Exploring Effective Zero Trust Architecture for Defense Cybersecurity: A Study

Youngho Kim, Seon-Gyoung Sohn, Kyeong Tae Kim, Hae Sook Jeon, Sang-Min Lee, Yunkyung Lee, and Jeongnyeo Kim*[*]
Cyber Security Research Division,
Electronics and Telecommunications Research Institute,
DAEJEON, KOREA
[e-mail: wtowto@etri.re.kr(Youngho Kim), sgsohn@etri.re.kr(Seon-Gyoung Sohn),
ktkim@etri.re.kr(Kyeong Tae Kim), hsjeon88@etri.re.kr(Hae Sook Jeon),
sangm@etri.re.kr(Sang-Min Lee), neohappy@etri.re.kr(Yunkyung Lee),
jnkim@etri.re.kr(Jeongnyeo Kim)]
[*]Corresponding author: Jeongnyeo Kim

*Received March 23, 2024; revised July 16, 2024; accepted August 21, 2024;
Published September 30, 2024*

Abstract

The philosophy of Zero Trust in cybersecurity lies in the notion that nothing assumes to be trustworthy by default. This drives defense organizations to modernize their cybersecurity architecture through integrating with the zero-trust principles. The enhanced architecture is expected to shift protection strategy from static and perimeter-centric protection to dynamic and proactive measures depending on the logical contexts of users, assets, and infrastructure. Given the domain context of defense environment, we aim three challenge problems to tackle and identify four technical approaches by the security capabilities defined in the Zero Trust Architecture. First approach, dynamic access control manages visibility and accessibility to resources or services with Multi Factor Authentication and Software Defined Perimeter. Logical network separation approach divides networks on a functional basis by using Software Defined Network and Micro-segmentation. Data-driven analysis approach enables machine-aided judgement by utilizing Artificial Intelligence, User and Entity Behavior Analytics. Lastly, Security Awareness approach observes fluid security context of all resources through Continuous Monitoring and Visualization. Based on these approaches, a comprehensive study of modern technologies is presented to materialize the concept that each approach intends to achieve. We expect this study to provide a guidance for defense organizations to take a step on the implementation of their own zero-trust architecture.

Keywords: Access Control, Cybersecurity, Defense, Segmentation, Zero Trust Architecture

This work was supported by the Korea Research Institute for Defense Technology Planning and Advancement (KRIT) - Grant funded by Defense Acquisition Program Administration (DAPA)(KRIT-CT-21-037).

http://doi.org/10.3837/tiis.2024.09.011 **ISSN : 1976-7277**

1. Introduction

Cybersecurity is essential to the operations of critical infrastructures in defense. The rapidly-evolving threat actors make it arduous to protect the critical infrastructure from sophisticated cyber threats around the world. There have been numerous cyber-attacks targeting the military and defense infrastructures. According to a cybersecurity report [1] from the United States (US) Department of Defense (DoD), the department has experienced over 12,000 cyber incidents since 2015 through 2021. For instance, joint cybersecurity advisory revealed that multiple APT groups compromised network of an organization in the defense industry. In the end, the threat actors gained long-term access and conducted malicious activities to steal sensitive information.

As a way of designing a secure network architecture, grouping devices that share same security requirements within a network is a well-known approach to protect against adversarial lateral movement. Therefore, the best design principle would be separating networks for different purposes in an organization in terms of both data access and network connection [2]. The idea of the separated networks allows to isolate traffic with designated security requirements from the traffic under different security conditions. The same principle applies to the design of defense network infrastructures. The **Fig. 1** shows an example of defense networks with three different security requirements. For example, the combat network controls strictly the entire lifecycle of data. The secret data demanding highest caution are produced, distributed, and destroyed internally among certified servers and never leave outside the dedicated network. Accordingly, defense infrastructure requires that security enforcements for strict access control have to be in place all the time.

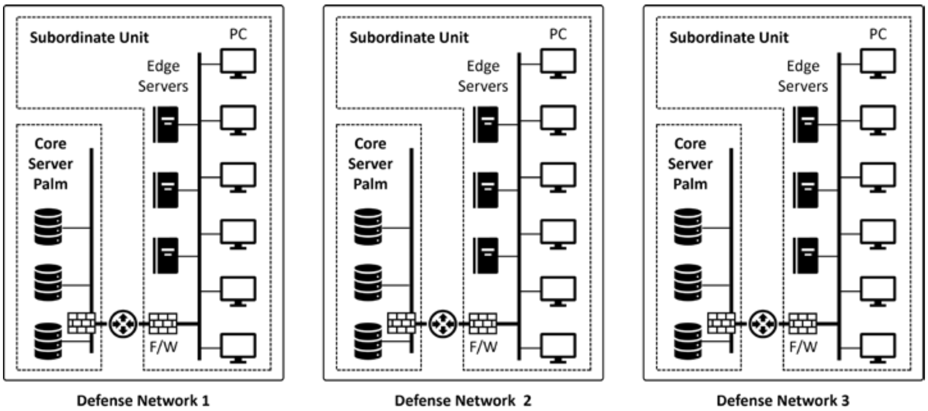


Fig. 1. Example of defense networks with three different security requirements.

Physically separated networks by design helps to improve defense cybersecurity. Meanwhile, the defense cybersecurity is subjected to security threats stemming from the two components: network and asset. Each of the three separated networks in **Fig. 1** forms a closed perimeter of communications. This design presumably allows no links between different networks at all. However, in practice there could be logical connections or sometimes physical connections by user's inadvertent errors. The hackers can exploit the connection links to infiltrate the isolated network that is supposed to be hidden from the outside world. Recent critical infrastructures interact with commercial technologies. This collaboration leads to inevitable connection links with the external network governed by different security policy and enforcement. For example, a private company that builds the military computer network made a temporary connection link for a set-up process and forgot to remove it. Then malicious code through the loophole may infect thousands of computers in the defense network.

Generally, the defense network infrastructure comprises a set of segregated networks with different security requirements. Each network has a specific mission and a designated level of accessibility according to its security policy. However, the defense network has same security challenges as the organization with isolated networks has. First, network separation by design does not necessarily guarantee a screen of blocking all unauthorized access. Inadvertent errors could lead to logical connections and allow attackers to exploit them. Conventional defense network forms a physically closed perimeter and most of security screening processes take place at the perimeter. However, malicious activities exemplified by a Stuxnet worm targeting SCADA systems are able to break into segregated networks and circumvent the perimeter-centric screening process [3]. Second, internal assets constituting the defense infrastructure can be a direct attack surface exposed to malicious activities. Regardless of the gravity of consequences vulnerable assets might incur, the current defense network infrastructures do not sufficiently address the continuous monitoring on the internal assets.

This paper offers a comprehensive study of modern technologies to implement zero-trust principles in the context of defense. The architecture is expected to shift protection strategy from static and network-based perimeters to dynamic border concentrating on dynamic assets, users, and security contexts. The rest of this paper is structured as follows. Section 2 presents principles of zero-trust and identifies target challenges for defense cybersecurity. As a countermeasure, technical capabilities of dynamic access control are discussed in Section 3, and logical network separation techniques are detailed in Section 4. Technical capabilities of data-driven analysis and security awareness techniques are presented in Sections 5 and 6, respectively. Section 7 discusses the challenges and future research directions. Finally, the conclusion is presented in Sections 8.

2. Zero Trust Architecture

2.1 General concept

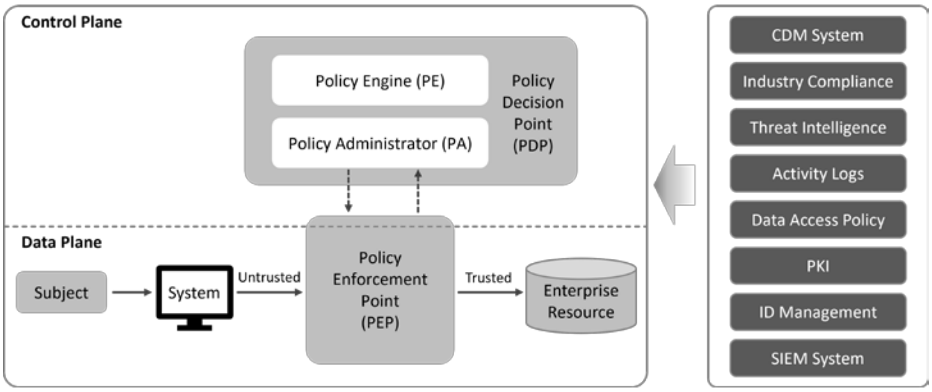


Fig. 2. Conceptual structure of Zero Trust.

According to the MITRE ATT&CK framework [4], recent cyber-attacks are being carried out roughly through initial access, internal network infiltration, and data leakage phases. At first, the attacker utilizes various methods that range from purchasing user accounts of the target company on the dark web to collecting accounts by sending malicious emails disguised as work-related. They also include bypassing additional account authentication procedures such as one-time passwords. After infiltrating the internal network, they keep trying to gain access to the central server that manages multiple accounts and devices to distribute malicious code to obtain additional information. At the final step, the attackers may access the data server where internal confidential data such as employee information are stored to take the information out.

The concept of Zero Trust was first presented by Forester's John Kindervag in 2010 [5]. Since then, independent approaches, implementation, and development plans have been proposed by information security organizations. Emerging attacks that use security threats intelligence tend to evade the static perimeter-based security model. Therefore, it is necessary to strictly restrict access to resources representing data and services from users and devices that do not meet the security policy.

NIST SP 800-207 'Zero Trust Architecture' [6] proposed foundational strategies, operating conditions, and structures to materialize the zero-trust principles. The architecture is expected to improve an existing information protection system by converting a single point gateway-centric screen into multi-point dynamic access control for resources. The conceptual structure shown in **Fig. 2** requires access permissions to be determined by the Policy Engine (PE) through any authentication and authorization process. Based on the determination, the Policy Enforcement Point (PEP) allows the requesting subject to access the resource. The Policy Administrator (PA) keeps monitoring the user's behavior and immediately blocks any access to the resource if an abnormality is identified.

2.2 Defense Cybersecurity

The importance of the cybersecurity modernization through the zero-trust architecture applies to the defense cybersecurity. The DoD provides the Cybersecurity Reference Architecture [7] to advance its cybersecurity systems. The reference architecture aims to mitigate the threats that exist both inside and outside traditional network boundaries. The operational activities of the architecture shown in **Fig. 3** are drawn from the existing frameworks such as zero-trust architecture, the MITRE ATT&CK Framework [4], and the MITRE D3FEND [8]. The arrows stemming from the user and device pillar allow workload or data in data plane to be screened at the enforcement point. Other two pillars in the right hand make up a control plane to develop confidence levels of the user and device pillars in the data plane and automate the response process.

