Accredited Ranking SINTA 2
Decree of the Director General of Higher Education, Research, and Technology, No. 158/E/KPT/2021
Validity period from Volume 5 Number 2 of 2021 to Volume 10 Number 1 of 2026

Published online on: **http://jurnal.iaii.or.id**

JURNAL RESTI
(Rekayasa Sistem dan Teknologi Informasi)
Vol. 6 No. 3 (2022) 380 - 386 ISSN Media Electronic: 2580-0760

A Security Framework for Secure Host-to-Host Environments

Togu Muara Sianturi[1], Kalamullah Ramli[2]
[1,2]Department of Electrical Engineering, Faculty of Engineering, Universitas Indonesia
togu.muara01@ui.ac.id, kalamullah.ramli@ui.ac.id

Abstract

Data security is an infrastructure designed to protect and secure data from unauthorized access, data manipulation, malfunction, destruction, and inappropriate data disclosure. Currently, organizations widely use data transfer to validate and verify data using different media particularly in host-to-host connections. This research focuses on data exchanged (end-to-end communication) using Multi Protocol Label Switching (MPLS), metro ethernet, and Software Defined Wide Area Network (SD-WAN) network architecture with third parties. This research aims to develop a design and analysis framework for verifying data transferred from one host to another in ABC organization by applicable security standards that are appropriate and follow its needs to help the organization. Furthermore, the analysis result is used as materials for drafting a cybersecurity framework through the three standards ISO/EIC 27001:2013, NIST SP800-161, and ITU-T X.805. The methodology used in this study is the comparative analysis of three frameworks, requirement analysis, and content analysis to develop a framework. The framework proposed of eight security dimensions, five threats, and providing mitigation is expected to enhance the security system of data exchange on host-to-host connections in ABC organization.

Keywords: *end-to-end communication; MPLS; metro ethernet; SD-WAN; data exchange; data security*

1. Introduction

The growth of technology is currently a challenge in every organization, especially in data processing and data security itself that is related to data transmission communication. One of the derivatives of data processing, namely data transmission, is the process of transferring structured data in an approved standard format from one computer (host) to another computer system. It is very important to ensure the security of the data exchanged because the possible risks are data loss, the reputation of the organization, and the riskiest is the distribution of the data. To maintain the security chain, IT governance is needed to align strategies, regulate and control everything related to digital technology to achieve goals with a level of risk that can be measured and mitigated [1].

The main focus of this study is the security and integrity of data transferred from one host to another via MPLS, Metro-e, and SD-WAN using a web service mechanism. We choose these architectures because these three architectures are the most frequently used by an organization in transferring data using a private network. Data transfer in a private network is usually used for data validation, verification, sending important or confidential data to third parties, and vice versa. Data transmitted consists of confidential, restricted, and ordinary data [2]. Confidentiality and availability are very important in transmitting the data, particularly if there is verification of financial transactions with banks. It is expected that the results of the analysis using three standards will design a framework that can mitigate security risks on host-to-host connections.

These are the related researches about secure data transfer in a host-to-host environment with third parties. Guanyi Lu and Xenophon Koufteros in 2019 did research about organizing practices to combat supply chain security breaches. To diagnose an organization’s supply chain security status, supply chain security management practices are categorized into four classes based on their objectives - detection, prevention, response, and mitigation [3]. Giovanna Culot, et al in 2021 researched on addressing industry 4.0 cybersecurity challenges. One of the implementation areas addressed was the lack of visibility and monitoring of suppliers. In industries with low cybersecurity maturity, this might be a potential threat to data and information [4]

2. Research Methods

The method that was carried out in this studi can be seen in Figure 1.

Accepted: 15-04-2022 | Received in revised: 12-05-2022 | Published: 30-06-2022

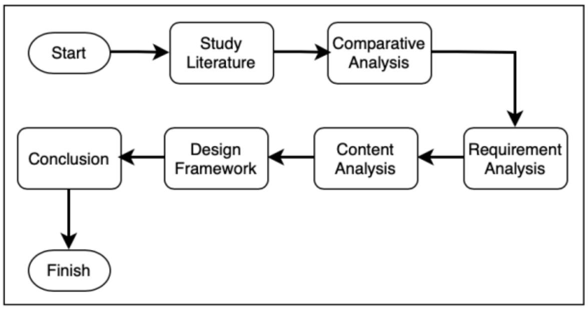

Figure 1. Research Methodology

2.1 Literature Study

This section reviews related information of MPLS, Metro-e, and SD-WAN because these technologies are implemented and used in ABC organization.

