applied sciences

MDPI

Article

A Proposal for a Zero-Trust-Based Multi-Level Security Model and Its Security Controls

Jun-Hyung Park †, Sung-Chae Park † and Heung-Youl Youm *

Department of Information Security Engineering, Soonchunhyang University, Asan 31538, Republic of Korea; junhyung.park@sch.ac.kr (J.-H.P.); zoesc.park@sch.ac.kr (S.-C.P.)
* Correspondence: hyyoum@sch.ac.kr
† These authors contributed equally to this work.

Abstract: The rapid advancement of technology and increasing data utilisation have underscored the need for new models to manage and secure big data effectively. However, the constraints of isolated network environments and the limitations of existing security frameworks hinder the adoption of cutting-edge technologies such as AI and cloud computing, as well as the safe utilisation of data. To address these challenges, this study proposes an enhanced security model that integrates the concepts of Multi-Level Security (MLS) and Zero Trust (ZT). The proposed model classifies data into the following three sensitivity levels: "Classified", "Sensitive", and "Open". It applies tailored security requirements and dynamic controls to each level, enhancing both data security and usability. Furthermore, the model overcomes the static access control limitations of MLS by incorporating ZT's automated dynamic access capabilities, significantly improving responsiveness to anomalous behaviours. This study contributes to the design and evaluation of a new security model that ensures secure data protection and utilisation, even in isolated network environments such as those of military and governmental organisations. It also provides a foundation for the future development of advanced security frameworks.

Keywords: cybersecurity; zero trust; multi-level security; security model; security strategy; security control

check for updates

Academic Editors: Peter R. J. Trim and Yang-Im Lee

Received: 20 November 2024
Revised: 31 December 2024
Accepted: 8 January 2025
Published: 14 January 2025

Citation: Park, J.-H.; Park, S.-C.; Youm, H.-Y. A Proposal for a Zero-Trust-Based Multi-Level Security Model and Its Security Controls. *Appl. Sci.* **2025**, *15*, 785. https://doi.org/10.3390/app15020785

Copyright: © 2025 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

1.1. Background

The advancement of technologies such as artificial intelligence (AI), cloud computing, and 6G has led to a dramatic increase in the volume of data available. Big data are being utilised not only by private enterprises, but also by academia, government, and public organisations, driving research and analysis across various domains. Many organisations are simultaneously leveraging big data and adopting new technologies to enhance productivity, improve efficiency, and create new value [1–3]. However, restricted environments, such as those employing isolated network systems, including military and government organisations, face challenges in quickly and efficiently adopting emerging technologies for data utilisation [4]. At the same time, the rapid evolution of digital environments has resulted in increasingly complex IT infrastructures, accompanied by more sophisticated cyber risks or threats [5]. The emergence and proliferation of advanced IT technologies, such as cloud computing, AI, and quantum computing [6,7], have introduced new demands for data utilisation and security frameworks. This has led to an increased emphasis on the need for new security models that can maintain enhanced security and support data utilisation efficiently [8].

In particular, the spread of remote work, telecommuting, and hybrid work following the COVID-19 pandemic has exposed the limitations of traditional security frameworks. This has highlighted the necessity of establishing more sophisticated mechanisms for managing users and implementing security controls when accessing internal information assets via external networks [9]. Furthermore, global regulations, such as FISMA [10] and GDPR [11,12], call for differentiated security controls based on data sensitivity. Simultaneously, the rise in advanced cyber attacks, such as Advanced Persistent Threats (APTs), underscores the increasing need for systematic security strategies to safeguard Sensitive data in organisations [13]. In this context, the Multi-Level Security (MLS) framework has gained attention as a model that differentiates security policies according to data sensitivity, thereby protecting the data that organisations store, utilise, or process while supporting efficient data utilisation.

As a result of this background, the Republic of Korea's National Intelligence Service (NIS) announced a roadmap in September 2024 aimed at transitioning to a Multi-Level Security (MLS) framework, which applies differentiated security controls based on the sensitivity of data [14].

The MLS framework in the Republic of Korea is a security framework that ensures confidentiality and integrity by refining access controls based on data sensitivity. It is particularly recognised as an effective data-centric security model in environments with varying data sensitivity levels. MLS categorises data into classifications such as "Classified", "Sensitive", and "Open", applying appropriate security controls to each level to manage access to data or resources systematically in organisations. However, as the MLS model predominantly relies on static access controls, it faces limitations in continuously verifying the identity of users, devices, or systems attempting to access resources or data, making it challenging to respond promptly to abnormal access behaviours.

The Zero Trust (ZT) model is a security framework based on the principle of "never trust, always verify", employing dynamic access control to validate all access requests continuously [15]. Unlike traditional perimeter-based security models, the Zero Trust approach treats both internal and external users as potential threats. Implementing continuous verification for all access attempts effectively defends against advanced cyber threats, such as Advanced Persistent Threat (APT) attacks, as well as risks that may arise within the network [16,17].

The MLS model provides a security framework based on data sensitivity; however, it operates under the assumption of trust towards internal users, relying on static access controls, which lack continuous verification.

The abovementioned limitations can be addressed by integrating the Zero Trust model, which offers dynamic access control and continuous verification of access to data and resources. A security framework that combines MLS with Zero Trust can continuously validate the identity of users, devices, and systems attempting access and provide differentiated access controls based on the sensitivity of the data. This integrated approach ensures a security model that considers the protection of data, the reliability of access behaviours, and data utilisation.

1.2. Contribution

This study proposes an MLS model based on Zero Trust that aims to overcome the limitations of existing MLS models that rely on static access control and to provide systematic and dynamic access control. For this purpose, this study identified data used, processed, or utilised in an organisation's information assets into three levels (Classified, Sensitive, and Open) according to sensitivity, and identified security controls suitable for the components of the proposed model by reflecting the security requirements that each level should meet.

This paper contributes a design approach that addresses the limitations of static security controls while simultaneously enhancing both security and usability within an advanced security model.

1.3. Structure of This Paper

The structure of this paper is as follows: Section 2 reviews related works, outlining the concepts of the MLS and Zero Trust security models and discusses them. Section 3 introduces MLS classification criteria, proposes a convergence security model that combines MLS and Zero Trust, providing detailed descriptions of its components, and explains the results of comparative analysis with other models. Section 4 proposes security controls to address the security risks outlined in Section 3 and describes security measures as controls applicable to the proposed model. Furthermore, it analyses the model's robustness and efficiency through hypothetical risk scenarios and evaluates its security capabilities. Finally, Section 5 concludes this study and outlines directions for future work.

2. Related Works and Their Analysis

2.1. Multi-Level Security

Multi-Level Security is defined as a concept of processing information with different classifications and categories that simultaneously permits access to users with different security clearances and denies access to users who lack authorisation [18]. Based on this conceptual definition, the MLS model can be considered a security model that hierarchically classifies an organisation's information assets according to their data sensitivity and risk impact and applies appropriate security controls and policies to each layer. Furthermore, this clause seeks to compare and analyse the MLS models in the United States and Korea.

The Multi-Level Security in the United States and the Republic of Korea reflects each country's unique environments and security requirements, adopting a differentiated approach based on the sensitivity of information and the criticality of systems. Both countries enhance their overall security levels by applying classification criteria aligned with their respective security objectives.

The United States federal government employs FIPS 199 (Federal Information Processing Standards Publication 199) [19] as a standard for assessing the security level of information systems. FIPS 199 establishes confidentiality, integrity, and availability as the core security objectives and categorises information into the following three levels: Low, Moderate, and High. This framework evaluates the potential impact of each classification, systematically managing the sensitivity of information assets and the potential consequences of system loss or compromise.

The method of assessing the impact of breaches on an organisation for each security objective is determined by comprehensively considering factors such as the sensitivity of information, threat elements, and the scale of potential damages. For instance, if information leakage has minimal impact on the organisation's mission, assets, or citizens, it is classified as Low Impact. If it significantly disrupts organisational operations, it is considered Moderate Impact, and if it poses severe risks to national security or human lives, it is classified as High Impact. This approach focuses on setting an appropriate security level for each system and applying security controls tailored to each classification.

In essence, the classification of information systems in the United States independently evaluates the sensitivity of information and the potential impact of breaches. This serves as the basis for adopting a detailed approach to security, enabling the implementation of granular security measures aligned with each classification.

Since 2006, the Republic of Korea has implemented and operated a network segregation system, primarily in government and public institutions. This system has played

a critical role in protecting the systems of government, public institutions, and financial companies from security threats and risks such as hacking [3]. However, with the accelerating pace of digital transformation and the advancement of cutting-edge technologies, such as cloud computing and artificial intelligence (AI), the network segregation system has become a limiting factor in leveraging these technologies.

In response, the Republic of Korea is transitioning from its traditional physical and logical network segregation system towards a more flexible approach. This involves adopting an MLS framework based on the classification of data sensitivity, aiming to strike a balance between the usability of data and the security level.

The Republic of Korea's MLS framework classifies data into two broad categories based on disclosure status: non-public and public data. Non-public data are further subdivided into Classified and Sensitive data, resulting in the following three classifications: Classified, Sensitive, and Open.

Subsequently, the framework analyses the configuration environment of information services and selects appropriate security controls that align with security principles based on the evaluation results. Table 1 shows a comparison of MLS in the Republic of Korea and the United States.

Table 1. Comparison analysis of the Republic of Korea and the United States' MLS.