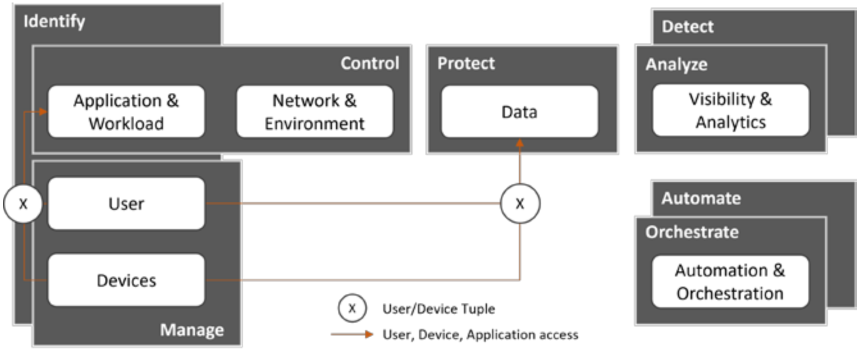


Fig. 3. Operational activities of cybersecurity reference architecture.

The enhanced cybersecurity model in defense eliminates the traditional idea of presumably trusted or untrusted networks. Instead, dynamic confidence levels from continuous verification determine authentication and authorization policies for access to resources. Based on this security model, the DoD also provided a zero-trust reference architecture [9] and zero-trust strategy [10]. They aim for a resilient framework protecting the defense infrastructure from malicious cyber activities. In addition to the major five pillars in the conventional zero-trust architecture, Automation and Orchestration pillar are emphasized to automate security responses in accordance with enforcement policy. Also, the Visibility and Analytics pillar stresses an ability of making dynamic changes to security policy from other pillars' behavior. All seven zero-trust pillars shown in **Fig. 3** provide the basis for the defense security model to implement its zero-trust principles.

2.3 Target Challenges

The U.S. Cyber Command published Command Challenge Problems Set Guidance [11] to address its cybersecurity problems, which are organized into six categories. First of all, challenge problems in vulnerabilities and exploits category include recognizing exploitable vulnerabilities and generating defensive patches rapidly against them. Challenge problems in network security, monitoring, and visualization category tackles the node-to-node interactions to defend the perimeter and the interior of the network. And modeling and predictive analytics category seeks solutions to the challenge problems which include automated anomaly detection, automated threat discovery. Challenge problems in persona and identity category cover the offensive activities involving people and cyber actors. The category of permeability and agility across domains address the challenge problems in sharing and collaboration with external partners. Finally, challenge problems in infrastructure and transport category feature risks in large-scale data collection, storage, and transport.

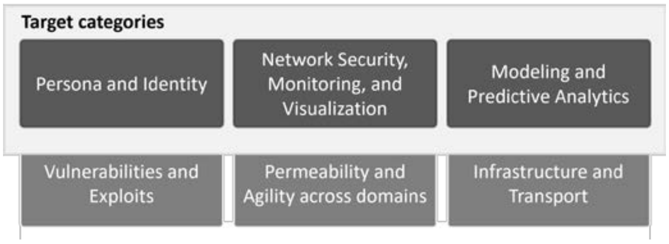

Target categories
Persona and Identity
Network Security, Monitoring, and Visualization
Modeling and Predictive Analytics
Vulnerabilities and Exploits
Permeability and Agility across domains
Infrastructure and Transport

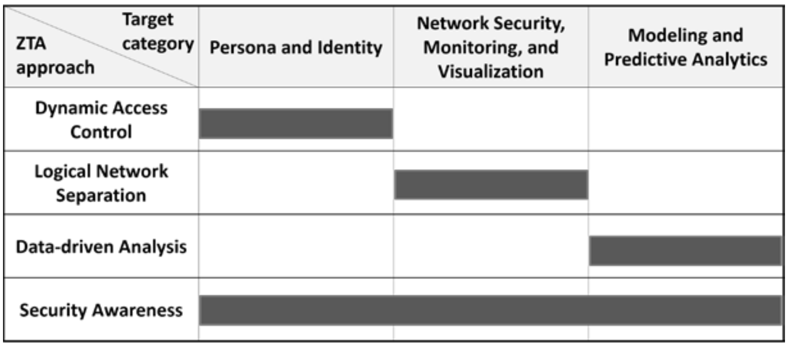
Fig. 4. Target categories from the Command Challenge Problem Set.

Zero-trust architecture (ZTA) alone is not enough to address all challenge problems of the six categories mentioned. The first step is to select target challenges in defense domain in **Fig. 4** for ZTA to effectively tackle. And this article aims to offer technical capabilities of ZTA as applicable solutions to the target challenges. After a thorough investigation of the major capabilities in the DoD's zero-trust reference architecture and strategy, we have come to the following justifications to investigate technical approaches in **Fig. 5**.

- Identity fabrication and credential misuse are primary challenge problems in person and identity category. To tackle the problems, the boundaries of all resources need to be separated and protected under appropriate authentication and authorization. Dynamic access control approach places a strong emphasis on safeguarding important data and resources. It involves the use of identity feature to protect, restrict and enforces access to data. Also, dynamic access control with continuous authentication and authorization allows to defend against the offensive activities in persona and identity category.
- Challenge problems in network security, monitoring, and visualization category involve mapping of network topology to defend both the perimeter and the interior of

the network. Meanwhile, traditional perimeter-centric security measures can no longer provide effective protection against sophisticated attacks. In the circumstances, logical network separation approach is expected to improve the ability to detect and prevent lateral movement.

- Data-driven analysis approach uses modeling and predictive analytics to characterize adversary behavior. In particular, behavior analytics is crucial for identifying insider threats, which can be particularly challenging to detect. By monitoring user and entity behavior patterns, organizations can spot anomalies that may indicate malicious actions or compromised accounts among trusted users.
- Security awareness approach keeps minimal privileges on all resources, assuming that every access is a potential security threat. Every access attempt to a resource must be validated, which requires continuous monitoring of all resources. In this regard, security awareness helps to maintain overall security posture that addresses problems in the target categories. However, huge amount of data produced everyday makes it difficult for security analysts to comprehend situations and make prompt response to cyber-attacks. With individual piece of information together, security awareness allows to get in-depth insight to actively defend against potential security threats.



Target category / ZTA approach	Persona and Identity	Network Security, Monitoring, and Visualization	Modeling and Predictive Analytics
Dynamic Access Control	■		
Logical Network Separation		■	
Data-driven Analysis			■
Security Awareness	■	■	■

Fig. 5. Technical approaches applicable to target categories.

3. Dynamic Access Control

3.1 Multi-Factor Authentication

An individual in a defense organization may possess multiple personas demanding different privileges to access data. This fact leaves the problem of how the right user gets access to the determined data with appropriate credentials. PKI has been DoD's primary authentication technology. In reality, not all users in the department and applications can use PKI certificates. DoD systems accept a wide range of credentials including passwords, biometrics, one-time passwords, and other authenticators. Multi-factor Authentication (MFA) of DoD provides a combination of authenticators that provide different factors in a risk managed framework [12].

Two-Factor Authentication (2FA) is a security mechanism used to provide an additional layer of protection against online cyber threats. The concept of 2FA involves two main aspects: the first is entering a password to access an account and perform online transactions and the second is utilizing user authentication layers like one-time password (OTP) or security tokens.

Bhanderi et al. [13] examined various use cases of 2FA authentication methods, comparing security and usability. In this study, users expressed high satisfaction with one-time PINs (OTP) received via email or SMS, while there was a critical response to security token usage. PKI was observed as a low user satisfaction and problematic solution.

Saleem and Shoshan [14] proposed a multi-factor authentication system that combines user-friendliness and cost-effectiveness. In this approach, during the registration phase, users select and memorize three images. During the login phase, they simply choose the images in the correct order as a means of authentication.

Conventional authentication methods are vulnerable as they lack the ability to continuously monitor and verify a user's identity, allowing for malicious or unintentional usage of computer systems while the user logged in. To enhance the authentication process, there is a need for methods that can continuously verify a user's identity. Continuous User Authentication (CUA) has proven to be a solution to address these limitations. CUA involves capturing unique behavioral patterns that represent a user group's usage footprint from web server log files and integrating then into an n-gram model. As users interact with web-based software, their stored profiles are compared to their current behavior, and any deviations that are deemed indicative of malicious activity trigger alerts to report the issues.

The Federal Identity, Credential and Access Management (FICAM) architecture [12], [15] describes a set of security practices that help organizations ensure that the right individuals or entities have access to the appropriate resources at the correct time and for valid reasons. FICAM outlines three core functions: identity management, credential management and access management. Identity management involves creating digital profiles based on defining characteristics of an entity. Credential management links digital identities with authoritative credentials. Access management uses trusted identities and privileged credentials to grant access to authorized entities, which can be people (human entities) or non-person entities (NPEs). As for assurance level, NIST SP 800-63A [16] introduces three identity assurance levels (IAL) for personal entities to verify their identities. NIST SP 800-63B [17] defines three Authenticator Assurance Levels (AAL) for authentication information. AAL1 is a single factor authentication like a username and password. AAL2 is a multi-factor authentication, which includes a username and password to be one element. AAL2 also includes software certificates issued by PKI. AAL3 requires a cryptographic authenticator with a private key stored in a hardware token. The choice of AAL for authentication depends on the sensitivity level of the protected resources being accessed. Username and password authentication necessitate separate passwords for different systems, making password management complex and considered unsafe due to potential hacking.

3.2 Software Defined Perimeter (SDP)

As with the aforementioned SCADA systems, network segregation in the defense intends to improve the cybersecurity by design. However, that does not necessarily guarantee blocking all unauthorized access. For example, South Korea's Defense Data Center was infiltrated by North Korean hackers and classified military documents were stolen in September 2016 [18]. Despite its isolated network and perimeter-based firewalls, a temporary network link to the military intranet for maintenance work led to infiltration and internal infections into the military network.

According to the DoD's Cybersecurity reference architecture [7], cyber resilience is essential to enabling the system to respond to and recover from cyber events. A more specific principle in the document states that control over authorized data flows and preventing rogue connection help increase the cyber resilience. As integral parts of cyber resiliency engineering framework, NIST recommends privilege restriction and realignment for effective authorization techniques. Specifically, the former takes into account attributes of user and system elements to regulate privileges. The latter organizes systems and resource usages to fit mission or functional needs, and keeps down the links between mission-critical and non-critical services [19]. The **Fig. 6** shows an example of attribute-based access control accomplishing the privilege restriction and realignment techniques.

Among the efforts, Cloud Security Alliance (CSA) devised Software-Defined Perimeter (SDP) to address dynamically changing security situation and rapidly evolving attacks, against which traditional perimeter-based defense approaches are ineffective. SDP hides network resources from unauthorized users and only allows for restricted access to those resources to perform predetermined mission even if the access is authorized. This restricted access model verifies and authenticates the identity of devices or applications before granting access to the services provided by infrastructure. Inherently, the infrastructure remains in 'black' state, making it invisible to unauthorized requestor. This 'Deny by default' principle in SDP helps to mitigate various network-based attacks that include port scanning, spoofing, denial-of-service, and man-in-the-middle attacks. Implementing the principle of least privilege, SDP in the defense reduces the attack surfaces significantly and makes its security architecture more resilient to cyber-attacks. Academic efforts have been made to fuse SDP and existing network security.