2.1.1 Host-to-Host

Host-to-host connection is often also referred to end-to-end communication, which is a form of communication within a computer network that occurs between hosts, namely computers and other devices that are connected [5]. Recognition between hosts through computer network addresses based on Internet Protocol so that computers that are connected and communicate with each other can recognize through network addresses. Host-to-host connections are usually used to validate, verify, and transfer data between organizations using different network architectures. Host-to-host is widely used by organizations to establish connections such as data exchange and payment transactions.

2.1.2 MPLS

Multi-Protocol Label Switch (MPLS) is a technology in an IP based communication system that is efficient and facilitates data traffic management by sending data based on priority on the data label, not based on IP Address so that the quality is guaranteed. Therefore, there are companies or government boards still using this technology. Initially, MPLS was developed to improve performance in ISP networks without adequate security considerations. An advantage of using MPLS is that it can be used to improve Quality of Service (QoS) and the most important thing is security. The most significant is the concept of VPN which segregates the traffic according to the criteria set by the customers, making the connection secure and private [6].

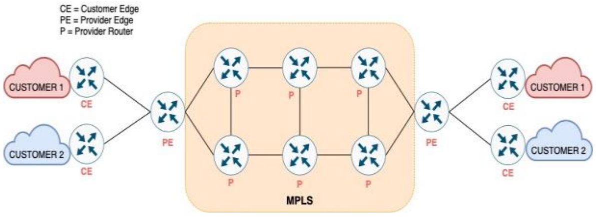

Figure 2. MPLS Architecture [6]

Figure 2 shows that each customer can communicate over MPLS architecture. MPLS components are Customer Edge router (CE), Provider Edge router (PE), and Provider router (P).

2.1.3 Metro Ethernet

Metro Ethernet (Metropolitan-Area Ethernet) is a network based on the ethernet standard that serves metropolitan areas through a Metropolitan Area Network (MAN). This technology can be used as a metropolitan access network, connecting business customers and individual users to a WAN, or to provide communications within a metropolitan area. Metro-e also supports high bandwidth such as 10 Mbps to 10000 Mbps [7]. Metro-e issued by a service provider or ISP consists of layer 2 or 3 switches and routers. There are at least two types of Metro-e services that can be used, point-to-point and point-to-multipoint. Point-to-point is a service that connects two separate points in one area. Point-to-multipoint is a service that connects a single point with several separate points.

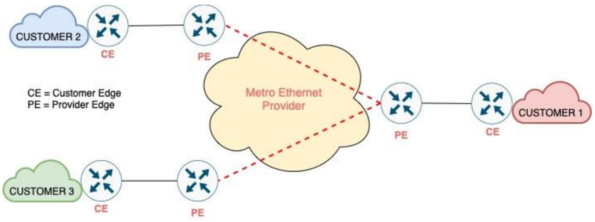

Figure 3. Metro-e Architecture [7]

Figure 3 shows that each customer can communicate over Metro-e architecture. Dotted lines describe point-to-point connectivity from customer to other customer based on the service provider.

2.1.4 SD-WAN

Software-Defined Networking (SDN) is a new network architecture that is dynamic, manageable, cost-effective, and adaptable. In the SDN concept, there is an open interface that allows an application entity to control the connectivity provided by several network resources, control the traffic flow and inspect or modify the traffic [8]. SD-WAN is a specific application form of Software-Defined Networking (SDN) technology that is applied to Wide Area Network (WAN) connections, which are used to connect corporate networks including branch offices and data centers that have wide geographical distances. This technology will help reduce complexity with zero-touch provisioning that can overcome the risk of human error [9].

2.1.5 ISO/EIC 27001:2013

ISO/IEC 27001:2013 is an international standard that focuses on Information Security Management Systems (ISMS). The official name for this standard is Information Technology - Security Techniques - Information Security Management Systems -

DOI: https://doi.org/10.29207/resti.v6i3.4018

Requirements. This standard was created to meet the needs of implementing, establishing, monitoring, operating, maintaining, reviewing, and improving security management systems [4]. The determination of the ISMS policy is based on a risk management approach, which begins with an understanding of the business environment and an evaluation of resources and processes to identify possible information security risks [11, 12]. ISO 27001 was chosen in this research because giving recommendations on controlling information security risks.