Questions	Korea	US
Policy and Regulation	- National Information Security Basic Guidelines [20] - National Cloud Computing Security Guidelines [21]	- E-Government Act of 2002 (Public Law 107-347) [22] - Federal Information Security Management Act of 2002 (FISMA) [10]
Purpose	Enhancing security by applying different levels of security based on the importance of business information and information systems while fostering conditions for the utilisation of AI, cloud technologies, and public data in the public sector.	Providing criteria for classifying information systems and determining security levels to consistently apply the federal government's security policies and procedures within the RMF (Risk Management Framework) environment [23].
Applicable Target	Central Government, Local Government, Public Institutions	Federal agencies
Security categorisation	The sensitivity of the data stored, used, and processed by the system - Classified, Sensitive, Open	Information and information system potential impact - Low, Moderate, High
Base document	National Network Security Framework Guidelines (Scheduled for publication in February 2025) [24]	FIPS 199 (Standards for Security Categorisation) [19]

2.2. Zero Trust and Its Architecture

Zero Trust is a new security paradigm designed to protect organisational resources by continuously validating access requests to the resources. It is based on the principle of "never trust, always verify", and eliminates the concept of a trusted network inherent in traditional perimeter-based security models [15]. Zero Trust was initially introduced as a concept within cybersecurity, but, over time, it has evolved into a comprehensive and advanced security model through various studies and practical applications. Since the early 2000s, the limitations of static defences in perimeter-based security models have been identified. The Jericho Forum addressed these issues by publishing research on de-perimeterisation [25], and, in 2010, the concept was further developed by John Kindervag, a researcher at Forrester [26]. John's research highlighted that implicit trust within a network

increases vulnerabilities to lateral movement and insider threats. He proposed adopting a security framework that continuously validates access requests at all points of interaction.

Zero Trust is a security model based on the principle of "never trust, always verify", requiring continuous authentication and validation for all access requests. The NIST SP 800-207 [27], Zero Trust Architecture (ZTA), provides a framework for implementing these tenets and defines ZTA as "an enterprise cybersecurity architecture designed based on Zero Trust principles, aiming to prevent data breaches and restrict lateral movement within networks [15]".

NIST SP 800-207 outlines seven tenets that serve as Zero Trust principles, including treating all data and computing services as resources, securing all communications regardless of network location, and applying dynamic access policies based on contextual attributes. These tenets support the logical architecture design for access control through key components such as the Policy Enforcement Point (PEP), Policy Decision Point (PDP), and Policy Information Point (PIP).

Furthermore, based on the theoretical principles outlined in NIST SP 800-207, NIST SP 1800-35 [28] provides practical guidance for implementing ZTA in enterprise environments [29]. This document expands the applicability of ZTA through security technologies such as Enhanced Identity Governance (EIG), Software-Defined Perimeters (SDP), and micro-segmentation. In addition, it maps the security controls outlined in NIST SP 800-53 [18] and NIST Cybersecurity Framework (CSF) Version 1.1 and Version 2.0 [30,31], enabling the evaluation of Zero Trust Architecture's security capabilities, as well as the risk analysis and security measures.

Figure 1 illustrates the core and supporting components and processes of the general Zero Trust reference architecture proposed in NIST SP 1800-35. This architecture incorporates the Policy Enforcement Point (PEP) and the Policy Decision Point (PDP) defined in NIST SP 800-207. The Policy Information Point (PIP) plays a critical role in providing the information required by the PDP to make policy decisions.

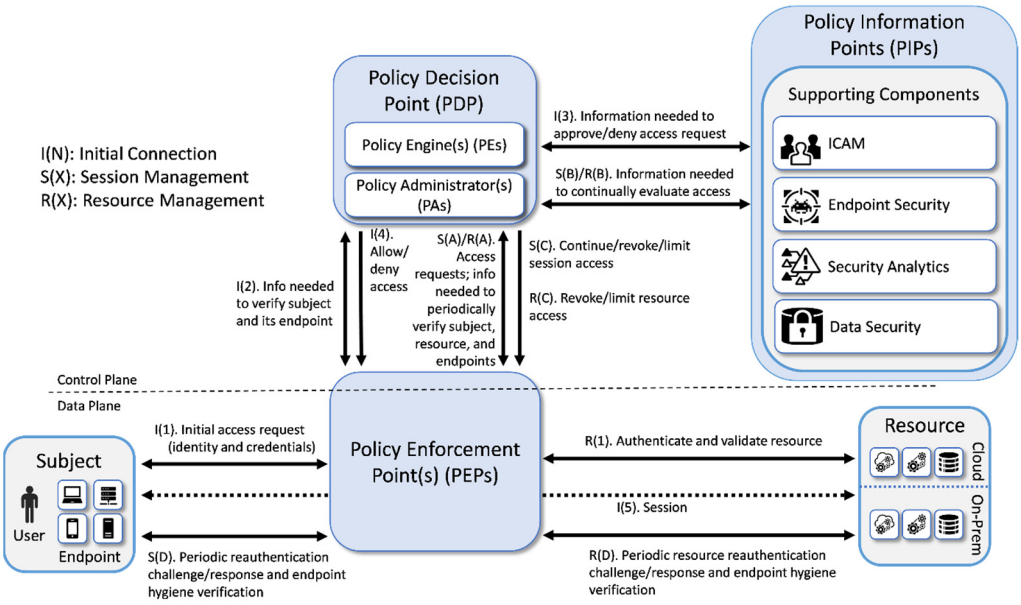


Figure 1. General Zero Trust Architecture reference [29].

The security process of ZTA consists of the following three steps: resource management, the session initiation step, and session management. In the session initiation step, a secure session is established through the authentication and authorisation of the subject. During the session management step, the security status of the session is continuously

assessed, while, in the resource management step, the security state of resources is periodically verified to maintain compliance.

NIST SP 1800-35 advances the theoretical principles presented in NIST SP 800-207 into a practical implementation strategy, enabling organisations to perform dynamic access management and strengthen their security posture. Through this approach, ZTA provides an effective solution to address the complex cybersecurity threats of the modern era.

3. Introduction of MLS Classification Criteria and Proposed Zero-Trust-Based MLS Model

3.1. Multi-Level Security Classification Criteria in the Republic of Korea

In the Republic of Korea, the network segregation systems adopted by the government and public institutions have posed challenges to the adoption of cloud computing technologies and the application of AI technologies. The Republic of Korea is exploring transitioning to a Zero-Trust-based Multi-Level Security framework to overcome these limitations. The core of the Republic of Korea's Multi-Level Security framework lies in categorising data based on operational data sensitivity into Classified data (C), Sensitive data (S), and Open data (O), and applying differentiated security controls accordingly. Figure 2 shows the classification criteria based on data sensitivity [32].

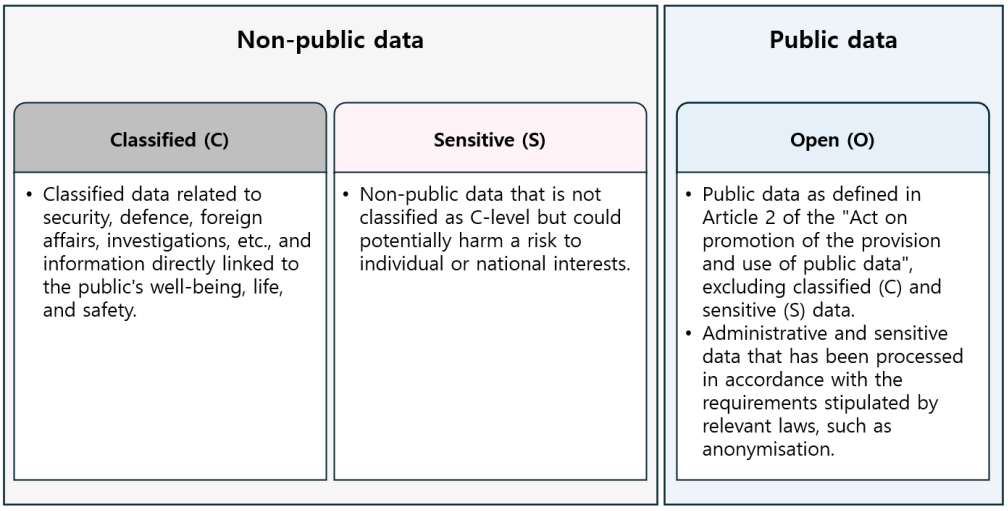


Figure 2. Classification criteria based on MLS data sensitivity [32].

However, most information systems store and process data of varying classifications. In such cases, it may be challenging to apply differentiated security controls based solely on data sensitivity. To address this, information systems storing or processing data are also classified into three levels of equivalent data, and security controls are applied accordingly. The classification of an information system is determined based on the highest level of data stored or processed within that system. For instance, if both Classified data (C) and Sensitive data (S) are present within a single information system, the system is classified as C. Based on this principle, when data of different classifications are stored, generated, or transferred within the same system, the security principles illustrated in Figure 3 are applied [32].

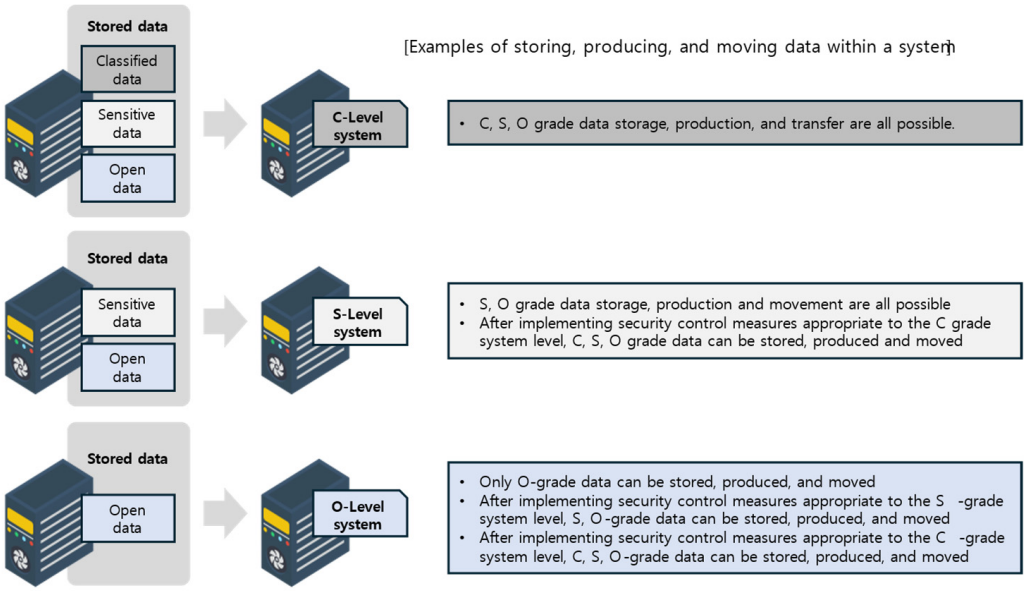


Figure 3. Security principles according to information and system level [32].