Sallam et al. [20] proposed an integration of SDN and SDP to address problems ranging from controller replication to policy conflict and authentication method issues. The framework shows promising results from DDoS and Port Scanning attacks while maintaining 75% of network throughput. Similarly, Moubayed et al. [21] proposed an SDP-based framework which adopts the client-gateway structure of SDP and tests it against DDoS attacks and port scanning attacks. The SDP security network has shown resilience against DDoS attacks and port scanning, maintaining high average network throughput even though it takes longer during the initial connection.

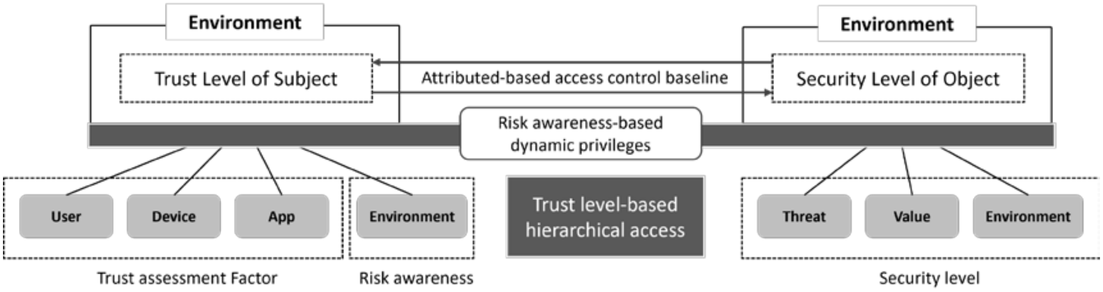


Fig. 6. Access control model.

SDP limits security risks isolating user access based on user accounts, policy and resources. Kumar et al. [22] presented a Monte Carlo simulation to determine SDP risks in collaboration with domain experts to evaluate various SDP configurations using a competitive co-evolution framework. The simulations in their work tested the strength of various SDP configurations against multiple types of attackers.

Finally, Omar and Abdelaziz [23] compared network access control (NAC) solutions and SDP for the most suitable solution. The approach shows how SDP can improve NAC and overcome security issues. SDP only allows authenticated connections relying on four elements: SDP controller, Single Packet Authorization (SPA) protocol, Mutual Transport Layer Security (mTLS) and dynamic firewalls. No packet can pass through the dynamic firewall until there is an access permission granted from the SDP controller. SDP presents advantages in improving security compared to the conventional NAC. First, SDP can authenticate users before the necessary services are exposed outside. Second, SDP encrypts the channel delivering data from the user's device to the service while NAC needs extra appliances for data encryption. Lastly, SDP dynamically determines the access rights by examining the current status of requesting user or device.

4. Logical Network Separation

4.1 Software Defined Network (SDN)

Software-Defined Networking (SDN) is a conceptual framework that involves the separation of the control plane and the data plane. While SDN is commonly associated with a close relationship with OpenFlow, it is not confined solely to OpenFlow as its underlying technology. SDN represents a more comprehensive concept, encapsulating network architecture or a new paradigm. OpenFlow, on the other hand, serves as one of the interface technologies for SDN. **Fig. 7** depicts the fundamental structure of Software-Defined Networking (SDN).

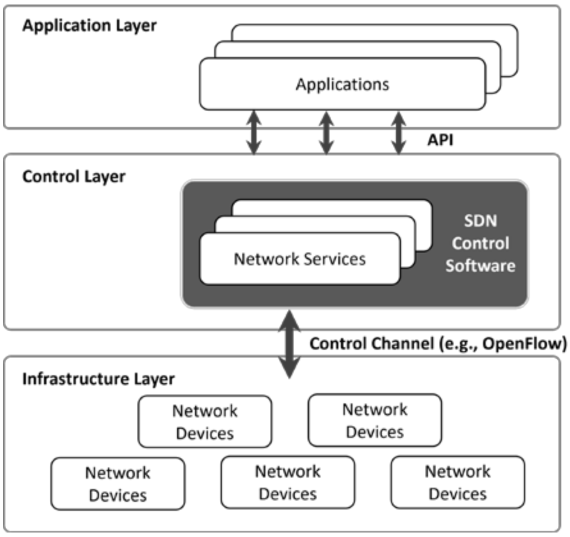


Fig. 7. Fundamental structure of SDN.

In this framework, network intelligence is centralized within the SDN controller, enabling comprehensive network management, where the entire network is viewed as a unified logical switch. This centralized control empowers administrators to manage the entire network through standardized interfaces, reducing their reliance on specific vendors and simplifying network design and operation. Furthermore, one of the advantages of SDN is that network devices can be simplified because they only need to perform the role of forwarding packets according to the controller's configuration. This advantage is highly suitable for environments that demand a large number of network devices [24], [25], [26].

The Ministry of National Defense of Korea has introduced SDN as part of establishing a cloud environment within the Defense Integrated Data Center (DIDC) [27]. In data centers, a scale-out architecture is necessary to efficiently utilize network resources according to fluctuations in demand. Constructing such an architecture poses challenges, notably due to the compatibility issues arising from diverse operating systems among network vendors. The widespread adoption of SDN is a common solution to overcome these difficulties. However, introducing SDN into a defense network environment is considered to hold a new significance. It is believed that SDN, by efficiently managing and advancing the intelligence level in the physical switch domain, will become an essential element for the DIDC, contributing to an efficient network architecture in the DIDC's network environment.

The Defense Information Systems Agency (DISA), responsible for IT services in the U.S. Department of Defense (DoD), is making efforts to adopt SDN [28]. They believe that utilizing SDN is advantageous for the DoD components and combat commands to deploy networks, provide services, and ensure the stability of the network. When a network attack occurs, it is believed that SDN has the advantage of quickly addressing security issues. Despite the advantages of SDN in terms of network security, it is acknowledged that the SDN controller becomes a primary target for attackers. Additionally, as the controller plays a crucial role and changes are typically have an impact across the entire network, ensuring that applications are authenticated, connections are securely encrypted, and security policies are correctly applied is important.

SDN presents advantages in enhancing security compared to traditional networks, yet it also introduces new vulnerabilities and threats. This explains the attack surfaces and threats that can arise at each layer and interface of SDN. In the context of SDN, there have been numerous efforts to categorize attacks based on the attack surface. Nevertheless, each of these attempts defines attacks on the attack surface slightly differently. In this paper, we would like to explain the attack using four attack surfaces as a framework: the application layer, the control layer, the control channel, and the infrastructure layer. All attack surfaces possess its own vulnerabilities and threats that can be targeted by various threats. And, specific vulnerabilities may compromise network components within their respective layers or target elements of other layers. Therefore, it is not straightforward to clearly distinguish specific attacks based on the attack surface.

The application layer is where applications defining network behavior and policies are located. Applications with excessive privileges can terminate other applications or APIs, potentially leading to security vulnerabilities. And malicious applications can negatively impact the performance of applications and controllers by consuming critical system resources like memory and CPU. Additionally, these malicious SDN applications can interfere with the execution of applications and controllers. Misconfigurations in applications or APIs can also potentially lead to a security vulnerability by allowing the modification of information within the controller. Lastly, the false flow rules inserted by malicious or compromised applications can disrupt the operation of SDN [29], [30], [31], [32].

The control layer is the layer where the network controller resides, responsible for network intelligence and control, directly managing network devices. Malicious applications or switches can create new rules that conflict with the existing ones, bypassing established security policies or firewall regulations. To evade flow rule, compromised applications can transmit false information to the controller, allowing them to manipulate network information. This manipulation leads to incorrect rule, resulting in network disconnections. As an unauthorized controller access, the compromised applications can access and modify controller’s internal data, such as network policies, switch tables, and system commands, without authorization. Ultimately, it can lead to information leakage, policy violations, or even the shutdown of the controller [29], [30], [31], [32], [33].

The control channel is the communication interface between the controller and switches, primarily facilitating the exchange of configuration requests from switches and configuration information from the controller. Control channels with insufficient encryption can be vulnerable to eavesdropping, potentially leading to unauthorized packet sniffing and the theft of network information. ARP Spoofing involves intercepting ARP requests to falsify ARP tables. This manipulation acts as a gateway for executing Man-in-the-Middle (MITM) attacks, allowing the attacker to intercept network packets, steal sensitive information, and eavesdrop on communication channels [29], [30], [31], [32], [33], [34].

The infrastructure layer is the layer responsible for forwarding packets using network devices such as switches. Compromised controllers or switches can generate a large number of packet-in messages, which can disrupt normal access to the controllers. Also, compromised controllers or switches can flood the controller with fabricated feature-response messages, populating switch's rule with fake entries. As a result, this adversely affects the controller's performance. Control Packet Injection involves attackers sending forged control packets to the controller or switches, thereby exploiting vulnerabilities or inducing errors that can impact the operation of the devices. As a last type of attack, Side-Channel Attack leverages information exposed by the physical implementation or operational behavior of a system. In this attack, data related to the operation of switches, packet processing, and controller response times is gathered through side-channels and used for malicious purposes [30], [31], [32], [33], [35]. **Table 1** is s a brief summary of attacks and solutions for addressing the attack surface SDN [33], [35], [36].

Table 1. Brief summary of attacks and solutions for addressing the attack surface SDN

Attack surface	Attacks	Solutions
Application layer	Excessive Privileges Malicious Application Misconfiguration Fake Flow Rule Insertion	The application layer should establish a trusted network connection and perform identity authentication for each network component. Also, the confidentiality of the network connection should also be maintained.
Control layer	Flow Rule Tunneling Flow Rule Modification/Evasion Unauthorized Controller Access	Ensuring service continuity is of paramount importance because controller disruption affects the entire network. Furthermore, it is crucial to maintain the confidentiality and integrity of the controller configuration. Using inaccurate information for network configuration by the controller can result in numerous issues. Therefore, it is essential to provide accurate network information, and to do so, maintaining the confidentiality of network topology information is of paramount importance.
Control channel	Eavesdropping ARP Spoofing/Man-in-the-Middle	Considering that the control channel handles communication between the controller and various network devices, it encompasses sensitive network data and critical control decisions. Therefore, the control channel must maintain confidentiality and integrity. Also, the connection between the controller and the device should always be available.
Infrastructure layer	Packet-in Flooding Flow Rule Flooding Control Packet Injection Side-Channel Attacks	Securing the control channel is of utmost importance. Additionally, it is crucial to preserve the confidentiality of the flow tables entries which represent network control policies.

4.2 Micro-segmentation

Micro-segmentation is the concept that protects resources by breaking a network infrastructure into smaller logical segments shown in **Fig. 8** to prevent lateral movement by attackers [37]. In this section, we introduce several approaches that have attempted to achieve micro-segmentation for zero-trust principles.

