributed around the world. The minimum level of machine capability that can work with the DTB system is chosen to be 2 CPU cores and 4 GB of memory. Cloud capabilities will support expansion (scalability) and continuity in processing (reliability) and can also change efficiency (performance) flexibly.

All created servers are assigned a domain name that allows them to be online on the Internet and communicate with each other. Researchers can change the domain name themselves using the Route53 service of AWS. The next part is the Gateway system, a virtual connection point for each country participating in data exchange. The Customs Department will generally be the administrator of this system. However, in testing, the system could not be installed on the Customs Department's system, so the system was replicated on AWS and installed in three test countries: Singapore, Thailand, and Indonesia. The Gateway system will be responsible for verifying and passing data. Therefore, using the cloud system will allow flexibility in capabilities, such as bandwidth. The last part will be the computer system of Trader and Authority called Data Source Systems, which simulates the exchange of data between them under the data pipeline concept to make the simulation more accurate and complete. Trader's system in Indonesia: Therefore it was created using the AWS cloud system in Australia, and the Authority system of Thailand was created using the Singapore cloud system to demonstrate system interoperability in different zones, as shown in Fig. 13.

A process monitoring agent system has been developed [20] to record information exchanged in this research. This agent will be linked to every system designed to record information exchange and express it in a format that is easy for researchers to understand.

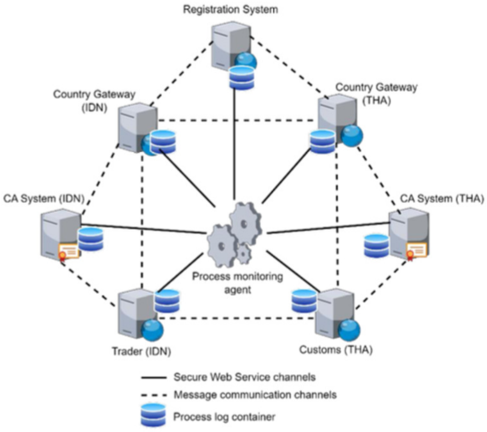
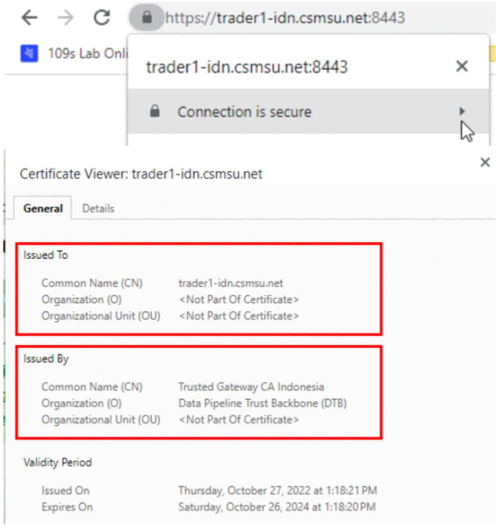


Fig.13: *DTB Prototype Infrastructure.*

Software Implementation:

In developing prototype software, the critical thing for exchanging information is to create a Chain of trust between actors, which will be based on the work of PKI Technology and Digital Certificates. Therefore, this research uses the open-source software EJBCA [21] to create Digital Certificates for every component. In DTB, EJBCA acts as a Trusted Third Party (TTP) that can verify the actors that exchange data in the system using the principles of Digital Certificate. Simulating TTP using EJBCA has the advantage that the software allows external systems to use various capabilities via a Web Service as a Restful API, making prototype system development much more manageable. As shown in Fig. 14. that can correctly use the created DS with the developed website.


https://trader1-idn.csmsu.net:8443

109s Lab Onli

trader1-idn.csmsu.net:8443

Connection is secure

Certificate Viewer: trader1-idn.csmsu.net

General Details

Issued To

Common Name (CN) trader1-idn.csmsu.net
Organization (O) <Not Part Of Certificate>
Organizational Unit (OU) <Not Part Of Certificate>

Issued By

Common Name (CN) Trusted Gateway CA Indonesia
Organization (O) Data Pipeline Trust Backbone (DTB)
Organizational Unit (OU) <Not Part Of Certificate>