3.2. Proposed Zero-Trust-Based MLS Model

Section 4.2 presents an MLS model based on Zero Trust. The proposed security model incorporates PDP and PEP, the core logical components of the Zero Trust Architecture, and classifies resources into Classified, Sensitive, and Open categories according to the MLS framework of the Republic of Korea. Furthermore, if data of different classifications are stored within a single system, lateral movement between classifications within the same system is prohibited, in accordance with Zero Trust principles.

Figure 4 depicts the proposed Zero-Trust-based MLS model and data flow. The proposed security model categorises data flow into three broad types based on the resources accessed. The three categories are as follows:

- When an external subject accesses C-level resources (Orange line): C-level resources represent the highest level of data or systems, such as national secrets, requiring security equivalent to the traditional network segregation framework. Therefore, external users who are not located within the same network as the C-level data or systems can only transmit data via network bridging solutions within the network segregation system.
- When an internal subject accesses C-level resources (Green line): This type of subject resides within the same network as the C-level resources and refers to users or systems authorised to access C-level data or information systems. Since they are located within the same network as the C-level resources, there is no need for network bridging solutions during communication. However, access to the resources is granted only after validation by the PDP and PEP, in accordance with Zero Trust principles.
- When a subject accesses S- and O-level resources, regardless of being internal or external (Blue line): This type involves access to resources other than C-level resources (i.e., S- and O-level resources). Access is dynamically controlled by the PDP and PEP based on the subject's identity and authorisation, as well as the state of the resource being accessed.

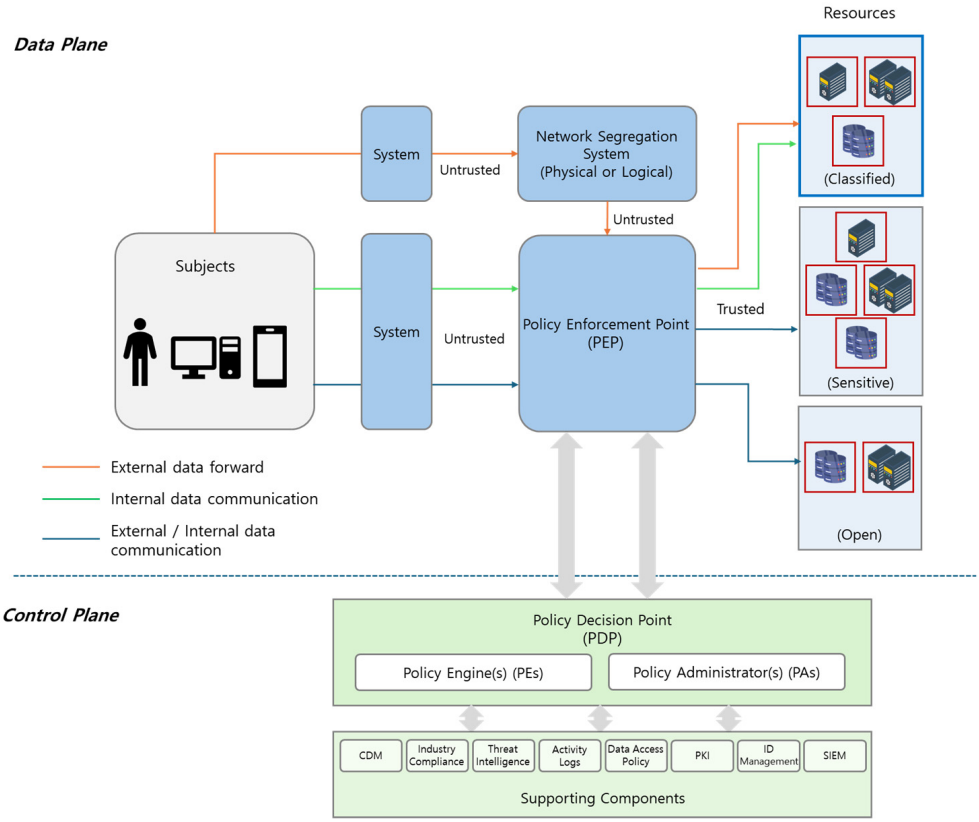


Figure 4. Proposed Zero-Trust-based MLS Model.

The MLS model offers the advantage of systematically managing and categorising an organisation's assets and data. However, it is primarily based on static security controls, making it challenging to adapt to dynamic environmental changes. The ZT model provides robust security through its inherent characteristic of validating all access requests. However, excessive security measures may potentially decrease operational productivity [33]. Therefore, when adopting a Zero-Trust-based model, resolving the trade-off between security and operational efficiency is crucial. Also, there are several studies that have explored approaches and technologies, such as multi-factor authentication (MFA) and adaptive authentication, to balance between these two models [34–36].

As such, the proposed model in this study aims to leverage the advantages of these two models, seeking to overcome the limitations of static security controls in the MLS through the automated dynamic access control of Zero Trust. One of the key elements of a Zero-Trust-based security model is the automated decision making and enforcement of security policies. This involves controlling and continuously validating access to networks and resources and is particularly related to dynamic access control. Dynamic access control does not rely on static rules. Instead, it dynamically adjusts access permissions based on the status of users and systems, environmental factors, and real-time active logs [37]. In essence, dynamic access control underpins automated security policy decision making and enforcement, contributing to the establishment of a more efficient security environment. This enables security administrators and operators to reduce the need for manually managing access permissions, as the system automatically applies and enforces security policies. As a result, this approach enhances management and operational efficiency, providing the capability to respond promptly to evolving security demands in real-time.

3.3. Risk Analysis of Proposed Zero-Trust-Based MLS Model

Security risk refers to the potential for malicious actors (or unintentional actions or incidents) to harm, damage, cause loss to, render unusable, or reduce the effectiveness of security controls for organisational assets [38]. This section identifies and systematically classifies various security risks that may arise within an organisation. The identified risks that could impact data or systems across all levels (C, S, and O) are defined as General risks. Risks that may occur across two levels are classified under the level associated with the higher data sensitivity.

Tables 2–5 illustrate the risks categorised into the following four classifications: General, Classified, Sensitive, and Open.

Table 2. General risks.

General Risks	Description
Data Tampering	Possibility of decreased reliability due to unauthorised modification of data.
Insider Threat	Potential for insiders to leak or misuse data without authorisation.
Unauthorized Access	Risk of unauthorised users accessing the system.
Malware and Ransomware Infection	Potential for data loss or system failure due to malware infection.
Privilege Abuse	Possibility of authorised users improperly accessing or modifying data.
Poor Log Management	Limitations in detecting and tracking abnormal activities.
Phishing and Social Engineering Attacks	Risk of users being deceived into leaking data or credentials being stolen.
Data Backup Failure	Failure to recover data during system failures.
Device Loss and Theft	Risk of data exposure due to device loss or theft.
DoS and DDoS Attacks	Attacks that compromise availability through denial-of-service.
Network Security Vulnerabilities	Risk of external attacks if network security is weak.
Administrator Privilege Compromise	Possibility of unauthorised access to critical national data if administrator privileges are stolen.
Lack of User Security Awareness	Potential for basic security incidents due to users' lack of security awareness.

Table 3. Risk according to the Classified level risks.

Potential Risks	Description
National Secret Leakage	Risk of exposing classified information that could severely impact national security if leaked.
Cyber Terrorism and Attacks	Risk of data leakage or destruction due to attacks targeting critical national assets.
Real-Time Monitoring Failure	Potential risks arising from the failure of real-time monitoring.
Physical Security Breach	Risk of intrusion, theft, or tampering at physical locations where data are stored.
Encryption Key Management Failure	Risk of exposing encrypted confidential information due to compromised encryption keys.
High-Risk System Vulnerabilities	Potential for external attacks due to system vulnerabilities.
Lack of Regular Security Audits	Risk of security defects being exposed if periodic audits are not conducted.

Table 4. Risk according to the Sensitive level risks.

Potential Risk	Description
Personal Information Leakage	Risk of personal information being leaked, leading to violations of individual rights and identity theft.
Data Integrity Compromise	Risk of Sensitive data being tampered with, providing incorrect information to individuals.
Sensitive Data Leakage from Privilege Abuse	Risk of authorised users misusing sensitive information.
Inadequate Access Control for External Contractors	Risk posed by external personnel handling sensitive information not adhering to security procedures.
Insufficient Periodic Access Rights Review	Risk of unauthorised individuals accessing data for extended periods due to inadequate access rights reviews.
Unauthorised Access to Backup Data	Risk of unauthorised access to backed-up Sensitive data.
Missing Log Records	Risk of missing logs of sensitive information access, making it difficult to trace causes in case of incidents.
Insufficient Auditing	Risk of security issues arising from inadequate audits of sensitive information access.

Table 5. Risk according to the Open level risks.

Potential Risks	Description
Unauthorised Information Modification	Risk of public information being altered, potentially compromising its reliability.
Public Data Deletion	Risk of public data being deleted, preventing the seamless provision of services.
Lack of Basic Access Control	Risk of unauthorised individuals easily accessing and viewing information.
Security Vulnerabilities Due to Unpatched Systems	Risk of the system being exposed to attacks due to the lack of the latest patches.
Information Distortion	Risk of public information being tampered with, leading to the dissemination of incorrect information.
General Phishing Attacks	Risk of information being misused due to providers being deceived by phishing attacks.
Network Configuration Errors	Risk of service disruption due to availability issues caused by network configuration errors.
Poor Device Management	Risk of physical security being compromised if public information devices are lost or stolen.