Tactical military networks combine multiple devices, communication methods, and technologies to perform surveillance, reconnaissance, and tactical missions. Interoperability and security are crucial for sharing information between allies in these networks. To achieve this, resources must be segmented to minimize the attack surface and protect infrastructure from malicious activity [38].

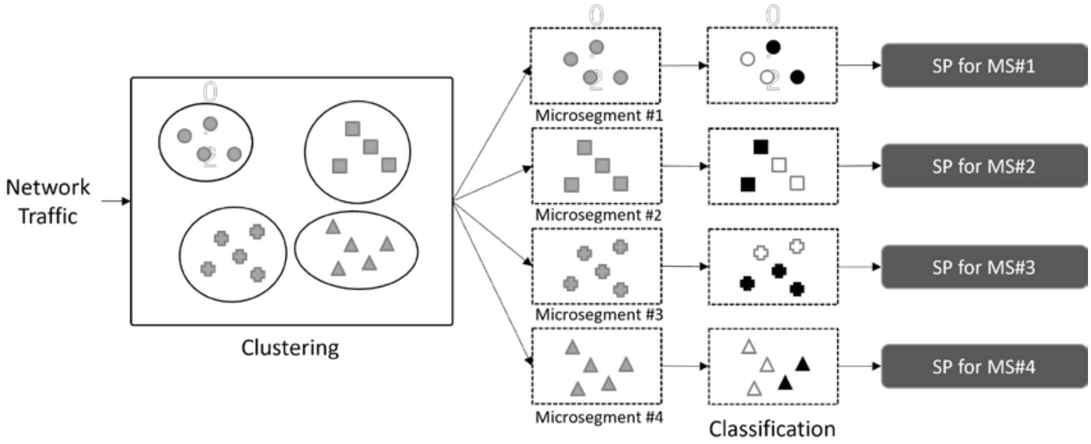


Fig. 8. Micro-segmentation creation procedures.

Enabling the interconnection of separate and disparate services (Army, Navy, and Air Force) is necessary to achieve the U.S. Department of Defense's Joint Area Command and Control (JADC2) strategy. JADC2 connects the sensors of all military services into one network to simplify the planning, execution, and sustainment of military operations in the land, air, sea, cyber, and space domains. The network solution for battlefield must guarantee minimum network performance and provide resiliency to abrupt and unexpected changes which may occur in network topology during combat. Therefore, it is necessary to build the battlefield network on an architecture that has strong isolation or segmentation between network functions or services [39].

The Cybersecurity and Infrastructure Security Agency (CISA) leads the efforts to manage and reduce threats to the nation's critical cyber and physical infrastructure. They aim to strengthen collaboration with government and private sector organizations. Recently, CISA published an infographic titled 'Layering Network Security Through Segmentation' to assist in strengthening networks against cyber threats [40].

Chen et al. [41] proposed a multi-dimensional security framework using the zero-trust architecture that deals with subject, object, environment, and contexts of a 5G medical system. Based on this framework, the authors presented a security-aware protection system and discussed the security enhancements. The achievement covers virtualized network, data collaboration, IoT environment, and integrated 5G network security to meet the security requirements of 5G medical applications. The authors in the paper utilize micro-segmentation approaches that are relevant to virtualized components, including virtual machines, containers, and microservices. It allows data interactions between authorized systems and connections, which are continuously maintained by the fine-grained access policies in the fluid environment. And this system utilizes micro-segmentation technologies to attain separation of the network environment, interdomain segmentation, and end-to-end segmentation.

Arifeen et al. [42] proposed an automated micro-segmentation model by utilizing machine learning algorithms to lessen the lateral movement of malicious activities by an attacker. This model generates the micro-segments depending on network traffic and screens the malicious traffic at the entrance of each segment. The process of creating the logical segments using machine learning algorithms is a two-step process. First, devices with similar functionalities or behavior are grouped into a micro-segment. And then policy for traffic classification will be determined on the basis of the segment. Separating the normal traffic based on the micro-segment is effective in blocking malicious traffic, according to their experiment.

Sheikh et al. [43] presented a network security architecture that supports the zero-trust, based on a concept that monitors network traffic using packet header information to allow authorized communication. They used Illumio, a network micro-segmentation tool, to materialize the zero-trust principles at the network layer. Illumio writes policies to a white list traffic between the source and the destination. These policies can be used to segregate the enterprise network into micro-segments to control the traffic between the source and the destination.

Xie et al. [44] proposed a zero-trust protection approach based on network micro-segmentation, security gateway, and device context perception. The security gateway module is used to authenticate and authorize access to the south-to-north traffic. The micro-segmentation module is used to perform adaptive network traffic control for east-west traffic. The security environment awareness module is used to check the security of the network access device in real time. The micro-segmentation protection system built on the zero-trust architecture includes three functions. First, adaptive micro-segmentation protection function provides an isolation between the internal host network layer and the business layer. Credit network access and access control function focus on the user permission to realize application-level security access. Finally, equipment environment perception function addresses the user identity and senses the device security environment from multiple dimensions.

The solution by Rocha et al. [45] addresses the implementation of a zero-trust security model to thwart APT attacks on LAN environment. To develop the security model, the authors micro-segmented the LAN network into two VLANs. Then they applied the Next-Generation Firewalls (NGFW) to implement micro-segmentation. The segment is equipped with its own security policy. Their experimental results show that maintain discrete network policies for different micro-segment can prevent unauthorized access to network resources. However, this is too complex to automate the whole process.

Hakiri et al. [46] presented the SECurity and Resiliency Techniques for Differentiated 5G OPerationS (SECRETED 5G OPS), which aims to protect differentiated operations in the 5G network. To this end, the project defines and executes verification tasks for real-time industrial systems. This fine-grained cybersecurity allows an efficient and continuous security verification in 5G networks. Micro-segmentation technically demands managing and supervising resource allocation and security operations for channels between endpoints. This project addressed the need to define network segmentation that allows the real-time monitoring for the zero-trust implementation.

Ma et al. [47] proposed an idea which automatically generates policies for micro-segmented network in cloud environments. The objective of the paper is to find the possibility of merging static analysis with dynamic learning methods to automate the process of microsegmenting network, which can diminish the cost of policy deployment as well as make it compatible with different application scenarios. The framework is divided into an application plane, control plane, and data plane. In particular, the application plane is used to apply a micro-segmentation concept. And then the control plane deploys access control policies, and the data plane collects statistics such as IP flow to recognize networks. The authors focus on the accurate classification of behavior-aware groups for micro service applications. According to this policy model, policies are automatically generated using a higher-level declarative language in accordance with data plane interface requirements.

Micro-segmentation can be implemented in different ways within the context of organization. Application segmentation aims to protect high-value applications that perform critical functions by controlling east-west traffic between applications. User segmentation is a way to provide limited application visibility to specific groups of users by granting them limited access. Process-based segmentation builds a perimeter around each process or service level to create a single segment, which aims to achieve a higher level of granularity and reduce the attack surface to a much smaller area. Tier-level segmentation is separating applications that comprise multiple tiers such as web servers to isolate each application tier from the others and prevent unauthorized movement between tiers. Finally, environment segmentation aims to separate environments such as development, test, and production to prevent communication between them. **Table 2** shows types of micro-segmentation and approaches.

Table 2. Types of micro-segmentation and approaches

Approach	**Type of micro-segmentation**	**Reference**
A protection method in 5G-based healthcare platforms leveraging security awareness and zero-trust architecture	Application Segmentation	Chen et al. [41]
A malware mitigation method leveraging automated network micro-segmentation and machine learning algorithms	Application Segmentation	Arifeen et al. [42]
A network security architecture based on the concept of analyzing packet information in network traffic for authorized communication	Tier-Level Segmentation	Sheikh et al. [43]
A protection method leveraging security gateway, and network micro-segmentation, and device environment perception	User Segmentation	Xie et al. [44]
A security model using micro-segmentation and NGFW concepts to prevent APT attacks on LAN networks	Process-Based Segmentation	Rocha et al. [45]
A network slicing solution for secure and differentiated operations in 5G networks	Application Segmentation Tier-Level Segmentation	Hakiri et al. [46]
Solution to generate network segmentation policies for cloud environments	Application Segmentation	Ma et al. [47]

5. Data-driven Analysis

5.1 Artificial Intelligence

In the framework of zero-trust architecture, leveraging Artificial Intelligence (AI) for cyber defense is crucial because it allows for continuous monitoring of user behavior, device security, and network transactions. Fundamentally, zero-trust security operates on the principle that neither users nor devices should automatically be deemed safe, with AI playing a key role in perpetually verifying identities and analyzing threats to uphold this standard [7], [9], [10]. AI is particularly adept at quickly analyzing large datasets, which is essential for identifying potential security issues. It not only helps in recognizing established threats but also in spotting new, unusual patterns that could indicate emerging dangers. Thus, AI in zero-trust architect is pivotal in developing sophisticated cyber defense strategies through its data-driven analysis capabilities.

Kaasen et al. [48] investigated the necessity of developing an autonomous cyber defense system for military unmanned vehicles, highlighting the critical need to address the safety risks posed by cyber-attacks on these assets. The study examines the case of a military unmanned ground vehicle compromised by an insider threat, analyzing the data generated from this incident to create a robust detection mechanism.

Unicorn [49] introduced a framework that builds upon traditional signature-based detection systems by identifying anomalies in cybersecurity data. It evaluates various statistical and machine learning techniques to establish a link between the behavior of devices and their expected operational state. The study singles out the Quantile Regression Forests method as the most effective for predictive accuracy. Utilizing this method, it proposes an anomaly detection system that marks behaviors deviating from expected prediction intervals as unusual. Through the analysis of historical incidents and the progression of threats, AI is positioned to forecast potential future attacks, enabling organizations to adopt a proactive defense stance.

Shen et al. [50] proposed Recurrent Neural Networks (RNNs) and deep learning algorithms to predict security events based on historical data. The significance of this research lies in its ability for defenders to not only detect malicious activities but also predict an attacker's future actions. Moving beyond the binary outcomes of previous research, the approach uses RNNs for predicting future events, underlining the stability of these models over time and introducing a method to recalibrate the system upon detecting a drop in accuracy. The importance of the long-term memory features of RNNs in forecasting events is highlighted, showcasing their superiority over simpler forecasting methods.

Naseri et al. [51] explored the role of Federated Learning (FL) in anticipating cyber-attack events. It introduces Cerberus, a collaborative platform for training RNN models across various organizations, assessing its performance in terms of utility, stability, confidentiality, and mutual benefits. The paper sheds light on the advantages and obstacles of employing FL for security incident prediction, providing valuable perspectives on its application in predictive security efforts.

Li et al. [52] underlined the criticality of network security in smart city contexts and suggests an innovative method for forecasting network security situations. This method features feature separation and a dual attention mechanism, advocating for the use of RNNs to chronologically model intrusion events. The introduced feature separation technique distinctively processes categorical and numerical data, using word embeddings for the former, thereby maintaining feature consistency, addressing overfitting, and lowering training expenses.