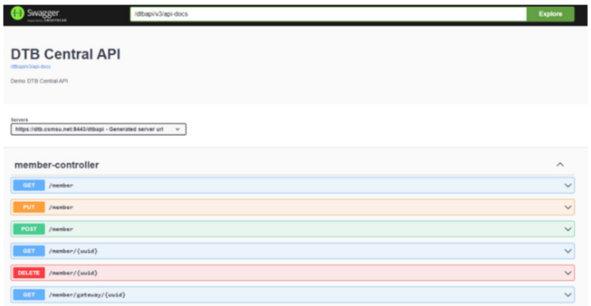
Validity Period

Issued On Thursday, October 27, 2022 at 1:18:21 PM
Expires On Saturday, October 26, 2024 at 1:18:20 PM

Fig.14: *EJBCA Digital Certificate.*

The system's main components, DTB, have been developed according to the designed concept. Java technology is used for back-end software development, and Angular is used for front-end software development, with details as follows.

Registration System (RS) is software that provides services to members such as adding, deleting, editing, and checking reliability. This system will be linked only to the member's computer system (machine to machine). Therefore, the RS system will be operated as a Web API that allows other systems to connect to perform various operations. There is no need for a UI part used to interact with users.


Swagger /dtbapi/v3/api-docs Explore

DTB Central API

/dtbapi/v3/api-docs

Demo DTB Central API

Servers
https://dtb.csmsu.net:8443/dtbapi - Generated server url

member-controller

GET /member
PUT /member
POST /member
GET /member/{uuid}
DELETE /member/{uuid}
GET /member/gateway/{uuid}

Fig.15: *DTB Registration System Web API.*

The software in the back-end system is run on the Tomcat Application Server because Java is a competent technology, and developing parts consistent with DTB's capabilities is convenient and fast.

The software in the Gateway System is the part that must interface with the user. Therefore, it has been developed in 2 systems: a front-end system that is Angular and a back-end system that is Java. Users will use the gateway system to perform various tasks related to data exchange. Whether it is registration, checking the trustworthiness of other users in the system, or searching for different users, they are all connected securely. It allows users to receive the most updated and accurate information before exchanging information in a trusted connection.

Testing Data:

The data is used for testing to simulate the operation of the system. It includes information related to requesting tax deductions for the origin of goods or Certificates of Origin exchanged in ASEAN countries. One hundred twenty-eight fields refer to the product bill and product details. In total, there are 16,944 forms and a list of 65,002 products. The Certificate of Origin form data is used in tax measures, and the Customs Department will use this data to process and make decisions in the product release process. This data is sent to the Customs Department system before the goods arrive, and it is pretty extensive. Therefore, tax reduction and release will be considered once the goods arrive based on the received data. The product origin data is crucial for testing the system. It is also used to analyze the sample of storage space usage during data exchange and to understand the business data storage structure, some of which must be kept as trade secrets. This information is provided by the Thailand Customs Department and is used in the actual customs system. The data is replicated and stored in the system of the trader who wishes to request a tax deduction and the computer system of the Customs Department. They will request access to that information directly through the DTB system that has been designed.

6.2 Testing and Evaluation

Data Access Control:

The first step of system testing is to experiment and measure the control of access to data in the Trader system according to the actual supply chain activity: the exchange of document forms regarding product origin. To be used in the tax deduction process (Certificate of Origin), the document information will be recorded abroad in the exporter's computer system, and information will be requested by the (simulated) Customs Department located in the country. The Customs Department will use the information to make decisions in the product release process, as shown in Fig. 16.