3.4. Key Components in the Proposed Zero-Trust-Based MLS Model

This section describes the key components of the model proposed in Section 3.2 above. Table 6 shows the detailed descriptions of each key component for the proposed model.

Table 6. Key components of the proposed security model.

Key Components	Description
Subject	The entity attempting to access a resource, including users or endpoint devices (e.g., mobile, PC).
Network Segregation System	Refers to the network segregation device, providing physical/logical separation between the internal network (where C-grade resources are located) and the external network connected to the internet. It may facilitate data transfer between networks through a network connection solution.

Table 6. *Cont.*

Key Components	Description
Policy Decision Point (PDP)	Composed of the Policy Engine (PE) and Policy Administrator (PA), it decides whether to approve or deny access requests and commands the PEP accordingly.
Policy Engine (PE)	An entity responsible for approving access requests based on trust evaluation algorithms.
Policy Administrator (PA)	An entity that communicates the start and end of sessions to the PEP based on decisions made by the Policy Engine.
Policy Enforcement Point (PEP)	An entity that connects the subject to the resource based on the commands from the PDP and ultimately terminates the connection.
Supporting Components	Organisational policies, logs, and other information used by the PE to evaluate access requests.

3.5. Comparison Analysis Between Proposed Zero-Trust-Based MLS Model with Other Models

By comparing the proposed model with the standalone MLS and Zero Trust model, this study aims to analyse the gaps between the standalone approaches and verify whether the proposed model is suitable for addressing the limitations of the standalone models. Additionally, it seeks to ensure adaptability to various operational environments by considering security and flexibility in adopting cutting-edge technologies. Finally, through the comparative analysis of the models, this study highlights the advantages of the proposed approach, emphasising its necessity and its contribution to advancing security practices.

Table 7 shows a comparative analysis of the proposed model, Zero Trust (ZT) model, and MLS-based Bell–Lapadula model. It involves deciding whether additional technologies or strategies are considered to enhance security, whether specific security controls or capabilities are proposed, whether security controls or capabilities are categorised and provided, with a focus on data protection, and the basis for security label classification. Through this comparison analysis, it is possible to determine whether the proposed model demonstrates superiority over the standalone models in terms of security and practical applicability.

Table 7. Comparative analysis of the other models.

Questions	ZT-Based MLS Model	CISA Maturity Model [39]	Bell–Lapadula Model [40] (MLS-Basis)
What is the type of the model?	Convergence model (ZT+MLS)	Single model	Single model
Does it propose a specific model?	To implement a Zero-Trust-based network, we propose a dynamic access control model based on the importance of key components and data	Presents a simple pillar-based maturity model	A model that describes a set of access control rules using security labels on objects and permissions on subjects
Does it consider additional technologies or strategies for improving security?	Considered In particular, a flexible network separation control strategy for introducing new technologies such as AI for the Classified level is presented	None	None
Does it propose security controls or capabilities?	Specific security controls for each component (e.g., PEP: AC-3-2: Dynamic Information Flow Control)	High-level capabilities for each pillar (Not specific. Vague and abstract)	None
Does it classify and provide security controls or capabilities focused on data protection?	Provides security controls for the sensitivity of data used, utilised, and processed in the organisation	Presenting capabilities focused on maturity	None
What is the basis for the classification of security labels?	Classification by data sensitivity - Classified, Sensitive, Open	Classification by maturity - Traditional, Initial, Advanced, Optimal	Classification of subject and object - Top secret, Secret, Confidential, Unclassified

4. Proposed Security Controls for the Zero-Trust-Based MLS Model and Its Robustness

4.1. Security Controls

Security controls refer to policies, procedures, technologies, and other measures designed to minimise security risks to organisational assets and enhance the overall security level [41]. Security controls are generally categorised into the following three types based on their nature: administrative, technical, and physical controls [42]. These are described as follows:

- Administrative controls: Security controls that manage security through policies, procedures, guidelines, and employee training.
- Technical controls: Security controls that utilise technical means, such as security solutions or equipment, to protect the organisation's information assets.
- Physical controls: Security controls aimed at protecting the organisation's facilities or infrastructure from physical threats.

The organisation's security manager selects the necessary security control measures based on the organisational environment and information assets, ensuring their appropriate application. This approach helps to minimise damage in the event of incidents, such as security breaches, and enables the establishment of a more secure organisational infrastructure [43].

In this section, the security controls required for the model proposed in Section 4 are provided. Security controls to be applied to the model's key components are categorised according to each data classification. Referring to NIST SP 800-53 [18], the security controls were selected and differentially categorised based on the level of data sensitivity.

First, the security controls that should be applied across the proposed model as a whole were involved in general. Additionally, specific controls required for key components of the model, including PDP, PEP, Resource, and Subject, were identified accordingly. Figure 5 summarises the security controls for the ZT-based MLS model. These security controls consist of general security controls that can be applied across all components of the proposed model and specific security controls for each of the four components. Furthermore, the required security controls vary according to the sensitivity of the organisational data, which are classified into the following three levels: C, S, and O.

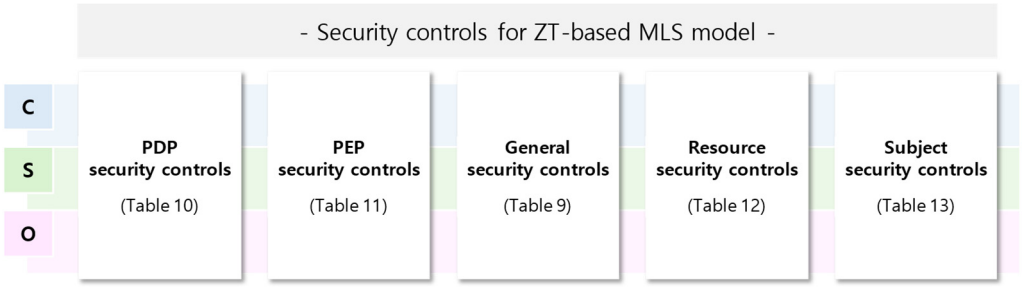


Figure 5. Summary of security controls for ZT-based MLS model.

Tables 8–12 outline the security controls that should be applied for the key components of the model proposed in Section 4 to implement an MLS framework. The leftmost column specifies the overarching security controls, with newly assigned numbers based on the security controls defined in NIST SP 800-53. The central column details the specific security controls corresponding to the overarching security controls, categorised by the level of security required for each classification. The labels in parentheses, such as (AC-17), refer to those described in NIST SP 800-53. For C-level data and systems, the highest level of security controls, equivalent to those of the traditional network segregation framework, was

applied. For S-level data and systems, high-level security controls satisfying the highest maturity level (Optimal) defined in CISA's Zero Trust maturity model [39] were applied. Finally, for O-level data and systems, security controls were applied to ensure availability and integrity while considering data usability aspects.

Table 8. General security controls.

Control	Specific Controls	C	S	O
AC-6 Remote Access (AC-17)	AC-6-1: Protection of Confidentiality and Integrity Using Encryption	√	√	
	AC-6-2: Privileged Commands and Access	√	√	√
	AC-6-3: Disconnect or Disable Access	√	√	√
	AC-6-4: Authenticate Remote Commands	√	√	√
AC-9 External Systems (AC-20)	AC-9-1: Limits on Authorised Use	√	√	
	AC-9-2: Non-Organisationally Owned Systems: Restricted Use	√	√	
	AC-9-3: Network Accessible Storage Devices: Prohibited Use	√	√	
CA-1 Continuous Monitoring (CA-7)	CA-1-1: Trend Analysis	√	√	√
	CA-1-2: Risk Monitoring	√	√	√
	CA-1-3: Automation Support for Monitoring	√	√	√
SC-3 Transmission Confidentiality and Integrity (SC-8)	Sc-3-1: Cryptographic Protection	√	√	√
	SC-3-2: Conceal or Randomise Communications	√	√	
SC-5 Cryptographic Protection (SC-13)	SC-5: Cryptographic Protection	√	√	√
CM-1 Baseline Configuration (CM-2)	CM-1-1: Automation Support for Accuracy and Currency	√	√	√
	CM-1-2: Retention of Previous Configurations	√	√	√
	CM-1-3: Development and Test Environments	√	√	√
CM-2 Impact Analysis (CM-4)	CM-2-1: Separate Test Environments	√	√	√
	CM-2-2: Verification of Controls	√	√	√
CM-3 Configuration Settings (CM-6)	CM-3-1: Automated Management, Application, and Verification	√	√	√
	CM-3-2: Respond to Unauthorised Changes	√	√	√
CM-4 Software Usage Restrictions (CM-10)	CM-4: Software Usage Restrictions	√	√	√
CM-5 User Installed Software (CM-11)	CM-5-1: Software Installation with Privileged Status	√		
CM-6 Signed Components (CM-14)	CM-6: Signed Components	√	√	√
RA-1 Risk Assessment (RA-3)	RA-1-1: Supply Chain Risk Assessment	√	√	√
	RA-1-2: Use of All Source Intelligence	√	√	√
	RA-1-3: Dynamic Threat Awareness	√	√	√
	RA-1-4: Predictive Cyber Analytics	√	√	√
RA-2 Vulnerability Monitoring and Scanning (RA-5)	RA-2-1: Impact-Level Prioritisation	√	√	
SI-1 Flaw Remediation (SI-2)	SI-1-1: Automated Flow Remediation Status	√	√	
	SI-1-2: Automated Patch Management Tools	√	√	√
	SI-1-3: Automatic Software and Firmware Updates	√	√	√
	SI-1-4: Removal of Previous Versions of Software and Firmware	√	√	√
SI-2 Malicious Code Protection (SI-3)	SI-2-1: Update Only by Privileged Users	√	√	√
	SI-2-2: Detect Unauthorised Commands	√	√	√
	SI-2-3: Malicious Code Analysis	√		
SI-5 Software, Firmware, and Information Integrity (SI-7)	SI-5-1: Integrity Checks	√	√	√
	SI-5-2: Automation Support for Distributed Testing	√	√	
	SI-5-3: Automated Notifications of Integrity Violations	√	√	
	SI-5-4: Cryptographic Protection	√	√	√
	SI-5-5: Integration of Detection and Response	√	√	√
	SI-5-6: Auditing Capability for Significant Events	√	√	√
	SI-5-7: Integrity Verification	√	√	√
	SI-5-8: Time Limit on Process Execution Without Supervision	√		

Table 9. PDP security controls.