Brown et al. [53] investigated the development of interpretable deep learning models for anomaly detection in system logs. The objective is to merge deep learning's robust capabilities with interpretability. A novel method integrating attention mechanisms into RNN language models is proposed, aimed at detecting anomalies in system logs while elucidating the model's reasoning without compromising performance. The research is dedicated to applying these models for intrusion detection, utilizing the Los Alamos National Laboratory (LANL) cybersecurity dataset.

5.2 User & Entity Behavior Analytics (UEBA)

In the realm of zero-trust architecture, behavior analytics becomes a key element in offering a sophisticated, proactive approach to threat identification and neutralization. This approach leverages a detailed inspection of user actions and system behaviors, enabling organizations to reinforce their defensive frameworks and secure essential resources [7], [9], [10].

Traditional security tools that rely on static correlation rules struggle to detect when seemingly authorized actions have malicious intent [54], [55]. To address these limitations, cyber security solutions have shifted towards machine learning. UEBA leverages extensive operational and security log data, enriched with additional context, to identify malicious activities. For example, an attacker with legitimate access to a network begins to exhibit unusual behavior, such as accessing large volumes of sensitive data they typically do not interact with, or attempting to access restricted areas of the network.

UEBA enhances security by using statistical analysis to detect anomalies, deriving contextual information to assess risks accurately, and employing meta-learning to adjust risk scores and minimize false positives. For anomaly detection, UEBA employs unsupervised learning to create profiles of typical user behavior, generating alerts for deviations that might indicate insider threats. It uses statistical analysis to spot these anomalies by comparing unusual low-probability events against established norms.

Salitin et al. [54] examined three primary threat detection methods: Signature-Based Detection, Anomaly-Based Detection, and Continuous System Health Monitoring. Signature-Based Detection identifies threats by comparing network traffic to a database of known signatures. Anomaly-Based Detection spots malicious activity by comparing current behaviors against established normal patterns. The study also evaluates various UEBA vendors to determine the effectiveness of behavior analytics in detecting real-time network attacks, with a particular focus on identifying zero-day threats.

Skopik et al. [56] presented AECID, an anomaly detection method specifically designed for monitoring unstructured textual event data in cyber-physical systems, setting it apart from traditional behavior-based anomaly detection methods. It utilizes machine learning for sequence and correlation analysis, enhancing the detection of unauthorized access or suspicious activities in real-time, thereby improving the security of physical access control systems.

Kaur et al. [57] proposed a technique for identifying unusual behavior and classifying users based on their activity patterns. The paper highlights UEBA within cloud environments, stressing the importance of comprehending user behavior and identifying anomalies to enhance security. It underscores the critical role of visibility and detection in cloud settings to mitigate security issues, demonstrating the essential function of UEBA in this context.

Data science enhances UEBA by deriving contextual information, such as user attributes and properties, to assess the risk of anomalies accurately. Yamauchi et al. [58] focused on establishing typical user behavior patterns to identify deviations that signal security threats. This involves analyzing daily activity patterns to detect anomalies. Different machine learning models improve anomaly detection by learning from historical data and identifying real-time irregularities. It includes contextual information such as device usage timing and nature, enhances the precision of anomaly detection systems.

Sugumaran et al. [59] emphasized the role of AI and neural networks in enhancing cybersecurity, particularly in detecting intrusions, identifying malware, and analyzing vulnerabilities. These advancements in AI scrutinize network traffic and software behavior to identify vulnerabilities and malicious actions. Neural network models further enhance detection capabilities by studying patterns of legitimate users, established malware, and known vulnerabilities, thus identifying irregularities and emerging threats.

Shashanka et al. [60] demonstrated how UEBA can enhance the detection and response capabilities of enterprise security systems. Through behavioral profiling, real-time monitoring, and integration with existing systems, UEBA provides a robust framework for identifying and mitigating potential security threats. The research utilizes Singular Value Decomposition (SVD), to detect anomalous behaviors among users, IP addresses, and devices within an enterprise. It highlights the critical role of behavior tracking and monitoring in identifying malicious activities and offers security analysts valuable contextual information for comprehensive investigations.

To reduce false positives, UEBA employs meta-learning, adjusting risk scores based on historical data and frequency of alerts. Zoppi et al. [61] investigated the application of meta-learning techniques to improve unsupervised intrusion detection in Cyber-Physical Systems (CPSs). It emphasizes the significance of AI and ML algorithms in enhancing CPS functionalities while addressing the challenge of misclassification. It supports using meta-learners, which combine multiple base-learners to decrease errors and improve the detection of both familiar and new threats, including zero-day attacks.

Savenkov et al. [62] aimed to develop mathematical and programmatic methods for identifying unusual user behavior by analyzing behavioral biometric traits. It addresses the challenges of extracting valuable information from unstructured data in UEBA systems by proposing the use of machine learning methods for analysis, particularly the k-nearest neighbors (KNN) method, to identify deviations in user behavior and notify administrators of potential security threats.

Zero trust security requires that all users and entities be authenticated, authorized, and validated before accessing applications and data, with continuous re-authentication, re-authorization, and re-validation throughout their session. This architecture necessitates comprehensive visibility into all users, devices, assets, and entities within the network. UEBA provides security analysts with detailed, real-time insights into activities such as device connection attempts and privilege escalation efforts.

Integrating UEBA with Zero Trust principles allows policies to trigger additional authentication or restrict access based on detected anomalies. Automated systems can alert security teams with detailed insights into suspicious activities, minimizing false positives and prioritizing significant threats. Over time, tracking minor alerts can reveal developing threats, ensuring comprehensive threat management.

By focusing on abnormal activities instead of predefined patterns, UEBA effectively addresses key security threats like compromised credentials and privileged-user compromise. Leveraging UEBA insights in Zero Trust environments enhances the ability to detect and respond to insider threats, allowing dynamic adjustments to access controls and maintaining a robust security posture.

6. Security Awareness

6.1 Continuous Monitoring

According to NIST SP 800-207 [6], continuous monitoring plays an important role for a zero-trust architecture to defend against common threats and improve an organization's security posture by managing risks. The frequency and complexity of cyber-attacks on U.S. Federal information systems are increasing, raising the likelihood of significant damage. Information Security Continuous Monitoring (ISCM) allows for real-time cyber situational awareness, enabling a prompt response to the high rates of vulnerabilities, persistent threats, and determined adversaries. Although monitoring information system security became a requirement for government agencies over 20 years ago for cybersecurity, many government agencies still lack the capabilities to effectively leverage ISCM to collect, aggregate, correlate, and analyze security-related information to enhance real-time threat detection, incident response, and risk-based decision making [63], [64].

The Federal Information Security Management Act (FISMA) [65], a U.S. federal law enacted in 2002 and amended in 2014, emphasizes continuous monitoring and securing information systems commensurate with risk to minimize cybersecurity threats and protect the nation's information assets. In addition, CISA's Continuous Diagnostics and Mitigation (CDM) program [66] provides cybersecurity continuous monitoring tools, integrated services, and dashboards to enhance the cybersecurity of government networks and systems.

Dimitrakos et al. [67] proposed a model for trustworthy continuous access control that addresses the need for continuous authentication from multi-sensors, evaluating trust level and enforcing access control in a dynamic IoT environment. This model was based on the convergence of advanced security technologies such as Attribute Based Access Control (ABAC), Usage Control (UCON), and probabilistic trust assessment. They proposed a UCON+ architecture that extends UCON sessions to handle the continuity and monitoring of interactions before access is granted. UCON+ supports continuous re-evaluation of trust-based policy conditions. The UCON+ architecture offers flexible and scalable trust evaluation and supports monitoring continuously about trust parameters and continuous re-evaluation of trust levels as part of the overall authentication policy reassessment. Also, the Trust Level Evaluation Engine (TLEE) component evaluates the level of trust from attributes of the environment.

Yao et al. [68] proposed a model which continuously observes a user's behavior and measures a behavior trust (BT). Access to a resource is granted only if BT surpasses the trust threshold (TT) which may change dynamically depending on the environment. They also proposed a Trust-Based Access Control (TBAC) model featuring user behavior, which consists of eight elements: User, Role, Resources, Operations, Permissions, Behavior Trust, Trust Threshold, and Authorization. The User element is the subject of access to resources. The Role element is the bridge between users and permissions. The Resource element is the object that the subject accesses. The Operation element uses Resources element. The Permission element is a binary tuple composed of operation and resources, representing the qualification to apply operations to resource element. The Behavior Trust element is the system's integrated trust evaluation of the user's historical and current behavior. The Trust Threshold element is the minimum trust required by the user to apply operations to Resource element. Finally, the Authorization element is in char of a dynamic authorization process.

Tunc et al. [69] presented Autonomic Network Management Engine (AZNME) to monitor network connections of an asset based on the zero-trust architecture. The system is required to continuously evaluate trust value as a way for situational awareness and apply mitigating measurements if necessary. With the self-managing procedure, the engine verifies that the network connections meet zero-trust architecture requirements. AZNME consists of four main modules: observer, controller, policy editor, and engine. The observer module states monitoring capabilities and their configuration attributes. And then the controller module performs the actions invoked by policies for management of the entities. The policy editor module is used to describe actions to be taken on the monitored resources and the way to evaluate trust each entity. Finally, the engine module coordinates all other modules and manages the environment.

6.2 Visualization

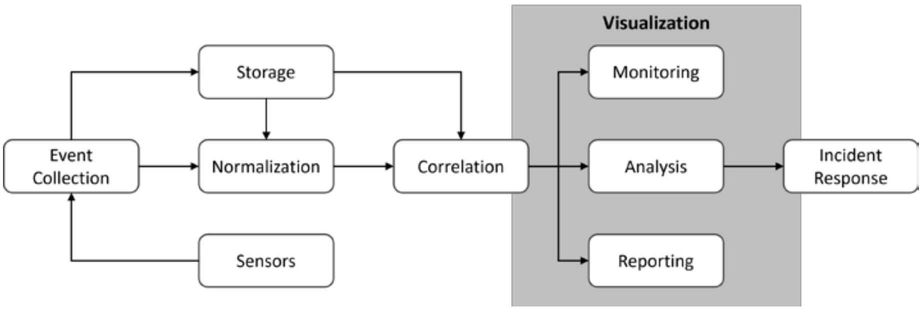


Fig. 9. The security incident management process and visualization coverage.

As a data representation model, cyber common operating picture (CCOP) provides situational awareness allowing military decision-makers to respond effectively in the cyber domain [70]. The CCOP in the military domain is required to visualize the current and historic situation of the organization's cyber assets [71]. According to the Technical Challenge Problem Set published by the US Cyber Command [11], describing complex networks and digital assets via visualization is essential to building deep network knowledge and awareness. The capability of observing the aggregate network and choosing relevant points is critical to defeating adversarial intrusion.

Visualizing the current situation about the infrastructure and security threats is important in defense cybersecurity [72], [73], [74]. Commanders need to gauge the situation to make an effective decision in protecting the infrastructure against current and potential cyber threats. In this regard, visualization provides a user-friendly tool for monitoring, analyzing, reporting overall situation based on the various security events. As the visualization impacts more processes, the coverage of scope in **Fig. 9** expands from correlation to incident response.