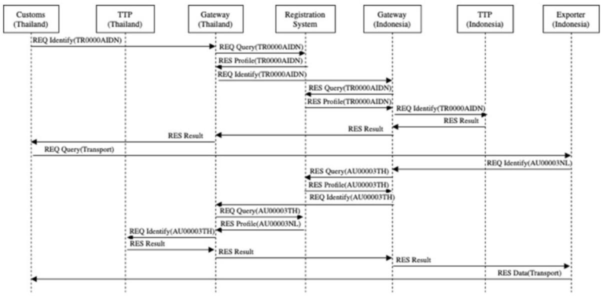


Fig.16: *Sequence of Data Access Control.*

The sequence diagram is a visual representation derived from a log that records the exchange process, demonstrating its high reliability. It begins with the Customs Department's request for member information via the Gateway. Once the Access Control List (ACL) validates the request, the information is shared with a trusted partner. The trustworthiness of both the requester and the data source is then verified using TTP. If both parties are deemed reliable, a Chain of Trust is established, enabling direct information exchange between partners via a secure web service. The experiment simulated the exchange of information between actors in different systems, as described in Table 3. The results showed that the information could be verified and exchanged correctly every time, with a 100% success rate, highlighting the reliability of the process. However, it is essential to note that each test requires configuring the domain name, creating a new digital certificate, and generating test data for the data source, all of which are time-consuming tasks. Therefore, we designed the experiment to include only twenty experiments, encompassing reliable and unreliable connections in each scenario. With four test scenarios, we performed the experiments 20 times per scenario, ensuring a thorough and robust testing process and 80 experiments.

Table 3: *Result of verified data exchange.*

Source	Destination	Trust Data Source	Distrust Data Source	Result
Customs Department	Exporter	10/10	10/10	100%
Exporter	Customs Department	10/10	10/10	100%
Gateway (TH)	Gateway (IDN)	10/10	10/10	100%
Gateway (IDN)	Gateway (TH)	10/10	10/10	100%

Data Integrity:

In an example data exchange scenario where an error occurs, data changes before reaching its destination. The designed DTB system checks the data integrity during exchange by using a message digest with a hash function to verify the source and destination data. Inspection using message digest can check the information exchanged in the system correctly. If the data is changed to be different from the original, the hash value will change and be detected every time the experiment, accounting for 100% of the experiment.

The customs department's data exchange in the Single Window system frequently causes errors. This is caused by using intermediary software or middleware to convert data to match the format of the Customs Department. These transformations cause errors in the data. Customs will request that information be resubmitted in the event of a mistake. On average, sending the information again takes 1-3 days. Also, if a software developer finds a bug and fixes the middleware, it takes approximately 14 days to fix each bug in the software, which causes significant delays. Data exchange in data pull allows the requester to access data directly from the source, resulting in correct and consistent data. It reduces time and errors in the data conversion process.

Data Exchange Processing:

Currently, exchanging data through the Single Window system requires the middleware described in the previous section. It causes errors in the data and delays related to supply chain activities, such as container clearance. Information and its accuracy are crucial in releasing containers in the Green Lane procedure, as seen in Fig. 17. There was an error in the request for new information, and there were seven steps to consider when getting the latest information. Compared with the data pull exchange shown in Fig. 18, the number of new data acquisition steps is reduced to 3, representing a reduction of 58%, which makes supply chain activities significantly faster.

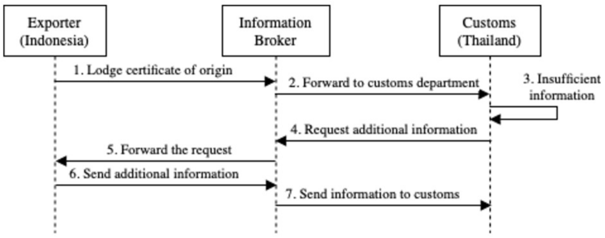

Exporter (Indonesia)
Information Broker
Customs (Thailand)
1. Lodge certificate of origin
2. Forward to customs department
3. Insufficient information
4. Request additional information
5. Forward the request
6. Send additional information
7. Send information to customs

Fig.17: *Traditional Request of Additional Data.*

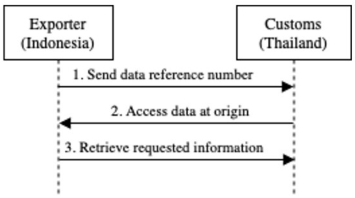

Exporter (Indonesia)
Customs (Thailand)
1. Send data reference number
2. Access data at origin
3. Retrieve requested information

Fig.18: *Data Pipeline Request.*

Data Confidentiality:

When exchanging valuable, confidential business information that must not be disclosed to unrelated persons, The exporter hires a freight forwarding company to deliver the goods to the destination. The shipping company may need to rent a trip by ocean liner to transport goods across countries. In this situation, the sea carrier company should not know the customer (exporter) of the freight forwarder company, which is essential information for the company. The sea carrier company may offer better deals to the exporter for future services. It causes the transport company to lose business, as shown in Fig. 19.