Control	Specific Controls	C	S	O
AC-1 Access Enforcement (AC-3)	AC-1-1: Dual Authorisation	√	√	
	AC-1-2: Assert and Enforce Application Access	√	√	√
	AC-1-3: Discretionary and Mandatory Access Control	√	√	√
AC-6 Remote Access (AC-17)	AC-6-1: Protection of Confidentiality and Integrity Using Encryption	√	√	
	AC-6-2: Privileged Commands and Access	√	√	√
	AC-6-3: DISCONNECT OR DISABLE ACCESS	√	√	√
	AC-6-4: Authenticate Remote Commands	√	√	√
AC-8 Access Control for Mobile Devices (AC-19)	AC-8-1: Restrictions for Classified Information	√	√	
	AC-8-2: Full-Device- or Container-Based Encryption	√	√	
AC-9 External Systems (AC-20)	AC-9-1: Limits on Authorised Use	√	√	
	AC-9-2: Non-Organisationally Owned Systems: Restricted Use	√	√	
	AC-9-3: Network Accessible Storage Devices: Prohibited Use	√	√	
AC-10 Access Control Decisions (AC-24)	AC-10-1: Transmit Access Authorisation Information	√	√	√
	AC-10-2: No User of Process Identity	√	√	√
SC-6 Collaborative Computing Devices and Applications (SC-15)	SC-6-1: Physical or Logical Disconnect	√	√	

Table 10. PEP security controls.

Control	Specific Controls	C	S	O
AC-1 Access Enforcement (AC-3)	AC-1-1: Dual Authorisation	√	√	
	AC-1-2: Assert and Enforce Application Access	√	√	√
	AC-1-3: Discretionary and Mandatory Access Control	√	√	√
AC-2 Account Management (AC-2)	AC-2-1: Automated System Account Management	√	√	
	AC-2-2: Disable Accounts	√	√	√
	AC-2-3: Automated Audit Action	√	√	
	AC-2-4: Inactivity Logout	√	√	√
	AC-2-5: Dynamic Privilege Management	√	√	√
	AC-2-6: Privileged User Accounts	√	√	√
	AC-2-7: Dynamic Account Management	√	√	√
	AC-2-8: Account Monitoring for Atypical Usage	√	√	√
AC-3 Information Flow Enforcement (AC-4)	AC-3-1: Object Security and Privacy Attributes	√	√	√
	AC-3-2: Dynamic Information Flow Control	√	√	√
	AC-3-3: Flow Control of Encrypted Information	√	√	√
	AC-3-4: One-Way Flow Mechanism	√	√	
	AC-3-5: Security and Privacy Policy Filters	√	√	√
	AC-3-6: Human Reviews	√	√	
	AC-3-7: Data Type Identifiers	√	√	√
	AC-3-8: Detection of Unsanctioned Information	√	√	√
	AC-3-9: Approved Solutions	√	√	√
	AC-3-10: Physical or Logical Separation of Information Flows	√		
	AC-3-11: Modify Non-Releasable Information	√	√	√
	AC-3-12: Data Sanitisation	√		
	AC-3-13: Filter Orchestration Engines	√	√	√
AC-4 Session Termination (AC-12)	AC-4-1: Timeout Warning Message	√	√	
AC-6 Remote Access (AC-17)	AC-6-1: Protection of Confidentiality and Integrity Using Encryption	√	√	
	AC-6-2: Privileged Commands and Access	√	√	
	AC-6-3: Disconnect or Disable Access	√	√	
	AC-6-4: Authenticate Remote Commands	√	√	
AC-7 Wireless Access (AC-18)	AC-7-1: Authentication and Encryption	√	√	
	AC-7-2: Disable Wireless Networking	√	√	
AC-8 Access Control for Mobile Devices (AC-19)	AC-8-1: Restrictions for Classified Information	√	√	
	AC-8-2: Full-Device- or Container-Based Encryption	√	√	

Table 10. *Cont.*

Control	Specific Controls	C	S	O
AC-9 External Systems (AC-20)	AC-9-1: Limits on Authorised Use	√	√	
	AC-9-2: Non-Organisationally Owned Systems: Restricted Use	√	√	
	AC-9-3: Network Accessible Storage Devices: Prohibited Use	√	√	
CA-1 Continuous Monitoring (CA-7)	CA-1-1: Trend Analysis	√	√	√
	CA-1-2: Risk Monitoring	√	√	√
	CA-1-3: Automation Support for Monitoring	√	√	√
IR-1 Incident Handling (IR-4)	IR-1-1: Automated Incident Handling Processes	√	√	√
	IR-1-2: Dynamic Reconfiguration	√	√	√
	IR-1-3: Continuity of Operation	√	√	√
	IR-1-4: Information Correlation	√	√	√
SC-2 Boundary Protection (SC-7)	SC-2-1: Physically Separated Subnetworks	√		
	SC-2-2: Access Point	√		
	SC-2-3: Deny by Default—Allow by Exception	√	√	
	SC-2-4: Restrict Threatening Outgoing Communication Traffic	√	√	
	SC-2-5: Prevent Exfiltration	√	√	
	SC-2-6: Restrict Incoming Communication Traffic	√	√	
	SC-2-7: Project Against Unauthorised Physical Connections	√	√	
	SC-2-8: Prevent Discovery of System Component	√	√	
	SC-2-9: Block Communication from Non-Organisationally Configured Hosts	√	√	
	SC-2-10: Personally Identifiable Information	√	√	
	SC-2-11: Classified National Security System Connections	√		
	SC-2-12: Connections to Public Networks	√		
SC-6 Collaborative Computing Devices and Applications (SC-15)	SC-6-1: Physical or Logical Disconnect	√	√	
SC-7 Session Authenticity (SC-23)	SC-7-1: Invalidate Session Identifiers at Logout	√	√	√
	SC-7-2: Allowed Certificate Authorities	√	√	√
SC-9 System Partitioning (SC-32)	SC-9-1: Separate Physical Domains for Privileged Functions	√	√	√
SC-10 Port and I/O Device Access (SC-41)	SC-10: Port and I/O Device Access	√	√	√
SC-11 Usage Restrictions (SC-4)	SC-11: Usage Restrictions	√	√	√
SI-3 System Monitoring (SI-4)	SI-3-1: System-Wide Intrusion Detection System	√	√	√
	SI-3-2: Automated Tools and Mechanisms for Real-Time Analysis	√	√	√
	SI-3-3: Automated Tool and Mechanism Integration	√	√	√
	SI-3-4: Inbound and Outbound Communication Traffic	√	√	√

Table 11. Resource security controls.

Control	Specific Controls	C	S	O
SC-8 Protection of Information at Rest (SC-28)	SC-8-1: Cryptographic Protection	√	√	
	SC-8-2: Offline Storage	√	√	
	SC-8-3: Cryptographic Keys	√	√	
AC-6 Remote Access (AC-17)	AC-6-1: Protection of Confidentiality and Integrity Using Encryption	√	√	
	AC-6-2: Privileged Commands and Access	√	√	√
	AC-6-3: Disconnect or Disable Access	√	√	√
	AC-6-4: Authenticate Remote Commands	√	√	√
SC-3 Transmission Confidentiality and Integrity (SC-8)	SC-3-1: Cryptographic Protection	√	√	
	SC-3-2: Conceal or Randomise Communications	√	√	
SC-4 Cryptographic Key Establishment and Management (SC-12)	SC-4-1: Availability	√	√	
	SC-4-2: Symmetric Keys	√	√	
	SC-4-3: Asymmetric Keys	√	√	√
AC-5 Security and Privacy Attributes (AC-16)	AC-5-1: Dynamic Attribute Association	√	√	√
	AC-5-2: Maintenance of Attribute Association by Individuals	√	√	√
	AC-5-3: Attribute Displays on Objects to be Output	√	√	√
	AC-5-4: Consistent Attribute Interpretation	√	√	√
	AC-5-5: Attribute Reassignment—Regrading Mechanisms	√	√	

Table 11. *Cont.*

Control	Specific Controls	C	S	O
SC-1 Information in Shared System Resources (SC-4)	SC-1-2: Multi-Level or Periods Processing	√	√	√
SC-8 Protection of Information at Rest (SC-28)	SC-8-1: Cryptographic Protection	√	√	
	SC-8-2: Offline Storage	√	√	
	SC-8-3: Cryptographic Keys	√	√	
SC-2 Boundary Protection (SC-7)	SC-2-1: Physically Separated Subnetworks	√		
	SC-2-2: Access Point	√		
	SC-2-3: Deny by Default—Allow by Exception	√	√	
	SC-2-4: Restrict Threatening Outgoing Communication Traffic	√	√	
	SC-2-5: Prevent Exfiltration	√	√	
	SC-2-6: Restrict Incoming Communication Traffic	√	√	
	SC-2-7: Project Against Unauthorised Physical Connections	√	√	
	SC-2-8: Prevent Discovery of System Component	√	√	
	SC-2-9: Block Communication from Non-Organisationally Configured Hosts	√	√	
	SC-2-10: Personally Identifiable Information	√	√	
	SC-2-11: Classified National Security System Connections	√		
	SC-2-12: Connections to Public Networks	√		

Table 12. Subject security controls.