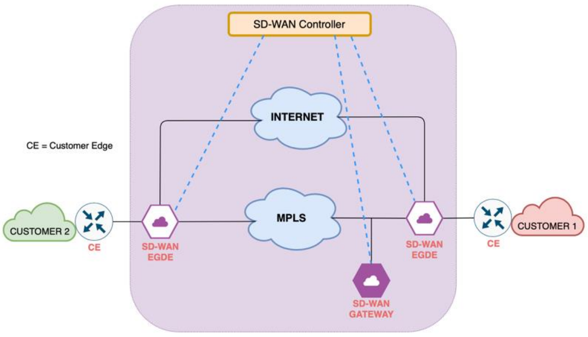

Figure 4. SD-WAN Architecture [10]

2.1.6 NIST SP 800-161

NIST has a special publication 800-161 “Supply Chain Risk Management Practices for Federal Information Systems and Organizations” which builds on the basic concepts described in detail in the NIST framework and other publications. NIST SP 800-161 aims to identify, assess, select, and implement risk management processes and mitigation controls within an organization, specifically managing risks resulting from supply chain processes [13]. These identified controls can be modified and adapted to suit any organization based on its requirements and objectives [14]. In addition to the organization, SCRM controls should apply to vendors, developers, systems integrators, external service providers, industrial controls, and providers of operational technology products and services [15, 16].

2.1.7 ITU-T X.805

ITU-T X.805 defines end-to-end communication security and secure network architecture for specific systems. According to the X.805 specification, architecture can be applied independently of the basic network technology to various types of networks. ITU-T X.805 defines the common security-related architectural elements required to provide end-to-end communication security [17]. The purpose of this framework is as a basis for developing detailed recommendations for end-to-end network security. This framework was developed to provide a systematic and organized way to address five threats to telecommunications networks.

2.2 Comparative Analysis

The following comparisons analysis of three frameworks has been made:

Table 1. Comparison of the Three Frameworks

Model	Focus Area	Objectives	Categories
ISO/EIC 27001:2013	Information security management systems	1. Plan 2. Do 3. Check 4. Act	14 security controls
NIST SP 800-161	Supply chain risk management practices for federal information systems and organizations	Identify, assess, select, and implement risk management processes and mitigation controls within an organization, specifically managing risks resulting from supply chain processes	19 security controls
ITU-T X.805	End-to-end communication security and secure network architecture for specific systems	Develop detailed recommendations for end-to-end network security	9 security planes

2.3. Requirement Analysis

Requirements analysis is the stage of identifying the security dimensions contained in the host-to-host connection. Security dimension is a collection of security measures designed to address a specific aspect of network security. This recommendation identifies eight security aspects that protect against all security threats. This dimension is not limited to network, but also API and user data. In addition, the security dimension applies to both service providers and third parties. The following requirement analysis has been made:

Table 2. Requirement Analysis

No	Security Dimension	Requirement
1.	Integrity	Ensures the correctness or accuracy of data, including addition, subtraction, deletion, and multiplication.
2.	Availability	a. Ensure the availability of network elements, stored information, information flows, services, and applications. b. Asset inventory
3.	Confidentiality	a. Confidential data that must be controlled and determined b. Network devices configuration and user identification c. Rules are enforced that impose confidentiality obligations on third parties to whom confidential information is provided

DOI: https://doi.org/10.29207/resti.v6i3.4018

No	Security Dimension	Requirement
		d. Confidentiality obligations for external workers, e.g. Engineer on Site (EOS) e. Confidential information is managed and reviewed
4.	Non-Repudiation	Ensure sender cannot deny that message has been sent and the integrity of the message remains intact and maintained.
5.	Communication Security	a. Device, server and support library security b. Log management c. Network security management d. Network security monitoring
6.	Privacy	a. Maintain personal information that is stored and only the desired parties are allowed to know b. Sensitive document protection procedures
7.	Access Control	a. Rules for managing hosts and APIs access b. Remote access c. Network devices access
8.	Authentication	a. Manage administrator account permissions b. Rules about personal authentication are established and enforced