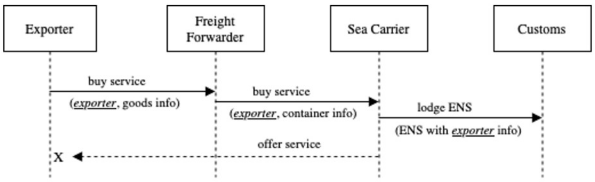
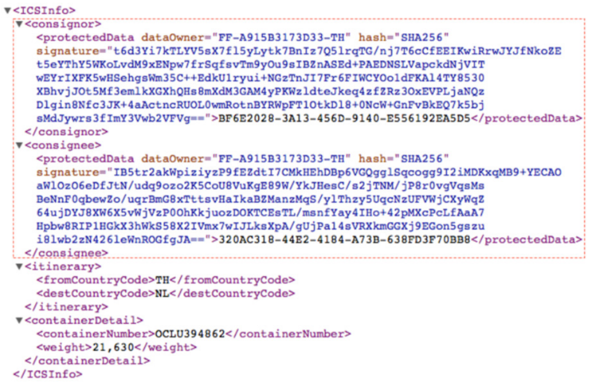


Fig.19: *Problem of unencrypted business data.*

It is maintaining the confidentiality of information by disclosing it only to those involved. Therefore, it is a method that must be used in exchanging data. In the DTB system, data encryption uses the public key generated through Public Key Infrastructure (PKI) technology. This cryptographic approach ensures that only the intended recipient with the corresponding private key can decrypt and access the data. By leveraging PKI, the system guarantees that unauthorized parties cannot intercept or tamper with the information, as the data remains securely encrypted throughout its transmission and storage.

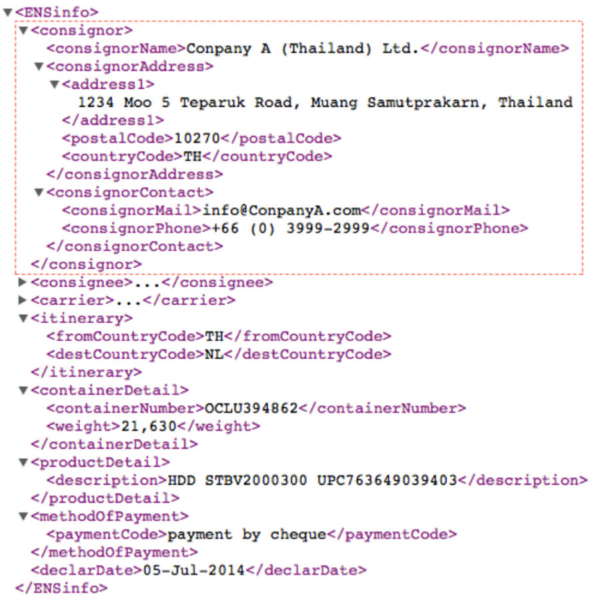
As illustrated in Fig. 20, the data is encrypted, preventing unauthorized users from accessing its contents, even if they manage to obtain it. Only authorized parties with the correct private key can decrypt the data. Fig. 21 demonstrates how, upon decryption, the data is presented exclusively to the relevant parties, ensuring confidentiality and data integrity, all made possible by the robust PKI technology.