Control	Specific Controls	C	S	O
AC-1 Access Enforcement (AC-3)	AC-1-1: Dual Authorisation	√	√	
	AC-1-2: Assert and Enforce Application Access	√	√	√
	AC-1-3: Discretionary and Mandatory Access Control	√	√	√
AC-2 Account Management (AC-2)	AC-2-1: Automated System Account Management	√	√	
	AC-2-2: Disable Accounts	√	√	√
	AC-2-3: Automated Audit Action	√	√	
	AC-2-4: Inactivity Logout	√	√	√
	AC-2-5: Dynamic Privilege Management	√	√	√
	AC-2-6: Privileged User Accounts	√	√	√
	AC-2-7: Dynamic Account Management	√	√	√
	AC-2-8: Account Monitoring for Atypical Usage	√	√	√
AC-3 Information Flow Enforcement (AC-4)	AC-3-1: Object Security and Privacy Attributes	√	√	√
	AC-3-2: Dynamic Information Flow Control	√	√	√
	AC-3-3: Flow Control of Encrypted Information	√	√	√
	AC-3-4: One-Way Flow Mechanism	√	√	
	AC-3-5: Security and Privacy Policy Filters	√	√	√
	AC-3-6: Human Reviews	√	√	
	AC-3-7: Data Type Identifiers	√	√	√
	AC-3-8: Detection of Unsanctioned Information	√	√	√
	AC-3-9: Approved Solutions	√	√	√
	AC-3-10: Physical or Logical Separation of Information Flows	√		
	AC-3-11: Modify Non-Releasable Information	√	√	√
	AC-3-12: Data Sanitisation	√		
	AC-3-13: Filter Orchestration Engines	√	√	√
AC-10 Access Control Decisions (AC-24)	AC-10-1: No User or Process Identity	√	√	√
AC-11 Separation of duties (AC-5)	AC-11: Separation of Duties	√	√	√
AC-12 Least Privilege (AC-6)	AC-12-1 Authorise Access to Security Functions	√	√	
	AC-12-2: Non-Privileged Access for Non-security Functions	√	√	√
	AC-12-3: Network Access to Privileged Commands	√	√	
	AC-12-4: Separate Processing Domains	√	√	
	AC-12-5: Privileged Accounts	√	√	
	AC-12-6: Privileged Access by Non-Organisational Users	√	√	
	AC-12-7: Review of User Privileges	√	√	√
	AC-12-8: Privilege Levels for Code Execution	√	√	√
	AC-12-9: Log Use of Privileged Functions	√	√	√
	AC-12-10: Prohibit Non-Privileged Users from Executing Privileged Functions	√	√	√

Table 12. *Cont.*

Control	Specific Controls	C	S	O
IA-1 Policy and Procedures (IA-1)	IA-1: Policy And Procedures	√	√	√
IA-2 Identification and Authentication (Organizational Users) (IA-2)	IA-2-1: Multi-Factor Authentication to Privileged Accounts	√	√	
	IA-2-2 Multi-Factor Authentication to Non-Privileged Accounts	√	√	
	IA-2-3 Individual Authentication with Group Authentication	√	√	
	IA-2-4 Access to Accounts—Separate Device	√	√	
	IA-2-5: Access to Accounts—Replay Resistant	√	√	
	IA-2-6: Acceptance of PIV Credentials	√	√	
	IA-2-7: Out-Of-Band Authentication	√	√	
IA-3 Device Identification and Authentication (IA-3)	IA-3-1: Cryptographic Bidirectional Authentication	√	√	
	IA-3-2: Device Attestation	√	√	
IA-4 Authentication Management (IA-5)	IA-4-1: Password-Based Authentication	√	√	
	IA-4-2: Public-Key-Based Authentication	√	√	
	IA-4-3: Protection of Authenticators	√	√	√
	IA-4-4: Multiple System Accounts	√	√	
	IA-4-5: Federated Credential Management	√	√	
	IA-4-6: Biometric Authentication Performance	√	√	
	IA-4-7: Expiration of Cached Authenticators	√	√	√
	IA-4-8: Managing Content of PKI Trust Stores	√	√	
	IA-4-9: Presentation Attack Detection for Biometric Authenticators	√	√	
	IA-4-10: Password Managers	√	√	√
IA-5 Identification and Authentication (Non-Organizational Users) (IA-8)	IA-5-1: Acceptance of PIV Credentials from Other Agencies	√	√	
	IA-5-2: Acceptance of External Authenticators	√	√	
	IA-5-3: Use of Defined Profiles	√	√	
	IA-5-4: Acceptance Of PIV-I Credentials	√	√	
	IA-5-5: Disassociability	√	√	
IA-6 Service Identification and Authentication (IA-9)	IA-6: Service Identification and Authentication	√	√	
IR-1 Incident Handling (IR-4)	IR-1-1: Automated Incident Handling Processes	√	√	√
	IR-1-2: Dynamic Reconfiguration	√	√	√
	IR-1-3: Continuity of Operation	√	√	√
	IR-1-4: Information Correlation	√	√	√

The security controls provided in this paper can be selectively applied by security professionals or cybersecurity teams based on the organisation's environment and information assets, allowing for the implementation of only the necessary measures. Additionally, it is possible to identify and apply further security controls beyond those specified in this study, if required.

Table 8 shows security controls that should be applied not only to specific components, but across the board, and categorises them according to their respective levels.

Table 9 shows the security controls that should be applied at the PDP of the proposed model and categorises them according to their respective levels.

Table 10 shows the security controls that should be applied at the PEP of the proposed model and categorises them according to their respective levels.

Table 11 shows the security controls that should be applied at the resource of the proposed model and categorises them according to their respective levels.

Table 12 shows the security controls that should be applied at the subject of the proposed model and categorises them according to their respective levels.

This paper proposes security controls that have been demonstrated to apply to security devices or solutions in operation. Moreover, these security controls can be selectively applied by security professionals or cybersecurity teams, depending on the organisation's environment and the characteristics of its information assets. Additional security controls not included in this study can also be identified and applied if necessary. Table 13 shows examples of the proposed security controls mapped to security solutions, such as NAC

and IDS [44]. These examples can serve as a reference to address real-world constraints (e.g., resource allocation or integration challenges) and facilitate practical solutions.

Table 13. Security control use cases in security solutions.

Security Solutions in Real World	Controls
Network Access Control (NAC)	AC-6: Remote Access (AC-17) CM-3: Configuration Settings (CM-6)
Intrusion Detection System (IDS)	CA-1: Continuous Monitoring (CA-7) RA-2: Vulnerability Monitoring and Scanning (RA-5)
Intrusion Prevention System (IPS)	AC-6: Remote Access (AC-17) AC-9: External Systems (AC-20)
Security Information Event Management (SIEM)	CA-1: Continuous Monitoring (CA-7) CM-2: Impact Analysis (CM-4) RA-1: Risk Assessment (RA-3)
Firewall	AC-6: Remote Access (AC-17) AC-9: External Systems (AC-20)
Virtual Private Network (VPN)	SC-3: Transmission Confidentiality and Integrity (SC-8)
DB Crypto Solution	SC-5: Cryptographic Protection (SC-13) SI-5: Software, Firmware, and Information Integrity (SI-7)
Patch Management System (PMS)	SI-1: Flaw Remediation (SI-3) CM-1: Baseline Configuration (CM-2) CM-6: Signed Components (CM-14)
Anti-Virus (AV)	SI-1: Flaw Remediation (SI-3) SI-2: Malicious Code Protection (SI-3) CM-6: Signed Components (CM-14)
Data Loss Prevention (DLP)	SC-3: Transmission Confidentiality and Integrity (SC-8)
Identity and Access Management (IAM)	CM-4: Software Usage Restrictions (CM-10) CM-5: User Installed Software (CM-11)

4.2. Robustness of Proposed Model Based on Attack Scenarios

This section introduces representative attack scenarios based on the risks identified in Section 3 and explains how the proposed security model in Section 4 defends against these risks through specific security controls. The two scenarios presented are based on a case attributed to attacks by North Korea's APT group [45] and an attack scenario disclosed by the National Security Agency (NSA) in the United States [46]. For each scenario, four significant risks are analysed, and the methods by which the proposed model's security controls address and mitigate these risks are described.

1. Attack Scenario 1
   A practical case related to Attack Scenario 1 is linked to North Korea's Andariel hacking group. Starting in October 2022, they launched attacks targeting the Republic of Korea's defence companies and contractors by stealing user credentials, infecting systems with malware, and exfiltrating data. Figure 6 illustrates the attack scenario and it involves an attacker compromising the credentials and device of an authorised user to install malware on the organisation's internal systems and exfiltrate Sensitive data, which is C-level data.
   - If the attacker uses the credentials of an authorised user with legitimate access to the organisational network, MFA (Multi-Factor Authentication) requires additional authentication. Furthermore, under the Zero Trust model, the access attempt would be detected as anomalous behaviour, since it is not originating from the user's usual device, enabling the system to defend against the attack (AC-1, AC-2, AC-8, AC-9, CA-1, IA-2).
   - If the attacker uses the authorised user's device to access the organisational network, MFA would demand additional authentication, such as biometric veri-

fication, providing strong authentication measures to defend against the attack (AC-1, AC-2, AC-9, IA-2).

- If malware is installed on critical systems after gaining access to the organisation's internal network, the Zero Trust principle prevents lateral movement, and the principle of least privilege ensures that unauthorised users cannot execute or modify data or files. This effectively prevents the propagation and installation of malware (AC-1, AC-2, AC-3, AC-5, AC-12, CA-1).
- Regarding the threat of Sensitive data exfiltration, security controls to detect and block anomalous traffic are applied, along with data encryption, providing robust protection against data leakage (AC-2, AC-3, AC-5, CA-1, SC-2, SC-8).