2.4 Content Analysis

Content Analysis is a research stage that is an in-depth discussion of the contents of documented information. This content analysis approach is a step taken as an effort to identify the characteristics of the conceptual standard/framework to present the processed data of research analysis. One part of content analysis is coding. Coding is carried out on each activity contained in the standard, a security framework that will be the material for grouping the results of the categorization of each activity. Each variety of the three frameworks is codified with the provision that A is the category code for the ISO/IEC 27001:2013 model, B is the NIST SP 800-161 model, and C is the ITU-T X.805 model. The following is an example of coding in the H2H column in the following table:

Table 3. Codification Framework Process

No.	Categories	H2H
	ISO/IEC 27001:2013	
1.	Information Security Policies	A1
2.	Organization of information security	A2
3.	Human resources security	A3
	NIST SP 800-161	
1.	Access Control	B1
2.	Awareness and Training	B2
3.	Audit and Accountability	B3
	ITU-T X.805	
1.	Security dimensions to the infrastructure layer, management plane	C1
2.	Security dimensions to the infrastructure layer, control plane	C2
3.	Security dimensions to the infrastructure layer, end-user plane	C3

The next step is to analyze the categories of each framework, referring to the Table 3 results and then mapping all controls in each category according to the security requirements of the host-to-host environment in ABC organization, so the next step is to conduct content analysis. The following are the results of the content analysis of the three frameworks in designing a secure host-to-host framework. According to the table below, interpreted the integrity requirement in Table 2 can be fulfilled with A4, A6, A9 categories in the ISO/IEC 27001:2013 model; B18, B19 categories in the NIST; and C8 category in the ITU-T X.805 model. Availability requirement can be fulfilled with A4, A13 categories in the ISO/IEC 27001:2013 model; B6, B11 categories in the NIST; and C1, C2 categories in the ITU-T X.805 model. And so on for the other security dimensions with the requirements that all three frameworks meet.

Table 4. The Result Content Analysis Framework

Security Dimensions	H2H A	H2H B	H2H C
Integrity	A4, A6, A9	B18, B19	C8
Availability	A4, A13	B6, B11	C1, C2
Confidentiality	A1, A2, A3, A4, A5, A11	B5, B14, B16	C2, C4, C6, C8
Non-Repudiation		B3	C8
Communication Security	A8, A9, A10	B3, B4, B5, B16, B18,	C2, C7
Privacy	A4, A14	B4	C1
Access Control	A2, A5	B1	C1, C2, C4, C7
Authentication	A2, A5	B4, B7	C1, C2

3. Results and Discussions

3.1 High Level Architecture

In host-to-host architecture, there are two important elements, network security and web services. Network security includes routers and firewalls. Router serves as a communication network link between ABC organization and third parties. While the firewall serves as a security perimeter that controls and oversees the flow of data packets on the network. The implementation of threat prevention on the firewall will improve cybersecurity solutions that can prevent, detect, and mitigate threats from attacks. Figure 5 describes the high-level architecture of host-to-host:

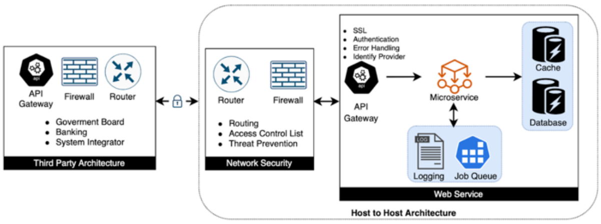

Figure 5. High Level Host-to-Host Architecture

Web service is an application with a set of data (database), software or part of software that can be

DOI: https://doi.org/10.29207/resti.v6i3.4018

accessed by third parties through a predetermined network connection. Web service can also be interpreted as a method of exchanging data that supports interoperability and interaction between systems on a network. So that web service can become a bridge between the various existing systems. In web service, there are API gateway, microservice, logging, job queue, cache, and database. API gateway is used to determine which API access can be accessed by third parties.

Third party architecture is an architecture that is used by third parties, government boards, banks, and system integrators in general. Some routers and firewalls connect third parties with ABC organization. API gateway is used as a service that is made specifically and as the main entry point for ABC organization to enter third party services.