This method of encryption not only protects sensitive information from external threats but strengthens trust among participants within the DTB system by facilitating the secure exchange of information. Additionally, PKI-based encryption enables compliance with industry standards and regulatory requirements for data protection, making it a robust solution for maintaining the privacy and confidentiality of sensitive information within the system.



```
▼<ICSInfo>
 ▼<consignor>
    <protectedData dataOwner="FF-A915B3173D33-TH" hash="SHA256"
    signature="t6d3Yi7kTLYV5sX7fl5yLytk7BnIz7Q5lrqTG/nj7T6cCfEEIKwiRrwJYJfNkoZE
    t5eYThY5WKoLvdM9xENpw7frSqfsvTm9yOu9sIBZnASEd+PAEDNSLVapckdNjVIT
    wEYrIXFK5wHSehgsWm35C++EdkU1ryui+NGzTnJI7Fr6FIWCYOoldFKAl4TY8530
    XBhvjJOt5Mf3emlkXGXhQHs8mXdM3GAM4yPKWzldteJkeq4zfZRz3OxEVPLjaNQz
    Dlgin8Nfc3JK+4aActncRUOL0wmRotnBYRWpFT1OtkDl8+0NcW+GnFvBkEQ7k5bj
    sMdJywrs3fImY3Vwb2VFVg==">BF6E2028-3A13-456D-9140-E556192EA5D5</protectedData>
  </consignor>
 ▼<consignee>
    <protectedData dataOwner="FF-A915B3173D33-TH" hash="SHA256"
    signature="IB5tr2akWpiziyzP9fEZdtI7CMkHEhDBp6VGQgglSqcogg9I2iMDKxqMB9+YECAO
    aWlOzO6eDfJtN/udq9ozo2K5CoU8VuKgE89W/YkJHesC/s2jTNM/jP8r0vgVqsMs
    BeNnF0qbewZo/uqrBmG8xTttsvHaIkaBZManzMqS/ylThzy5UqcNzUFVWjCXyWqZ
    64ujDYJ8XW6X5vWjVzP0OhKkjuozDOKTCEsTL/msnfYay4IHo+42pMXcPcLfAaA7
    Hpbw8RIP1HGkX3hWkS58X2IVmx7wIJLksXpA/gUjPal4sVRXkmGGXj9EGon5gszu
    i8lwb2zN426leWnROGfgJA==">320AC318-44E2-4184-A73B-638FD3F70BB8</protectedData>
  </consignee>
 ▼<itinerary>
    <fromCountryCode>TH</fromCountryCode>
    <destCountryCode>NL</destCountryCode>
  </itinerary>
 ▼<containerDetail>
    <containerNumber>OCLU394862</containerNumber>
    <weight>21,630</weight>
  </containerDetail>
</ICSInfo>
```

Fig.20: *Business Data Concealing.*



```
▼<ENSinfo>
 ▼<consignor>
    <consignorName>Conpany A (Thailand) Ltd.</consignorName>
   ▼<consignorAddress>
     ▼<address1>
        1234 Moo 5 Teparuk Road, Muang Samutprakarn, Thailand
      </address1>
      <postalCode>10270</postalCode>
      <countryCode>TH</countryCode>
    </consignorAddress>
   ▼<consignorContact>
      <consignorMail>info@ConpanyA.com</consignorMail>
      <consignorPhone>+66 (0) 3999-2999</consignorPhone>
    </consignorContact>
  </consignor>
 ▶<consignee>...</consignee>
 ▶<carrier>...</carrier>
 ▼<itinerary>
    <fromCountryCode>TH</fromCountryCode>
    <destCountryCode>NL</destCountryCode>
  </itinerary>
 ▼<containerDetail>
    <containerNumber>OCLU394862</containerNumber>
    <weight>21,630</weight>
  </containerDetail>
 ▼<productDetail>
    <description>HDD STBV2000300 UPC763649039403</description>
  </productDetail>
 ▼<methodOfPayment>
    <paymentCode>payment by cheque</paymentCode>
  </methodOfPayment>
  <declarDate>05-Jul-2014</declarDate>
</ENSinfo>
```

Fig.21: *Business Data Exposing.*

Based on the simulation and testing of the prototype, it is evident that the operation aligns with the initial assumptions. As this is a prototype system, cost analysis can be conducted by evaluating time and space complexities. Starting with time complexity, in the current data exchange system, if the data is insufficient for decision-making, additional data will be requested from the sender. This process is carried out sequentially based on the number of documents requiring additional data, resulting in a complexity of BigO(n) based on the number of documents. In contrast, the proposed system allows immediate data access without sorting, resulting in a complexity of BigO(1). Furthermore, the use of a hash function to manage data access control is explored in this research. A 256-bit (32-byte) data hash is utilized, with each permission policy occupying 760 bytes. This configuration allows for storing 1,315,789 policies per 1 GB of memory. Implementing the hash function will increase the total hash storage space to 4,2105,248 bytes (4 MB)

7. CONCLUSION

The research findings highlight a significant shift in how supply chain information is exchanged, moving from a data push to a data pull approach facilitated by the Data Pipeline concept. This change, driven by technological advancements, promises increased efficiency in supply chain operations. Adopting more efficient technology can speed up supply chain activities, regardless of high-speed communication and data acquisition formats.