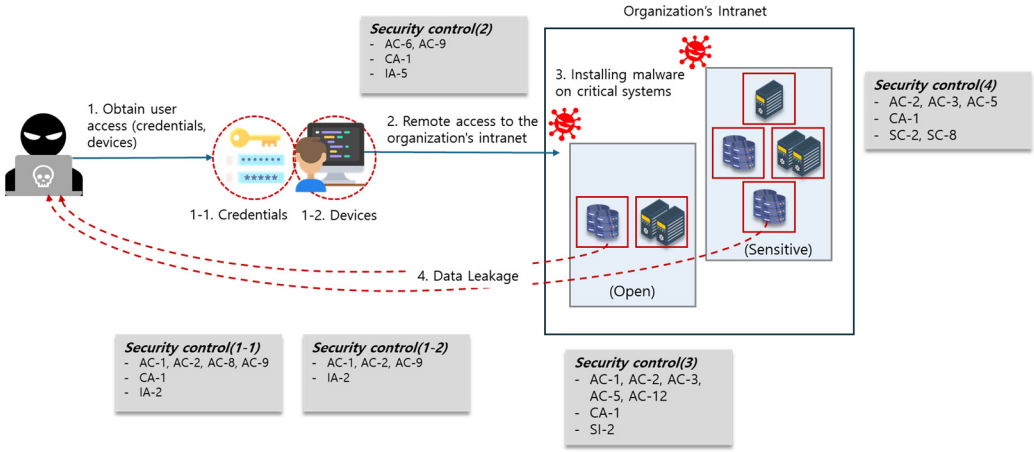


Figure 6. Attack Scenario 1.

2. Attack Scenario 2

A practical case for Attack Scenario 2 involves North Korea's Lazarus hacking group. Starting in November 2022, the group exploited vulnerabilities in network bridging systems to infiltrate internal networks and exfiltrate data from the Republic of Korea's defence companies and contractors. Figure 7 shows the attack from the North Korea's Lazarus hacking group and this scenario describes an attacker attempting to access a network-segregated environment to install malware on systems and exfiltrate Classified data, which is C-level data.

- The attacker targets organisational systems connected to the external network, which interfaces with the network bridging system, and attempts to infiltrate and distribute malware. However, as the organisation's systems adhere to the Zero Trust model, they employ diverse and robust authentication mechanisms and security controls against malware, effectively defending against the attack (AC-1, AC-2, AC-3, SI-2).
- If the attacker scans open ports used for testing purposes and attempts to infiltrate the internal network through the port, the organisation's security controls, such as those segregating the test environment and detecting anomalous traffic, enable defence against such attempts (CM-2, RA-2, SI-1, SC-6, SC-10, CA-1).
- Even if the attacker exploits vulnerabilities in the network bridging system to gain access to the internal network, the security controls applied within the network-segregated environment and the Zero Trust principles prevent lateral movement. Continuous validation of the permissions of subjects and objects further defends against attempts to collect critical organisational data (AC-1, AC-2, AC-3, AC-12, CA-1, SC-2, SI-3).

- Regarding the threat of classified data exfiltration, controls to detect and block anomalous traffic, as well as data encryption, ensure the prevention of data leaks (AC-2, AC-3, AC-5, CA-1, SC-2, SC-8).

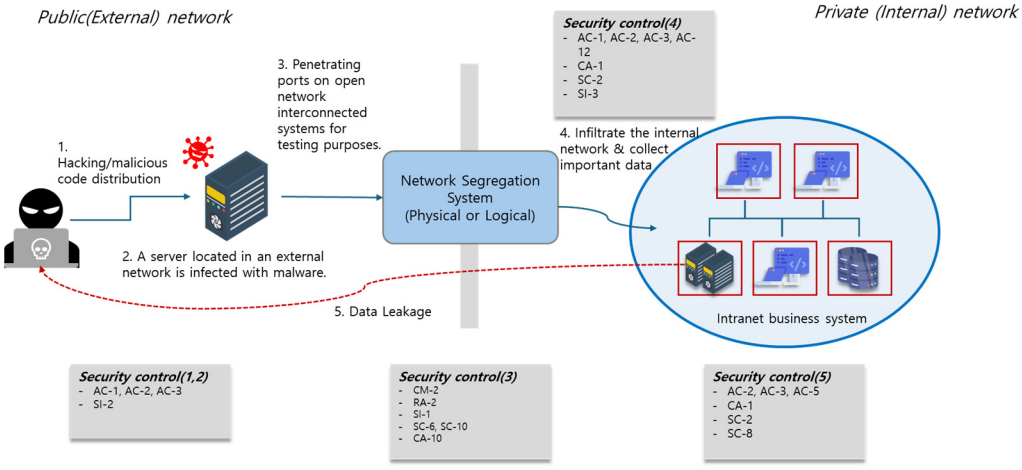


Figure 7. Attack Scenario 2.

Beyond the two attack scenarios described above, practical cases provide evidence of enhanced security controls. According to F5 Labs' "2023 Identity Threat Report: The Un-patchables" [47], an analysis of 159 companies and organisations identified credential stuffing, phishing, and multi-factor authentication (MFA) bypasses as major security attacks. Notably, the average attack rate of credential stuffing attacks was 19.4%, but it decreased significantly to 6% in organisations that implemented security controls such as MFA. This shows that MFA, or similar security controls, mitigate automated cyber-attacks. These cases imply that the appropriate security controls in practical environments can contribute to improving overall security.

5. Conclusions

5.1. Research Summary

The increasing utilisation of ICT technologies has played a significant role in enhancing organisational productivity. However, traditional network segregation systems have become a barrier to adopting new ICT technologies. While research into MLS frameworks is being conducted to overcome these limitations, the static access control approach of traditional MLS frameworks remains inadequate for effectively addressing dynamic security threats. Consequently, there is a growing need for research to develop a new security model that integrates the Zero Trust model, which supports dynamic access control, with the MLS framework.

This paper proposes a Zero-Trust-based MLS model and identifies potential risks through an impact analysis based on data classification by sensitivity. Additionally, to mitigate the identified risks, it systematically provides security controls to be applied to the components of the proposed security model and evaluates the model's security effectiveness through attack scenarios. This study aims to present a new security strategy for improving network segregation by designing a Zero-Trust-based MLS model capable of implementing dynamic access control and deriving suitable security controls for its components. Notably, this research holds significant importance, as it integrates the MLS framework announced in the Republic of Korea in September 2024 with the new security paradigm of Zero Trust, offering a developmental direction for future Zero-Trust-based MLS frameworks. The proposed security model serves as a strategic alternative by improving the traditional perimeter-focused network segregation system, enabling the adoption of

new technologies, and enhancing productivity. Simultaneously, it addresses the issue of reduced security levels in the MLS framework by leveraging Zero Trust principles, thereby enhancing both information usability and security.

5.2. Future Works

The future development of a Zero-Trust-based MLS model can focus on the following approaches to enhance its practical applicability and address sophisticated security challenges:

- Enhancing Dynamic Access Control: Developing advanced real-time trust-based dynamic authentication and continuous access validation mechanisms for users and organisational information assets. This ensures both security and data usability while adapting to evolving threats.
- Leveraging Artificial Intelligence and Machine Learning: Supporting automated policy management to create, update, and enforce security policies dynamically. This approach not only improves threat detection and response times, but also aligns with emerging technology trends.
- Strengthening Compatibility with International Standards: Aligning with global standards, such as those from NIST, ITU, and 3GPP, to ensure broader applicability across various industries while enhancing compliance with legal regulations and security frameworks.

In addition to these approaches, future work will focus on implementing the proposed security model in a testbed environment to validate its security effectiveness thoroughly. Efforts will also be made to develop trust evaluation algorithms for detailed dynamic access control and integrate these into the proposed model. These advancements are expected to significantly improve the model's practical relevance and usability in addressing increasingly complex security risks.

Author Contributions: Conceptualisation, J.-H.P., S.-C.P. and H.-Y.Y.; methodology, J.-H.P., S.-C.P. and H.-Y.Y.; validation, J.-H.P., S.-C.P. and H.-Y.Y.; formal analysis, J.-H.P., S.-C.P. and H.-Y.Y.; investigation, J.-H.P., S.-C.P. and H.-Y.Y.; resources, J.-H.P., S.-C.P. and H.-Y.Y.; writing—original draft preparation, J.-H.P., S.-C.P. and H.-Y.Y.; writing—review and editing, J.-H.P., S.-C.P. and H.-Y.Y.; visualisation, J.-H.P., S.-C.P. and H.-Y.Y.; supervision, J.-H.P., S.-C.P. and H.-Y.Y.; project administration, J.-H.P., S.-C.P. and H.-Y.Y.; funding acquisition, H.-Y.Y. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the Institute of Information and Communications Technology Planning and Evaluation (IITP) of Korea grant, funded by the Ministry of Science and ICT of Korea under grant number 2021-0-00112.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data presented in this study are available upon request from the corresponding author.