3.2 Security Issues in Host-to-Host Environment

The security of data transferred on host-to-host connection cannot be separated from the involvement of third parties. Utilization of transferred data includes transaction data, personal data as validation data, and other data as complementary information. Data security and privacy are of primary concern because data and resources on host-to-host are stored and controlled by both parties. Besides, communication service providers agreed by both parties are also a vulnerability and a gap in the entry of security threats. The following are security issues that may occur in host-to-host connections on three network architectures:

1. Data breach

Due to the dynamic and shared of network architecture, data theft can become a major problem. This may include data leaking, deletion, or modification in host-to-host connection. It can happen because of lack of authentication, authorization, weak passwords, and lack of disaster recovery. Confidential information must be determined and the rules clearly defined and announced to all stakeholders. According to ISO 27001, the information shall be classified in terms of legal requirements, value, criticality, and sensitivity to unauthorized disclosure.

2. Risk profiling

MPLS, Metro-e, and SD-WAN networks are generally provided by ISPs. These make organizations less involved with hardware and software ownership and maintenance. However, this leaves customers unaware of the internal security procedures, security compliance, hardening, patching, auditing, and logging processes. Organizations use risk profiling as a way to reduce potential risks and threats. Identification of software license lists and security perimeters with value and potential to save on maintenance costs. Applying security patches to OS, application, and device security then vulnerability assessments are applied to all assets before and after deployed and precautions are taken for identified vulnerabilities.

3. Changes to business model

In general, host-to-host service connection is provided by the ISP. Both the customer and the third party will choose the network architecture and ISP used to facilitate the installation and implementation process. Networks, servers, storage, and applications are under the control of ISPs and third parties, so it is necessary to evaluate the risks associated with losing control of the infrastructure. Identification and monitoring of infrastructure and networks to detect potential cybersecurity events, and also monitor the activities of service providers and partners to ensure service quality is still in line with the agreed agreement.

4. Business services continuity

The unavailability of network services can be a threat to host-to-host services. SD-WAN architectures that use internet connectivity are vulnerable to Denial of Service (DoS) attacks that cause service unavailability. Network connection implements high availability and sufficient redundancy to comply availability requirements. Network devices are always available to receive control information from legitimate sources and implement high availability devices.

5. Compliance and governance

ISP and third parties must provide some guarantees in Service Level Agreement (SLA) to reassure customers about security issues. The SLA should contain a comprehensive list of regulations governing the related systems, services, and compliance. External workers are required to submit a written confidentiality agreement (e.g., a non-disclosure agreement) before starting work and be reminded of their duty about confidentiality after their contract ends. An agreement containing a confidentiality clause must be signed with the third party. It should be ensured that confidentiality agreements are reached with partner companies before sharing confidential information.

6. Privacy issues

Aspects of data security and privacy are components that must be present in the requirement analysis of host-to-host connections. Protection of customers' personal information such as personal identity shall be ensured as required in relevant legislation and regulation where applicable. Procedures shall be implemented for the management and protection of sensitive documents and limited by policy.

3.3 Framework Proposed

After introducing security issues in host-to-host environment, next is to make an approach that allows analyzing and making the relation between security

DOI: https://doi.org/10.29207/resti.v6i3.4018

issues and solutions. In this section, the approach used is comparative analysis dan content analysis to ensure that the results can enhance the security system of data exchange on host-to-host connections. This helps to manage the data transferred in host-to-host connection more effectively and provides the security analysts to include the specific solution to counter the threat. The analysis results show eight aspects of the security dimension and five threat security issues.

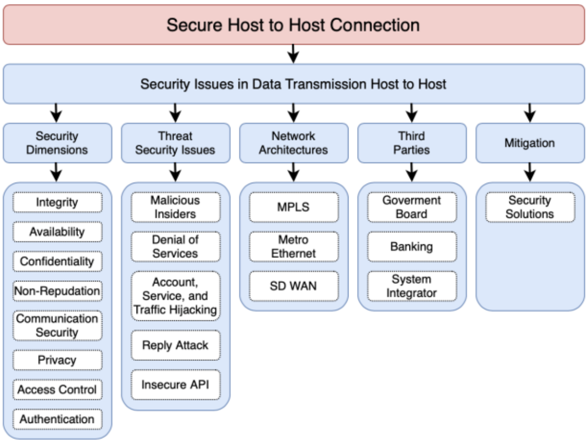

Figure 6. Framework Proposed for Secure Host-to-Host Connection

3.4 Mapping of Security Dimensions to Security Threats

The following threats are described in the framework proposed for secure host-to-host connection: malicious insiders (MI); denial of services (DOS); account, service, and traffic hijacking (ASTH); reply attack (RA); and insecure API (IAPI). Table 5 provides a mapping of security dimensions to the security threats.