Regarding improving supply chain visibility, the current data exchange methods via data push result in processing errors and ambiguity, which affect decision-making processes and lead to critical mistakes, such as releasing containers erroneously in systems like the Green Lane. The Distributed Trust Backbone (DTB) system, with its potential to bring about significant changes, ensures secure access to high-quality, up-to-date information, effectively addressing data transmission and redundancy issues. Moreover, the DTB system guarantees data integrity and security through robust access control mechanisms, utilizing existing Trusted Third Party (TTP) and Public Key Infrastructure (PKI) technologies. Protocols concerning Confidentiality, Integrity, Availability, and Accountability have been rigorously developed and tested to validate the secure exchange of information. Though still in the development phase, the proposed data exchange concept has the potential to bring about significant changes and is being prepared for submission to the authorities to enhance the current system. It is important to note that the proposed system is meant to supplement the current system. However, relatively certain aspects of it can be utilized to improve efficiency and effectiveness.

Additionally, this research focuses on designing a new communication system specific to the exchange of supply chain data, which no previous study has addressed under the concept of DataPipeline. Therefore, comparative performance measurement remains a challenge in the experiment. However, this research will be the basis for comparing design concepts in future research.

However, implementing this system is challenging due to the complex nature of supply chains and the involvement of diverse stakeholders. This research emphasizes the crucial role of collaboration between organizations, governments, and the private sector. Your involvement is critical to overcoming these challenges and fully realizing the benefits of efficient, accurate, and secure information exchange. Ultimately, supporting governmental and private sectors, including investments and policy adjustments, is crucial to accelerate the adoption of advanced information exchange practices in the supply chain.

ACKNOWLEDGEMENT

This research would not have been possible without the generous support and collaboration of the Thailand Customs Department. We express our deepest gratitude for their invaluable contribution in providing critical data, resources, and expertise essential to this study's successful completion. Their willingness to share knowledge and insights greatly enhanced the quality of our research, and we profoundly appreciate their team's time and effort in this project.

AUTHOR CONTRIBUTIONS

Conceptualization, Potchara Pruksasri and Suchart Khummanee; methodology, Potchara Pruksasri; software, Potchara Pruksasri; validation, Potchara Pruksasri and Suchart Khummanee; formal analysis, Potchara Pruksasri; investigation, Suchart Khummanee; data curation, Potchara Pruksasri; writing—original draft preparation, Potchara Pruksasri and Suchart Khummanee; writing—review and editing, Potchara Pruksasri and Suchart Khummanee; visualization, Potchara Pruksasri; supervision, Suchart Khummanee. All authors have read and agreed to the published version of the manuscript.

References

[1] D. Hesketh, "Weaknesses in the supply chain: Who packed the box?," *World Customs Journal*, vol. 4, no. 2, pp. 3-20, 2010.

[2] Y.-H. Tan, N. Björn-Andersen, S. Klein and B. Rukanova, *Accelerating Global Supply Chains with IT-Innovation: ITAIDE Tools and Methods*, Springer, 2014, pp.379.

[3] E. V. Stijn *et al.*, "The Data Pipeline," *Global Trade Facilitation Conference 2011Connecting International Trade:Single Windows and Supply Chains in the Next Decade*, 2011.

[4] P. Pruksasri, J. V. D. Berg and S. Keretho, "Accountability in Single Window systems using an Internal Certificate Authority: A case study on Thailand's National Single Window system," in *Proceeding of the 5th IADIS Multiconference on*

computer science and information systems, pp. 129-136, 2011.

[5] UNECE, "United Nations rules for electronic data interchange for administration, commerce, and transport," Accessed: 2023. [Online.] Available: `https://unece.org/trade/uncefact/unedifact/part-4-rules-electronic-data-interchange-administration-commerce-and-transport`

[6] S. Keretho, "UNESCAP High-level ExpertMeeting on "Reduction Poverty by Promoting Industrial Development through Trade Facilitation"," ASEAN single window initiative and Thailand's case experience for trade facilitation enhancement, 2010.