As a visual tool, Noel [75] proposed a web-based interactive technique for the CAPEC [76] catalog of attack patterns. The proposal utilizes the natural language description of CAPEC and applies text mining technique to build an overall hierarchy of attack patterns. This model transforms the traditional texts of attack patterns into vector space and allows to compute similarity between vectors representing each attack. The visualization in this work can be used to build higher-level security model.

Chen et al. [77] presented OCEAN, a network visualization system to monitor the live stream of network traffic in terms of time, source and destination information. The system provides a concept of connection river which illustrates picture of network flows shaped by the data source in a time slot. The OCEAN aims to provide in-depth insights over the traffic and allows to identify any anomalies in the traffic. Also, the OCEAN features a multi-level visualization of connections and collaboration views to work together dealing with multi-phase attacks.

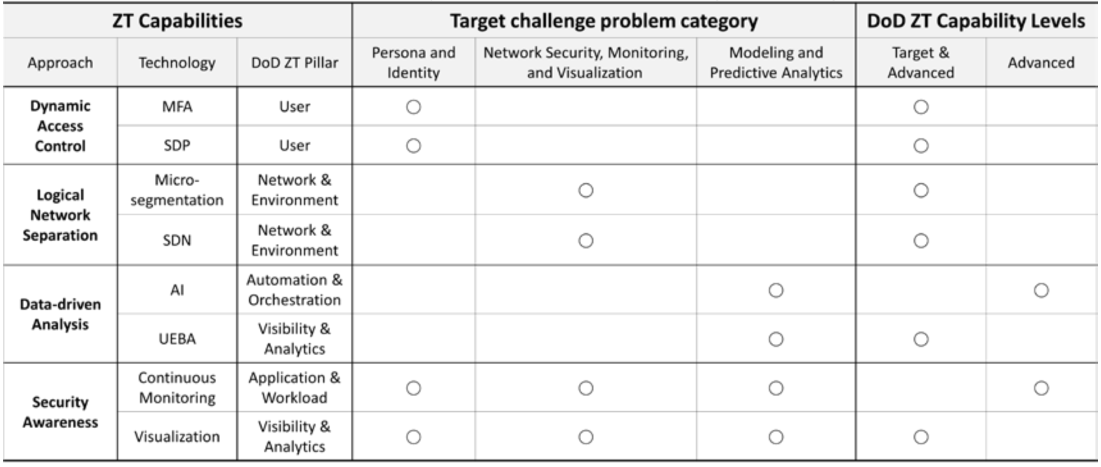
Hong et al. [78] proposed AlertVision, a novel visualization technique which provides a visual representation about the correlation between security alerts. The system presents insight over the relevance between security alerts like SIEM events, aiming to build threat intelligence from the high volume of information in wild. Therefore, the intelligence extracted from security alerts helps analyst not only identify high-level patterns of current attack but also predict potential threats in the future.

Noel et al. [79] presented CyGraph, a unified graph-based model to respond to current and potential cyber-attacks. This graph model predicts possible attack paths and vulnerabilities.

CyGraph puts together the predictions and actual security events to draw an overall picture for decision-making process. Upon receiving attack events, the predictive model correlates the alerts to known attack paths and proposes courses of action as appropriate response. In addition, CyGraph provides interactive visualization functionalities from its graph knowledge base which utilizes standard languages represented in STIX [80], CAPEC [76], and NVD [81].

In the Cyber-Physical System (CPS), a proactive measure to achieve security engineering effectively prevents the failure of security results in uncontrolled situation. Bakirtzis et al. [82] proposed an interactive security analysis model visualizing various views on the system, requirements and its associated attack vectors space. The system provides a common language between security practitioners and system designers. Also, the visualization technique stresses a fusion between system-theoretic security analysis and traditional attack vector analysis.

Table 3. Summary of ZT capabilities for target challenges



ZT Capabilities			Target challenge problem category			DoD ZT Capability Levels	
Approach	Technology	DoD ZT Pillar	Persona and Identity	Network Security, Monitoring, and Visualization	Modeling and Predictive Analytics	Target & Advanced	Advanced
Dynamic Access Control	MFA	User	○			○	
	SDP	User	○			○	
Logical Network Separation	Micro-segmentation	Network & Environment		○		○	
	SDN	Network & Environment		○		○	
Data-driven Analysis	AI	Automation & Orchestration			○		○
	UEBA	Visibility & Analytics			○	○	
Security Awareness	Continuous Monitoring	Application & Workload	○	○	○		○
	Visualization	Visibility & Analytics	○	○	○	○	

7. Challenges and Future Research Directions

The SDP architecture differs from traditional security measures, which means that integrating SDP may pose a risk of network and infrastructure disruptions. It is also demanding for SDP to keep trace of any changes that networks and applications make. With its centralized design, controller can lead to a single point of failure. While SDP has demonstrated scalability and manageability through integration with SDN, maintaining high availability and security have to be addressed as future work.

SDN systems have shown that security vulnerabilities and threats exist across all layers, and simply reinforcing security at each layer is insufficient. Therefore, a comprehensive system is necessary to make the entire network robust and secure. In particular, due to its centralized structure, addressing the security concerns associated with the controller is of paramount significance. Also, implementing micro-segmentation in real network can be challenging due to its complexity and compatibility with existing security frameworks. This can be exacerbated by the frequent changes in the network configurations.

AI models require substantial data to accurately identify threats. It is vital to develop models that either need less data or can detect a wider array of threats. Achieving a balance between minimizing false positives and false negatives is crucial, alongside ensuring that cybersecurity models are robust against manipulations by adversaries. Moreover, improving the adaptability of predictive models is essential to keep pace with the ever-changing landscape of cyber threats and understand their long-term evolution. Within the context of zero-trust architecture, User and Entity Behavior Analytics (UEBA) depend on the established behavioral patterns, which may evolve. Therefore, distinguishing potential threats from normal changes in the behavior analysis presents a significant challenge.

As for security awareness, data visualization for cybersecurity has inherent challenges due to the volume and complexity of data. The inherent factors cause a massive number of features to extract and prevent analysts from discovering the meaningful relationships among data. Hence, visualizing correlation across heterogeneous data sources can be a challenging problem. Combining and normalizing the multiple datasets need to be addressed in the future. Besides, the accuracy of the visual analytics matters in real network environment. It is necessary to evaluate feedback like [83] by comparing user interactive decision from the automated process. Also, more studies on the efficient continuous monitoring in terms of cost and management are considered to be future work.

8. Conclusion

Zero Trust is an evolving cybersecurity paradigm that allows defense to develop more resilient framework protecting its infrastructure from malicious cyber activities. This enhanced model eliminates the traditional idea of presumably trusted or untrusted networks. Instead, dynamic confidence levels from continuous verification determine an access to resources, concentrating more on the security contexts.

In this article, we introduced the security context of defense and ongoing efforts to build its zero-trust architecture. Apart from the general definition of the capabilities in the ZTA, we identified the target challenge problems in defense cybersecurity and presented technical capabilities. First, MFA and SDP are introduced as a dynamic access control approach to address identity fabrication and credential misuse problems in person and identity category. Its centralized design needs to be improved as a future work to avoid a single point of failure. Secondly, logical network separation approach by SDN and micro-segmentation is suggested to tackle challenge problems in network security, monitoring, and visualization category. The implementation complexity of micro-segmentation may aggravate compatibility with existing security framework. Minimizing impact by frequent changes to the network should be addressed in the future. Thirdly, challenge problems in modeling and predictive analytics category are covered by the data-driven analysis approach. In particular, AI and UEBA are presented to identify insider threats and malicious actions. Due to rapid evolution of cyber threats, improving predictive models and making them resistant to adversarial manipulation continuously are suggested as future works. Lastly, continuous monitoring and data visualization are mentioned to represent security awareness approach. The two capabilities covered challenge problems of the all three target categories in that they are essential in comprehending cybersecurity situations and making proper decisions. Due to the volume and complexity of data, study on the efficient methods for handling data is future work.

Zero-trust architecture alone is not enough to tackle all the problems in defense cybersecurity which is working in collaboration across different security class and domains. A gradual step is necessary to identify target challenges of the domain and map applicable capabilities of ZTA to the challenges. Comprehensive study in this article is expected to serve as an example for defense organizations to facilitate embedding the zero-trust principles in their cybersecurity architecture.

References

[1] DoD Cybersecurity, Enhanced attention needed to ensure cyber incidents are appropriately reported and shared, Nov. 2022. [Online]. Available: https://www.gao.gov/assets/gao-23-105084.pdf

[2] NSA, Network infrastructure security guide version 1.2, Oct. 2023. [Online]. Available: https://media.defense.gov/2022/Jun/15/2003018261/-1/-1/0/CTR_NSA_NETWORK_INFRASTRUCTURE_SECURITY_GUIDE_20220615.PDF

[3] D. Kushner, "The real story of stuxnet," *IEEE Spectrum*, vol.50, no.3, pp.48-53, 2013. [Online]. Available: https://spectrum.ieee.org/the-real-story-of-stuxnet

[4] MITRE ATT&CK Framework. [Online]. Available: https://attack.mitre.org/

[5] J. Kindervag, Build Security Into Your Network's DNA: The Zero Trust Network Architecture, Forrester Research Inc, 2010.
[Online]. Available: https://www.actiac.org/system/files/Forrester_zero_trust_DNA.pdf

[6] Scott Rose, Oliver Borchert, Zero Trust Architecture, National Institute of Standards and Technology (NIST) special publication 800-207, 2020. Artical (CrossRef Link)

[7] Department of Defense (DoD), Cybersecurity Reference Architecture, Jan. 2023. [Online]. Available: https://dodcio.defense.gov/Portals/0/Documents/Library/CS-Ref-Architecture.pdf

[8] MITRE D3FEND. [Online]. Available: https://d3fend.mitre.org/

[9] Department of Defense (DoD), Zero Trust Reference Architecture, Jul. 2022. [Online]. Available: https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v2.0(U)_Sep22.pdf

[10] Department of Defense (DoD), DoD Zero Trust Strategy, 2022. [Online]. Available: https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf

[11] U.S. Cyber Command, Technical Challenge Problems Guidance, Mar. 2020. [Online]. Available: https://www.caecommunity.org/news/us-cyber-command-technical-challenge-problems-guidance

[12] Department of Defense (DoD), DoD EnterpriseIdentity, Credential, and Access Management (ICAM) Reference Design, Ver. 1.0, Jun. 2020. [Online]. Available: https://dodcio.defense.gov/Portals/0/Documents/Cyber/DoD_Enterprise_ICAM_Reference_Design.pdf

[13] D. Bhanderi, M. Kavathiya, T. Bhut, H. Kaur, M. Mehta, "Impact of Two-Factor Authentication on User Convenience and Security," in *Proc. of 2023 10th International Conference on Computing for Sustainable Global Development (INDIACom)*, pp.617-622, New Delhi, India, Mar. 2023. Article (CrossRef Link)