Table 5. Mapping of Security Dimensions to Security Threats

Security Dimension	MI	DOS	ASTH	RA	IAPI
Integrity		Y			Y
Availability		Y			
Confidentiality	Y		Y		Y
Non-Repudiation		Y	Y	Y	
Communication Security			Y	Y	Y
Privacy			Y		Y
Access Control	Y	Y	Y	Y	Y
Authentication			Y	Y	

3.5 Mitigation

This section will explain the countermeasures of the threats that have been identified. A malicious insider is a person or group from within an organization with access to control, knowledge, and information that is used maliciously through a series of actions that compromise the confidentiality, integrity, and availability of information. This person or group may be from a third party, network service provider, or even the company. To confront this threat, ensure that only authorized personnel or hosts are allowed to perform administrative activities or manage API and applications. The expiration date of the agreement is managed and updated as needed according to third party access. Another effective measure is to manage access and authorization by combining the principle of least privilege and segregation of duties on access to networks and services.

Denial of service is a type of attack carried out by flooding host-to-host network traffic on a server, system, or network. This attack is a threat to the availability of host-to-host services. As a countermeasure for this attack, network devices are always available to receive control information from legitimate sources and implement high availability devices. Furthermore, the best approach to prevent this attack is to identify by counting the number of packets received, detecting the protocol and frequency of occurrence of the same protocol, then mitigate by setting a priority flow rule to block ports from attackers.

Account, service, and traffic hijacking is a threat from man-in-the-middle attacks, phishing, and spam. Account hijacking is usually accomplished with stolen credentials. Using stolen credentials, attackers can access sensitive information and compromise the confidentiality, integrity, and availability of host-to-host services. To confront this threat, protect network devices or configuration information from unauthorized access. This applies to the configuration information on the network device and the backup configuration information stored offline.

Reply attack is an attack on security protocols using a replay of data transmissions from a different sender into the system of the intended recipient, thereby tricking potential victims into believing that they have completed the data transmission. Replay attacks help hackers gain access to the network, obtain information that would not be easily accessible or complete duplicate transactions. To confront this threat provides a record that identifies each user or device that accesses and uses the network-based application and the actions taken. These records will be used as proof of access and use of the application.

Insecure API is a growing threat these days. API is a source of security problems, especially if it is not properly protected which might be relaxed in isolation end up insecure in combination [18]. Hackers can exploit insecure APIs to steal sensitive and private data. The solution protects API from unauthorized access through a web application firewall that might validate the request format. Ensure that all API traffic is encrypted but in a manner so as not to impact performance.

4. Conclusion

This paper presents the design and analysis of a framework for secure host-to-host environment on three

DOI: https://doi.org/10.29207/resti.v6i3.4018

network architectures. This research focuses on MPLS, Metro-e, and SD-WAN network architectures. Based on the content analysis carried out on the three frameworks ISO/EIC 27001:2013, NIST SP800-161, ITU-T X.805, a new framework is formed that can be used by ABC organization in measuring the level of data and connection security on host-to-host environment. The framework consists of eight security dimensions and provides mitigation as a solution to threats that can be the basis for mapping the improvement of ABC's organizational cybersecurity capabilities. In further research, the validation process can be carried out on the framework that has been produced. Besides, mapping of information technology risk management compliance by certain institutions can also be carried out to obtain a more comprehensive conceptual framework.

References

[1] A. Gurtu and J. Johny, "Supply Chain Risk Management: Literature Review," *Risks*, vol. 9, no. 1, 2021, doi: 10.3390/risks9010016.

[2] "Network Infrastructure Security Guidance," National Security Agency, 2022, vol. Version 1.0.

[3] G. Lu and X. Koufteros, "Organizing Practices to Combat Supply Chain Security Breaches," *IEEE Engineering Management Review*, vol. 47, no. 3, pp. 72-78, 2019, doi: 10.1109/EMR.2019.2931540.