[7] UNECE. *Recommendation No. 18 Facilitation Measures Related to International Trade Procedures.* (2023). Accessed: 2024. [Online]. Available: `https://unece.org/trade/uncefact/introducing-unedifact`

[8] A. K. Y. Ng, "Port Security and the Competitiveness of Short-Sea Shipping in Europe: Implications and Challenges," in *Risk Management in Port Operations, Logistics, and Supply Chain Security.* 1st ed., ImprintInforma Law from Routledge, 2007, pp.1-20.

[9] D. Hesketh, "Seamless electronic data and logistics pipelines shift focus from import declarations to the start of commercial transactions," *World Customs Journal*, vol. 3, no. 1, pp. 27-32, 2009.

[10] W. Hofman, "Supply Chain Visibility with Linked Open Data for Supply Chain Risk Analysis," *1st Workshop on IT Innovations Enabling Seamless and Secure Supply Chains Delft*, The Netherlands, pp. 77-78, 2011.

[11] M. V. Oosterhout , M. Zielinski , Y-H Tan, "Inventory of flows & processes in the port," *Virtuele Haven deliverable*, 2D1a, 2000.

[12] P. Pruksasri, J. V. D. Berg, W. Hofman and S. Daskapan, "Multi-level access control in the data pipeline of the international supply chain system," *Innovation in the High-Tech Economy*, pp. 79–90, 2013.

[13] B. Rukanova, S. Henningsson, H. Henriksen and Y.-H. Tan, "Digital trade infrastructures: a framework for analysis," *Complex systems informatics and modeling quarterly*, no. 14, 2018.

[14] B. Rukanova, Y.-H. Tan, R. Huiden, A. Ravulakollu, A. Grainger and F. Heijmann, "A framework for voluntary business-government information sharing," *Government Information Quarterly*, vol. 37, no. 4, p.101501, 2020.

[15] S. Samonas and D. Coss, "The CIA Strikes Back: Redefining Confidentiality, Integrity and Availability in Security," *Journal of Information System Security*, vol. 10, no. 3, pp. 21-45, 2014.

[16] G. Tejpal, R.K. Garg and A. Sachdeva, "Trust among supply chain partners: a review," *Measuring Business Excellence*, vol. 17, no. 1, pp. 51-71, 2013.

[17] S. Daskapan, *MEDUSA: Survivable information security in critical infrastructures*, S. Daskapan, 2005.

[18] H. Eertink, B. Hulsebosch and G. Lenzini, "STORK-eID; Secure Identity Across Borders Linked. Dutch Ministry of the Interior and Kingdom Relations," *Competitiveness and Innovation Framework Programme ICT Policy Support Programme (ICT PSP)*, Towards pan-European recognition of electronic IDs (eIDs), 2009.

[19] W. Hofman, H. Bastiaansen, J. V. D. Berg and P. Pruksasri, "A platform for secure, safe, and sustainable logistics," in *Proceedings of the e-Freight 2012 Conference*, pp. 9-10, 2012.

[20] P. Pruksasri, J. van den Berg and W. Hofman, "Global monitoring of dynamic information systems a case study in the international supply chain," *2014 International Computer Science and Engineering Conference (ICSEC)*, Khon Kaen, Thailand, pp. 317-322, 2014.

[21] EJBCA, *EJBCA Community - Open-source PKI software.* (2024). Accessed: 2024. [Online]. Available: `https://www.ejbca.org`

Potchara Pruksasri has obtained both B.Sc. and M.Sc. of Computer Science at Khon Kaen University Thailand in 2000 and 2005 respectively. In 2005, he has been employed as a lecturer at Mahasarakham University, Thailand. He is currently working on his Ph.D. research at Computer Science Department, Faculty of Informatics, Mahasarakham University. His research focuses on information security and access control of the supply chain information system to secure dataexchange of global supply chains.

Suchart Khummanee received the B.Eng. degree in Computer Engineering from the King Mongkut's Institute ofTechnology Ladkrabang, the M.Sc. degree in Computer Science from the Khon Kaen University, and the Ph.D. degree in Computer Engineering from the Khon Kaen University, Thailand. He is currently a full lecturer of Computer Science at the Mahasarakham University, Thailand. His research interests in the network security, computer networks, agricultural robotics,and Internet of things (IoT).