[14] B. O. ALSaleem and A. I. AlShoshan, "Multi-Factor Authentication to Systems Login," in *Proc. of 2021 National Computing Colleges Conference (NCCC)*, pp.1-4, Taif, Saudi Arabia, Mar. 2021. Article (CrossRef Link)

[15] Department of Defense (DoD) Instruction 8520.03, Identity Authentication for Information Systems, May. 19, 2023. [Online]. Available: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/852003p.pdf

[16] Digital Identity Guidelines, NIST SP 800-63-3, 2020. Artical (CrossRef Link)

[17] Digital Identity Guidelines: Authentication and Lifecycle Management, NIST SP 800-63B, 2017. Artical (CrossRef Link)

[18] S. Choe, North Korean Hackers Stole U.S.-South Korean Military Plans, Lawmaker Says, Oct. 2017. [Online]. Available: https://www.nytimes.com/2017/10/10/world/asia/north-korea-hack-war-plans.html

[19] R. Ross, V. Pillitteri, R. Graubart, D. Bodeau and R. McQuaid, "Developing Cyber-Resilient Systems: A Systems Security Engineering Approach," *National Institute of Standards and Technology (NIST) Special Publication 800-160*, vol.2, Dec. 2021. Article (CrossRef Link)

[20] A. Sallam, A. Refaey, and A. Shami, "On the Security of SDN: A Completed Secure and Scalable Framework Using the Software-Defined Perimeter," *IEEE Access*, vol.7, pp.146577-146587, Sep. 2019. Article (CrossRef Link)

[21] A. Moubayed, A. Refaey, and A. Shami, "Software-Defined Perimeter (SDP): State of the Art Secure Solution for Modern Networks," *IEEE Network*, vol.33, no.5, pp.226-233, 2019. Article (CrossRef Link)

[22] P. Kumar, A. Moubayed, A. Refaey, A. Shami, and J. Koilpillai, "Performance Analysis of SDP For Secure Internal Enterprises," in *Proc. of 2019 IEEE Wireless Communications and Networking Conference (WCNC)*, pp.1-6, Marrakesh, Morocco, Apr. 2019. Article (CrossRef Link)

[23] R. R. Omar and T. M. Abdelaziz, "A Comparative Study of Network Access Control and Software-Defined Perimeter," in *Proc. of 6th International Conference on Engineering & MIS 2020 (ICEMIS)*, pp.1-5, New York, NY, USA, Sep. 2020. Article (CrossRef Link)

[24] OpenFlow Switch Specification version 1.4.0, 2013. [Online]. Available: https://opennetworking.org/wp-content/uploads/2014/10/openflow-spec-v1.4.0.pdf

[25] ONF White Paper, Software-Defined Networking: The New Norm for Networks, Open Networking Foundation, 2012. [Online]. Available: https://opennetworking.org/wp-content/uploads/2011/09/wp-sdn-newnorm.pdf

[26] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner, "OpenFlow: Enabling innovation in campus networks," *ACM SIGCOMM Computer Communication Review*, vol.38, no.2, pp.69-74, Apr. 2008. Article (CrossRef Link)

[27] J. Jang and T. Kwon, "The Validity Analysis of SDN/NFV Military application," *The Journal of the Korea institute of electronic communication sciences*, vol.15, no.4, pp.687-694, Aug. 2020. Article (CrossRef Link)

[28] P. Goldstein, Why DISA Has Embraced SDN for the Pentagon, *FedTech*, Sep. 2018. [Online]. Available: https://fedtechmagazine.com/article/2018/09/why-disa-has-embraced-sdn-pentagon-perfcon

[29] J. C. C. Chica, J. C. Imbachi, and J. F. B. Vega, "Security in SDN: A comprehensive survey," *Journal of Network and Computer Applications*, vol.159, Jun. 2020. Article (CrossRef Link)

[30] A. Pradhan and R. Mathew, "Solutions to Vulnerabilities and Threats in Software Defined Networking (SDN)," *Procedia Computer Science*, vol.171, pp.2581-2589, 2020. Article (CrossRef Link)

[31] C. Yoon, S. Lee, H. Kang, T. Park, S. Shin, V. Yegneswaran, P. Porras, and G. Gu, "Flow Wars: Systemizing the Attack Surface and Defenses in Software-Defined Networks," *IEEE/ACM Transactions on Networking*, vol.25, no.6, pp.3514-3530, Dec. 2017. Article (CrossRef Link)

[32] K. Fatima, K. Zahoor, and N. Zakaria Bawany, "SDN Control Plane Security: Attacks and Mitigation Techniques," in *Proc. of 4th International Conference on Networking, Information Systems & Security (NISS)*, pp.1-6, 2021. Article (CrossRef Link)

[33] A. Feghali, R. Kilany, and M. Chamoun, "SDN security problems and solutions analysis," in *Proc. of 2015 International Conference on Protocol Engineering (ICPE) and International Conference on New Technologies of Distributed Systems (NTDS)*, pp.1-5, Paris, France, Jul. 2015. Article (CrossRef Link)

[34] M. Rahouti, K. Xiong, Y. Xin, S. K. Jagatheesaperumal, M. Ayyash, and M. Shaheed, "SDN Security Review: Threat Taxonomy, Implications, and Open Challenges," *IEEE Access*, vol.10, pp.45820-45854, Apr. 2022. Article (CrossRef Link)

[35] M. S. Farooq, S. Riaz and A. Alvi, "Security and Privacy Issues in Software-Defined Networking (SDN): A Systematic Literature Review," *Electronics*, vol.12, no.14, Jul. 2023. Article (CrossRef Link)

[36] M. Ahmed, S. S. Fatima, A. A. Khan, and S. A. S. Jafri, "Security Issues in Software Defined Networks," *ILMA Journal of Technology & Software Management*, vol.2, no.1, pp.29-36, Mar. 2022. Article (CrossRef Link)

[37] N. F. Syed, S. W. Shah, A. Shaghaghi, A. Anwar, Z. Baig and R. Doss, "Zero Trust Architecture (ZTA): A Comprehensive Survey," *IEEE Access*, vol.10, pp.57143-57179, May. 2022. Article (CrossRef Link)

[38] A. Poirrier, L. Cailleux and T. H. Clausen, "An Interoperable Zero Trust Federated Architecture for Tactical Systems," in *Proc. of MILCOM 2023 - 2023 IEEE Military Communications Conference*, pp.405-410, Boston, MA, USA, Oct. 2023. Article (CrossRef Link)

[39] A. Castañares, D. K. Tosh and C. A. Kamhoua, "Slice Aware Framework for Intelligent and Reconfigurable Battlefield Networks," in *Proc. of MILCOM 2021 - 2021 IEEE Military Communications Conference*, pp.489-494, San Diego, CA, USA, Nov. 2021. Article (CrossRef Link)

[40] CICA Publishes Infographic on Layering Network Security Through Segmentation, Jan. 2022. [Online]. Available: https://www.cisa.gov/news-events/alerts/2022/01/24/cisa-publishes-infographic-layering-network-security-through-segmentation

[41] B. Chen, S. Qiao, J. Zhao, D. Liu, X. Shi, M. Lyu, H. Chen, H. Lu, and Y. Zhai, "A Security Awareness and Protection System for 5G Smart Healthcare Based on Zero-Trust Architecture," *IEEE Internet of Things Journal*, vol.8, no.13, pp.10248-10263, Jul. 2021. Article (CrossRef Link)

[42] M. Arifeen, A. Petrovski, and S. Petrovski, "Automated Microsegmentation for Lateral Movement Prevention in Industrial Internet of Things (IIoT)," in *Proc. of 2021 14th International Conference on Security of Information and Networks (SIN)*, vol.1, pp.1-6, Edinburgh, United Kingdom, Dec. 2021. Article (CrossRef Link)

[43] N. Sheikh, M. Pawar, and V. Lawrence, "Zero trust using Network Micro Segmentation," in *Proc. of IEEE INFOCOM 2021 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pp.1-6, Vancouver, BC, Canada, May. 2021. Article (CrossRef Link)

[44] L. Xie, F. Hang, W. Guo, Y. Lv and H. Chen, "A Micro-Segmentation Protection Scheme Based on Zero Trust Architecture," in *Proc. of ISCTT 2021; 6th International Conference on Information Science, Computer Technology and Transportation*, pp.1-4, Xishuangbanna, China, Nov. 2021. Article (CrossRef Link)

[45] B. C. da Rocha, L. P. de Melo and R. T. de Sousa, "Preventing APT attacks on LAN networks with connected IoT devices using a zero trust based security model," in *Proc. of 2021 Workshop on Communication Networks and Power Systems (WCNPS)*, pp.1-6, Brasilia, Brazil, Nov. 2021. Article (CrossRef Link)

[46] A. Hakiri, A. S. Gokhale, Y. Brave, V. Formicola, S. Shekhar, C. Mahmoudi, M. A. Rahman, U. Ghosh, S. R. Hasan and T. Guo, "Techniques for realizing secure, resilient and differentiated 5G operations," in *Proc. of 2022 14th IFIP Wireless and Mobile Networking Conference (WMNC)*, pp.113-117, Sousse, Tunisia, Oct. 2022. Article (CrossRef Link)

[47] M. Ma, Z. Yu, and B. Liu, "Automatic generation of network micro-segmentation policies for cloud environments," in *Proc. of 2023 4th International Seminar on Artificial Intelligence, Networking and Information Technology (AINIT)*, pp.1-5, Nanjing, China, Jun. 2023. Article (CrossRef Link)

[48] A. D. Kaasen, G. Grov, F. Mancini and M. Baksaas, "Towards data-driven autonomous cyber defence for military unmanned vehicles - threats & attacks," in *Proc. of MILCOM 2022 - 2022 IEEE Military Communications Conference*, pp.861-866, Rockville, MD, USA, Nov. 2022. Article (CrossRef Link)

[49] J. Kohout, Security Information and Event Management, UNICORN. [Online]. Available: https://unicornsystems.eu/en/siem

[50] Y. Shen, E. Mariconti, P. A. Vervier, and G. Stringhini, "Tiresias: Predicting Security Events Through Deep Learning," in *Proc. of the 2018 ACM SIGSAC Conference on Computer and Communications Security (CCS '18)*, pp.592-605, Oct. 2018. Article (CrossRef Link)

[51] M. Naseri, Y. Han, E. Mariconti, Y. Shen, G. Stringhini, and E. D. Cristofaro, "Cerberus: Exploring Federated Prediction of Security Events," in *Proc. of 2022 ACM SIGSAC Conference on Computer and Communications Security (CCS '22)*, pp.2337-2351, Nov. 2022. Article (CrossRef Link)

[52] Z. Li, D. Zhao, X. Li, and H. Zhang, "Network security situation prediction based on feature separation and dual attention mechanism," *EURASIP Journal on Wireless Communications and Networking*, vol.2021, Sep. 2021. Article (CrossRef Link)