Acknowledgments: The authors would like to express our sincere gratitude to JaeYeol Jeong (Soonchunhyang University, Republic of Korea) for generously providing invaluable advice and guidance throughout the revision process of this manuscript.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Mehraj, S.; Banday, M.T. Establishing a zero trust strategy in cloud computing environment. In Proceedings of the 2020 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 22–24 January 2020; pp. 1–6.
2. Malatji, M.; Tolah, A. Artificial intelligence (AI) cybersecurity dimensions: A comprehensive framework for understanding adversarial and offensive AI. *AI Ethics* **2024**, 1–28. [CrossRef]
3. National Information Society Agency (NIA). *Public Data Sovereignty Cloud Application Direction for Super-Large AI Utilization in the Public Sector*; National Information Society Agency (NIA): Daegu, Republic of Korea, 2024.
4. Han, B.Y.; Choi, Y.K.; So, G.Y.; Shin, Y.T. A Study on Operation for DevOps Using Zero Trust in Network Separation Environment. *Converg. Secur. J.* **2024**, *24*, 27–34.
5. Rane, J.; Kaya Ömer Mallick, S.K.; Rane, N.L. Influence of digitalization on business and management: A review on artificial intelligence, blockchain, big data analytics, cloud computing, and internet of things. In *Generative Artificial Intelligence in Agriculture, Education, and Business*; Deep Science Publishing: Yakutiye, Turkey, 2024; pp. 1–26. [CrossRef]
6. Yin, H.L.; Fu, Y.; Li, C.L.; Weng, C.X.; Li, B.H.; Gu, J.; Lu, Y.S.; Huang, S.; Chen, Z.B. Experimental quantum secure network with digital signatures and encryption. *Natl. Sci. Rev.* **2023**, *10*, nwac228. [CrossRef] [PubMed]
7. Cao, X.-Y.; Li, B.-H.; Wang, Y.; Fu, Y.; Yin, H.-L.; Chen, Z.-B. Experimental quantum e-commerce. *Sci. Adv.* **2024**, *10*, eadk3258. [CrossRef] [PubMed]
8. Gill, S.S.; Wu, H.; Patros, P.; Ottaviani, C.; Arora, P.; Pujol, V.C.; Haunschild, D.; Parlikad, A.K.; Cetinkaya, O.; Lutfiyya, H.; et al. Modern computing: Vision and challenges. *Telemat. Inform. Rep.* **2024**, *13*, 100116. [CrossRef]
9. Naidoo, R. A multi-level influence model of COVID-19 themed cybercrime. *Eur. J. Inf. Syst.* **2020**, *29*, 306–321. [CrossRef]
10. United States Congress. Federal Information Security Management Act of 2002 (FISMA), 44 U.S.C. § 3541-3549. 2002. Available online: https://www.govinfo.gov (accessed on 20 November 2024).
11. European Union. General Data Protection Regulation (GDPR), Article 9: Processing of Special Categories of Personal Data. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679 (accessed on 21 September 2024).
12. European Union. General Data Protection Regulation (GDPR), Article 32: Security of Processing. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679 (accessed on 21 September 2024).
13. Obi, O.C.; Akagha, O.V.; Dawodu, S.O.; Anyanwu, A.C.; Onwusinkwue, S.; Ahmad, I.A.I. Comprehensive review on cybersecurity: Modern threats and advanced defense strategies. *Comput. Sci. IT Res. J.* **2024**, *5*, 293–310.
14. National Intelligence Service (NIS). National Intelligence Service Announces Major Cybersecurity Policy Directions in "CSK 2024". Available online: https://www.nis.go.kr/CM/1_4/view.do?seq=315 (accessed on 2 September 2024).
15. Stafford, V. *Zero Trust Architecture*; NIST Special Publication 800-207; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2020. Available online: https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-207.pdf (accessed on 2 September 2024).
16. Jabar, T.; Mahinderjit Singh, M. Exploration of mobile device behavior for mitigating advanced persistent threats (APT): A systematic literature review and conceptual framework. *Sensors* **2022**, *22*, 4662. [CrossRef] [PubMed]
17. Singh, S.; Sharma, P.K.; Moon, S.Y.; Moon, D.; Park, J.H. A comprehensive study on APT attacks and countermeasures for future networks and communications: Challenges and solutions. *J. Supercomput.* **2019**, *75*, 4543–4574. [CrossRef]
18. Force, J.T. *Security and Privacy Controls for Information Systems and Organizations*; NIST Special Publication 800-53 Revision 5; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2017. Available online: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf (accessed on 12 September 2024).
19. National Institute of Standards and Technology (NIST). *Standards for Security Categorization of Federal Information and Information Systems (FIPS 199)*; Federal Information Processing Standards Publication 199; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2004. Available online: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf (accessed on 18 September 2024).
20. National Cyber Security Center. Guidelines for National Information Security; Republic of Korea. Revised on 31 January 2023. Available online: https://www.ncsc.go.kr:4018/main/cop/bbs/selectBoardArticle.do?bbsId=InstructionGuide_main&nttId=18588&pageIndex=1#LINK (accessed on 16 December 2024).
21. National Cyber Security Center. *Guidelines for National Cloud Computing Security*; Republic of Korea. Revised on 31 January 2023. Available online: https://www.ncsc.go.kr:4018/main/cop/bbs/selectBoardArticle.do?bbsId=InstructionGuide_main&nttId=18590&pageIndex=1#LINK (accessed on 16 December 2024).
22. United States Congress. E-Government Act of 2002 (Public Law 107-347). Available online: https://www.congress.gov/bill/107th-congress/senate-bill/803 (accessed on 16 December 2024).
23. Ross, R. *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*; Special Publication (NIST SP); National Institute of Standards and Technology: Gaithersburg, MD, USA, 2018. [CrossRef]

24. National Cyber Security Center. Trends in the Promotion of National Cybersecurity Policy. NCSC. Available online: https://www.ncsc.go.kr:4018/main/cop/bbs/selectBoardArticle.do?bbsId=Notification_main&nttId=174371&menuNo=010000&subMenuNo=010300&thirdMenuNo=#LINK (accessed on 19 December 2024).
25. Jericho Forum. Jericho Forum Looks to Bring Network Walls Tumbling Down. Available online: https://www.csoonline.com/article/515503/data-protection-jericho-forum-looks-to-bring-network-walls-tumbling-down.html (accessed on 28 September 2024).
26. Kindervag, J. *Build Security into Your Network's DNA: The Zero Trust Network Architecture*; Forrester Research Inc.: Cambridge, MA, USA, 2010; pp. 1–16. Available online: https://www.actiac.org/system/files/Forrester_zero_trust_DNA.pdf (accessed on 10 September 2024).
27. *NIST SP 800-207*; Zero Trust Architecture. National Institute of Standards and Technology: Gaithersburg, MD, USA, 2020.
28. *NIST SP 800-35 (Initial Public Draft)*; Implementing a Zero Trust Architecture. National Institute of Standards and Technology (NIST): Gaithersburg, MD, USA, 2024.
29. National Institute of Standards and Technology (NIST). *Implementing a Zero Trust Architecture*; NIST Special Publication 1800-35 (Initial Public Draft); National Institute of Standards and Technology: Gaithersburg, MD, USA, 2024. Available online: https://csrc.nist.gov/pubs/sp/1800/35/ipd (accessed on 9 December 2024).
30. National Institute of Standards and Technology (NIST). *Framework for Improving Critical Infrastructure Cybersecurity*; Version 1.1; NIST: Gaithersburg, MD, USA, 2018. [CrossRef]
31. Pascoe, C.E. *The NIST Cybersecurity Framework 2.0*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2024. [CrossRef]
32. National Cyber Security Center. The Direction of ROK's Cybersecurity Policy. Available online: https://cybersummit.kr/eng/p2/c2/?d=2&tab=5&i=22 (accessed on 20 October 2024).
33. Bush, M.; Mashatan, A. From zero to one hundred: Demystifying zero trust and its implications on enterprise people, process, and technology. *Queue* **2022**, *20*, 80–106. [CrossRef]
34. Roy, S.; Phadke, A.C. A Review on Zero Trust—Balancing Security and Usability Needs. *Grenze Int. J. Eng. Technol.* **2023**, *9*, 2622–2629.
35. Shen, Q.; Shen, Y. Endpoint security reinforcement via integrated zero-trust systems: A collaborative approach. *Comput. Secur.* **2024**, *136*, 103537. [CrossRef]
36. Daah, C.; Qureshi, A.; Awan, I.; Konur, S. Enhancing zero trust models in the financial industry through blockchain integration: A proposed framework. *Electronics* **2024**, *13*, 865. [CrossRef]
37. Ministry of Science and ICT (MSIT); Korea Internet & Security Agency (KISA); Korea Zero Trust Forum (KZTF). *Zero Trust Security Guidelines 2.0*; Ministry of Science and ICT; Korea Internet & Security Agency; Korea Zero Trust Forum: Seoul, Republic of Korea, 2024. Available online: https://www.kisa.or.kr/2060204/form?postSeq=18&page=1#fnPostAttachDownload (accessed on 9 December 2024).
38. *ISO 22340:2024*; Security and Resilience—Protective Security—Guidelines for an Enterprise Protective Security Architecture and Framework. International Organization for Standardization (ISO): Geneva, Switzerland, 2024. Available online: https://www.iso.org/standard/85607.html (accessed on 27 September 2024).
39. Cybersecurity and Infrastructure Security Agency (CISA). *Zero Trust Maturity Model*; Version 2.0; CISA: Washington, DC, USA, 2023. Available online: https://www.cisa.gov/zero-trust-maturity-model (accessed on 24 October 2024).
40. Bell, D.E. Looking back at the Bell-La Padula model. In Proceedings of the 21st Annual Computer Security Applications Conference (ACSAC'05), Tucson, AZ, USA, 5–9 December 2005; p. 15.
41. *ISO/IEC 27002:2022*; Information Security, Cybersecurity and Privacy Protection—Information Security Controls. International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC): Geneva, Switzerland, 2022. Available online: https://www.iso.org/standard/75652.html (accessed on 27 September 2024).
42. Bae, Y.S. A study of effect of Information Security Management System [ISMS] certification on organization performance. *J. Korea Acad.-Ind. Coop. Soc.* **2012**, *13*, 4224–4233.
43. Kim, D.H. The Study on Corporate Information Security Governance Model for CEO. *Converg. Secur. J.* **2017**, *17*, 39–44.
44. Lakbabi, A.; Orhanou, G.; Hajji, S.E. Network Access Control Technology-Proposition to contain new security challenges. *arXiv* **2013**, arXiv:1304.0807. [CrossRef]
45. Korean National Police Agency. *Defense Industry Hacking Attacks Revealed*; Korean National Police Agency: Seoul, Republic of Korea, 2024. Available online: https://www.police.go.kr/component/file/ND_fileDownload.do?q_fileSn=157251&q_fileId=785128b4-1d02-43e4-a4ef-a6639437650e (accessed on 1 September 2024).

46. National Security Agency (NSA). *Embracing a Zero Trust Security Model*; National Security Agency: Fort Meade, MD, USA, 2021. Available online: https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.pdf (accessed on 12 September 2024).
47. F5 Labs. *2023 Identity Threat Report: The Unpatchables*; F5 Labs: Seattle, WA, USA, 2023. Available online: https://www.f5.com/content/dam/f5-labs-v2/article/pdfs/F5-LABS-2023-Identity-Report-01NOV23.pdf (accessed on 22 December 2024).

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.