[4] G. Culot, F. Fattori, M. Podrecca, and M. Sartor, "Addressing Industry 4.0 Cybersecurity Challenges," *IEEE Engineering Management Review*, vol. 47, no. 3, pp. 79-86, 2019, doi: 10.1109/EMR.2019.2927559.

[5] V. Mikhalev, L. Gomez, F. Armknecht, and J. Márquez, "Towards End-to-End Data Protection in Low-Power Networks," 2018, pp. 3-18.

[6] F. Bensalah, N. El Kamoun, and A. Bahnasse, "Scalability Evaluation of VOIP over Various MPLS Tunneling under OPNET Modeler," *Indian Journal of Science and Technology 10*, pp. 1-7, 2017.

[7] L. Velasco, J. Perelló, and G. Junyent, "Metro Ethernet Networks (MEN)," *Optical Communication Group - Universitat Politècnica de Cataluya (UPC)*, pp. 185-197, 2014.

[8] W. Sun, Y. Li, and S. Guan, "An Improved Method of DDoS Attack Detection for Controller of SDN," in *2019 IEEE 2nd International Conference on Computer and Communication Engineering Technology (CCET)*, 16-18 Aug. 2019 2019, pp. 249-253, doi: 10.1109/CCET48361.2019.8989356.

[9] S. Troia, L. M. M. Zorello, A. J. Maralit, and G. Maier, "SD-WAN: An Open-Source Implementation for Enterprise Networking Services," in *2020 22nd International Conference on Transparent Optical Networks (ICTON)*, 19-23 July 2020 2020, pp. 1-4, doi: 10.1109/ICTON51198.2020.9203058.

[10] F. Aldeeb and A. Ali Ahmed, *Software Defined Wide Area Network SD-WAN: Principles and Architecture*. 2021.

[11] M. Yasin, A. A. Arman, I. J. M. Edward, and W. Shalannanda, "Designing Information Security Governance Recommendations and Roadmap Using COBIT 2019 Framework and ISO 27001:2013 (Case Study Ditreskrimsus Polda XYZ)," in *2020 14th International Conference on Telecommunication Systems, Services, and Applications (TSSA*, 4-5 Nov. 2020 2020, pp. 1-5, doi: 10.1109/TSSA51342.2020.9310875.

[12] Angraini, Megawati, and L. Haris, "Risk Assessment on Information Asset an academic Application Using ISO 27001," in *2018 6th International Conference on Cyber and IT Service Management (CITSM)*, 7-9 Aug. 2018 2018, pp. 1-4, doi: 10.1109/CITSM.2018.8674294.

[13] L. Al-Alawi, R. Al-Busaidi, and S. Ali, "Applying NIST SP 800-161 in Supply Chain Processes Empowered by Artificial Intelligence," in *2021 22nd International Arab Conference on Information Technology (ACIT)*, 21-23 Dec. 2021 2021, pp. 1-8, doi: 10.1109/ACIT53391.2021.9677393.

[14] J. Martínez and J. M. Durán, "Software Supply Chain Attacks, a Threat to Global Cybersecurity: SolarWinds' Case Study," *International Journal of Safety and Security Engineering,* vol. Vol. 11, No. 5, pp. 537-545, 2021, doi: https://doi.org/10.18280/ijsse.110505.

[15] P. J. G. Guerra and D. A. S. Estay, "An Impact-wave Analogy for Managing Cyber Risks in Supply Chains," in *2018 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM)*, 16-19 Dec. 2018 2018, pp. 61-65, doi: 10.1109/IEEM.2018.8607563.

[16] T. Kieras, J. Farooq, and Q. Zhu, "I-SCRAM: A Framework for IoT Supply Chain Risk Analysis and Mitigation Decisions," *IEEE Access*, vol. 9, pp. 29827-29840, 2021, doi: 10.1109/ACCESS.2021.3058338.

[17] P. Rathod, V. Julkunen, T. Kaisti, and J. Nissilä, "Automatic acceptance testing of the web application security with ITU-T X.805 framework," in *2015 Second International Conference on Computer Science, Computer Engineering, and Social Media (CSCESM)*, 21-23 Sept. 2015 2015, pp. 103-108, doi: 10.1109/CSCESM.2015.7331876.

[18] M. Asghar and A. Amjad, "Securing Insecure Web API's in Cloud Computing," vol. 68, 2018.