[53] A. Brown, A. Tuor, B. Hutchinson, and N. Nichols, "Recurrent Neural Network Attention Mechanisms for Interpretable System Log Anomaly Detection," in *Proc. of 1st Workshop on Machine Learning for Computing Systems (MLCS '18)*, pp.1-8, Jun. 2018. Article (CrossRef Link)

[54] M. A. Salitin and A. H. Zolait, "The role of User Entity Behavior Analytics to detect network attacks in real time," in *Proc. of 2018 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT)*, pp.1-5, 2018. Article (CrossRef Link)

[55] R. Olaniyan, S. Rakshit, and N. R. Vajjhala, "Application of User and Entity Behavioral Analytics (UEBA) in the Detection of Cyber Threats and Vulnerabilities Management," in *Proc. of Computational Intelligence for Engineering and Management Applications: Select Proceedings of CIEMA 2022, Lecture Notes in Electrical Engineering*, vol.984, pp.419-426, Singapore, 2023. Article (CrossRef Link)

[56] F. Skopik, M. Wurzenberger, G. Höld, M. Landauer, and W. Kuhn, "Behavior-Based Anomaly Detection in Log Data of Physical Access Control Systems," in *Proc. of IEEE Transactions on Dependable and Secure Computing*, vol.20, no.4, pp.3158-3175, Jul.-Aug. 2023. Article (CrossRef Link)

[57] J. Kaur, K. Kaur, S. Kant and S. Das, "UEBA with Log Analytics," in *Proc. of 2022 3rd International Conference on Computing, Analytics and Networks (ICAN)*, pp.1-7, 2022. Article (CrossRef Link)

[58] M. Yamauchi, Y. Ohsita, M. Murata, K. Ueda, and Y. Kato, "Anomaly Detection for Smart Home Based on User Behavior," in *Proc. of 2019 IEEE International Conference on Consumer Electronics (ICCE)*, pp.1-6, Las Vegas, NV, USA, Jan. 2019. Article (CrossRef Link)

[59] D. Sugumaran, Y. M. Mahaboob John, J. S. Mary C, K. Joshi, G. Manikandan and G. Jakka, "Cyber Defence Based on Artificial Intelligence and Neural Network Model in Cybersecurity," in *Proc. of 2023 Eighth International Conference on Science Technology Engineering and Mathematics (ICONSTEM)*, pp.1-8, Chennai, India, Apr. 2023. Article (CrossRef Link)

[60] M. Shashanka, M.-Y. Shen and J. Wang, "User and entity behavior analytics for enterprise security," in *Proc. of 2016 IEEE International Conference on Big Data (Big Data)*, pp.1867-1874, 2016. Article (CrossRef Link)

[61] T. Zoppi, M. Gharib, M. Atif, and A. Bondavalli, "Meta-Learning to Improve Unsupervised Intrusion Detection in Cyber-Physical Systems," *ACM Transactions on Cyber-Physical Systems (TCPS)*, vol.5, no.4, pp.1-27, 2021. Article (CrossRef Link)

[62] P. A. Savenkov and A. N. Ivutin, "Methods of Machine Learning in System Abnormal Behavior Detection," in *Proc. of 11th International Conference on Advances in Swarm Intelligence (ICSI)*, vol.12145, pp.495-505, 2020. Article (CrossRef Link)

[63] T. AlSadhan, and J. S. Park, "Leveraging Information Security Continuous Monitoring to Enhance Cybersecurity," in *Proc. of 2021 International Conference on Computational Science and Computational Intelligence (CSCI)*, pp.753-759, Las Vegas, NV, USA, Dec. 2021. Article (CrossRef Link)

[64] T. AlSadhan and J. Park, "Assessing Information Security Continuous Monitoring in the Federal Government," in *Proc. of the 21st European Conference on Cyber Warfare and Security (ECCWS 2022)*, vol.21, no.1, pp.351-359, Chester, United Kingdom, Jun. 2022. Article (CrossRef Link)

[65] S.2521 - Federal Information Security Modernization Act of 2014. [Online]. Available: https://www.congress.gov/bill/113th-congress/senate-bill/2521

[66] Continuous Diagnostics and Mitigation (CDM) program, CISA. [Online]. Available: https://www.cisa.gov/resources-tools/programs/continuous-diagnostics-and-mitigation-cdm-program

[67] T. Dimitrakos, T. Dilshener, A. Kravtsov, A. La Marra, F. Martinelli, A. Rizos, A. Rosetti and A. Saracino, "Trust Aware Continuous Authorization for Zero Trust in Consumer Internet of Things," in *Proc. of 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, pp.1801-1812, Guangzhou, China, Dec. 2020. Article (CrossRef Link)

[68] Q. Yao, Q. Wang, X. Zhang and J. Fei, "Dynamic Access Control and Authorization System based on Zero-trust architecture," in *Proc. of the 2020 1st International Conference on Control, Robotics and Intelligent System*, pp.123-127, Jan. 2021. Article (CrossRef Link)

[69] C. Tunc, J. Durflinger, C. Mahmoudi, and V. Formicola, "Autonomic ZTA-based Network Management Engine (AZNME)," in *Proc. of 2022 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW)*, pp.25-30, Charlotte, NC, USA, Oct. 2022. Article (CrossRef Link)

[70] G. Conti, J. Nelson and D. Raymond, "Towards a cyber common operating picture," in *Proc. of 2013 5th International Conference on Cyber Conflict (CYCON 2013)*, pp.1-17, Tallinn, Estonia, Jun. 2013. Article (CrossRef Link)

[71] F. Skopik, A. Bonitz, , V. Grantz, and G. Göhler, "From scattered data to actionable knowledge: flexible cyber security reporting in the military domain," *International Journal of Information Security*, vol.21, no.6, pp.1323-1347, Dec. 2022. Article (CrossRef Link)

[72] M. Angelini, N. Prigent, and G. Santucci, "Percival: proactive and reactive attack and response assessment for cyber incidents using visual analytics," in *Proc. of 2015 IEEE Symposium on Visualization for Cyber Security (VizSec)*, pp.1-8, Chicago, IL, USA, Oct. 2015. Article (CrossRef Link)

[73] M. Angelini, S. Bonomi, S, Lenti, G. Santucci, and S. Taggi, "MAD: A visual analytics solution for Multi-step cyber Attacks Detection," *Journal of Computer Languages*, vol.52, pp.10-24, Jun. 2019. Article (CrossRef Link)

[74] S. Cho, I. Han, H. Jeong, J. Kim, S. Koo, H. Oh, and M. Park, "Cyber Kill Chain based Threat Taxonomy and its Application on Cyber Common Operational Picture," in *Proc of 2018 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*, pp.1-8, Glasgow, UK, Jun. 2018. Article (CrossRef Link)

[75] S. Noel, "Interactive Visualization and Text Mining For the CAPEC Cyber Attack Catalog," in *Proc. of the ACM Intelligent User Interfaces Workshop on Visual Text Analytics*, pp.1-8, 2015. Article (CrossRef Link)

[76] Common Attack Pattern Enumeration and Classification (CAPEC™). [Online]. Available: https://capec.mitre.org/

[77] S. Chen, C. Guo, X. Yuan, F. Merkle, H. Schaefer, and T. Ertl, "Oceans: Online collaborative explorative analysis on network security," in *Proc. of 11th Workshop on Visualization for Cyber Security*, pp.1-8, Nov. 2014. Article (CrossRef Link)

[78] J. Hong, J. Lee, H. Lee, Y. Chang, K. Choi, and S. K. Cha, "AlertVision: Visualizing Security Alerts," in *Proc. of 19th International Conference on Information Security Applications (WISA 2018)*, LNCS, vol.11402, pp.173-184, Jeju, Korea, Aug. 2018. Article (CrossRef Link)

[79] S. Noel, E. Harley, K. H. Tam, M. Limiero, and M. Share, "CyGraph: Graph-Based Analytics and Visualization for Cybersecurity," *Handbook of Statistics*, vol.35, pp.117-167, Elsevier, 2016. Article (CrossRef Link)

[80] STIX, OASIS Open. [Online]. Available: https://docs.oasis-open.org/cti/stix/v2.1/stix-v2.1.html

[81] National Vulnerability Database. [Online]. Available: https://nvd.nist.gov/

[82] G. Bakirtzis, B. J. Simon, C. H. Fleming, and C. R. Elks, "Looking for a Black Cat in a Dark Room: Security Visualization for Cyber-Physical System Design and Analysis," in *Proc. of 2018 IEEE Symposium on Visualization for Cyber Security (VizSec)*, pp.1-8, Berlin, Germany, Oct. 2018. Article (CrossRef Link)

[83] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "An evaluation framework for network security visualizations," *Computers & Security*, vol.84, pp.70-92, 2019. Article (CrossRef Link)

Youngho Kim received the B.S. and M.S. degrees in Computer Science from Korea University, Korea, in 1999 and 2001, respectively. He is a currently principal researcher with Electronics Telecommunications Research Institute (ETRI), Korea. His research interests include system software security, IoT security, network security, and defense cybersecurity.

Seon-Gyoung Sohn received the B.S. and M.S. degrees in Computer Science from Chonnam National University, Korea, in 1999 and 2001, respectively. She is currently a principal researcher at Electronics and Telecommunications Research Institute, Korea. Her main research interests include cybersecurity, security threat response, and cyber warfare.

Kyeong Tae Kim received the B.S. degree in Computer Engineering from Kangwon National University, Korea in 2004 and the M.S. degrees in Information and Communications from Gwangju Institute of Science and Technology, Korea in 2006, respectively. Since 2006, he has been a research member of Electronics and Telecommunications Research Institute, Korea. His research interests include AI, Network Security and Wireless Communication.

Hae Sook Jeon received her Ph.D. degree in Computer Engineering at University of Chungnam National University in 2015. She is currently a principal researcher at Electronics and Telecommunications Research Institute, Korea. Her research interests include wired network systems, embedded systems, land-based monitoring systems for ship equipment and cyber battlefield threat active countermeasure technologies.

Sang-Min Lee received the B.S. and M.S. degrees in Electronics Engineering from Kyungpook National University, Korea, in 1994 and 1996, respectively. He is a currently principal researcher with Electronics Telecommunications Research Institute, Korea. His research interests include SDN/NFV, cloud security, AI-based malware detection, and defense cybersecurity.

Yunkyung Lee received the M.S. degree from POSTECH in KOREA and the Ph.D. degree from the School of Computing at KAIST in Korea. She is currently the director of the Cyber Warfare Technology Research center in the Cyber Security Research Division, ETRI, Korea. Her research interests include IoT security, mobile security, network security, authentication, and Zero Trust.

Jeongnyeo Kim received her M.S. and Ph.D. degrees from Department of Computer Engineering at Chungnam National University. Currently, she is the head of the Cyber Security Research Division, ETRI, Korea. And since 2015, she is also a full-time professor in the Department of ICT Engineering(Information Security Major) at UST. Her research interests include IoT security, mobile security, system and network security, and secure OS.