Scientific Innovative Center Research

INSIDER THREATS AND SECURITY IN CORPORATIONS

Monograph

Table of Contents

Introduction 4
Chapter 1. Theoretical and Conceptual Foundations of Insider and Hybrid Threats 8
Section 1.1. Essence and Evolution of the Insider Threat Concept in Corporate Systems
Paulina Kolisnichenko 9
Section 1.2. Typology and Behavioral Determinants of Insider and Hybrid Threats
Oleksandra Liashenko 32
Section 1.3. Theoretical Models of Organizational Vulnerability and Security Resilience
Iryna Mazur 55

Chapter 2. Insider Threats in Corporate Governance and Organizational Structures 76
Section 2.1. Corporate Governance as a Mechanism of Control and Trust
Iryna Mihus 77
Section 2.2. Insider Threats to Managerial Decision-Making and Ethical Standards in Corporate Development
Yaroslav Kokhaniuk 96
Section 2.3. Institutional and Cultural Determinants of Insider Behavior in Corporation Governance
Andriy Push 113

Chapter 3. Cybersecurity and Digital Dimensions of Insider Threats 135
Section 3.1. Developing a Balanced Security Policy for Bring Your Own Device in Corporate Networks
Volodymyr Sokolov, Pavlo Skladannyi 136
Section 3.2. Research and Implementation of the Digital Signature Algorithm (DSA) in Ensuring Information Protection
Olena Kryvoruchko, Milana Bilych, Yevheniy Nikitenko 157
Section 3.3. Model of Integration of Loyalty Assessment Results into the Threat Management System of the Economic Security of an Industrial Enterprise
Kyrylo Zlobin 181

Conclusions 204
References 207

https://doi.org/10.36690/ITSC ISBN 978-9916-9320-4-9 (pdf)

Section 3.1. Developing a Balanced Security Policy for Bring Your Own Device in Corporate Networks

Volodymyr Sokolov[1], Pavlo Skladannyi[2]

[1]*Ph.D. (Information Technology), Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine, e-mail: v.sokolov@kubg.edu.ua, ORCID: https://orcid.org/0000-0002-9349-7946*

[2]*Ph.D. (Information Technology), Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine, e-mail: p.skladannyi@kubg.edu.ua, ORCID: https://orcid.org/0000-0002-7775-6039*

Citation:
Sokolov, V. & Skladannyi, P. (2025). Developing a Balanced Security Policy for Bring Your Own Device in Corporate Networks. In P. Kolisnichenko (Ed.), *Insider threats and security in corporations*. 216 p. (pp. 136–156). Scientific Center of Innovative Research. https://doi.org/10.36690/ITSC-136-156

Abstract. *With the rapid expansion of personal device usage in corporate environments, the Bring Your Own Device (BYOD) concept introduces significant cybersecurity challenges. This study focuses on formalizing and systematizing approaches to securing BYOD-enabled infrastructures within organizations. A comprehensive architecture is proposed based on seven interconnected models: a risk assessment model, Multi-Factor Authentication (MFA) model, a Zero Trust (ZT) access control model, an encryption security model, a network segmentation model, a security monitoring and response model, and a User Behavior Analytics (UBA) model. Each model is presented in a formal mathematical form, enabling quantitative evaluation of security metrics and adaptive protection aligned with real-time threat conditions. The architecture reflects a defense-in-depth principle, where safeguards at others mitigate weaknesses at one layer. The interaction between components forms a closed-loop system of analysis, control, and response in which user and device risk profiles influence access policies, authentication mechanisms, and monitoring intensity. Special emphasis is placed on dynamic trust evaluation and adaptive response based on behavioral anomalies. The models can be applied to design, assess, and optimize enterprise security frameworks in BYOD scenarios. The integration of these models allows for a highly modular and scalable approach to enterprise security, where a combination of statistical inference, user context, and technical indicators drives decision-making. This multi-factor model enhances resilience by enabling proactive detection and isolation of threats, ensuring that access decisions are granular and risk-aware. Formal metrics also support auditing, compliance, and continual improvement processes across diverse regulatory environments. Finally, directions for future research are outlined, including empirical validation of the models, integration of machine learning techniques, enhancement of behavioral analytics, and incorporation of economic cost models. The proposed approach provides a foundation for building secure, flexible, and scalable BYOD security systems in the era of digital mobility.*

Keywords: *BYOD, Risk Assessment, Zero Trust Architecture, Multi-Factor Authentication, Encryption, Network Segmentation, User Behavior Analytics, Security Monitoring, Access Control, Cybersecurity Modeling.*

ISBN 978-9916-9320-4-9 (pdf)

1. Bring Your Own Device Classification: essence and hierarchical scheme. BYOD security refers to the challenges and solutions associated with employees using their personal devices to access organizational networks and data. While BYOD can enhance productivity and flexibility, it introduces substantial security risks, particularly in relation to data protection, policy compliance, and user behavior. The central challenge involves maintaining security and control over confidential corporate data while allowing personal devices with heterogeneous security standards to connect to the network. Several key aspects of this issue can be identified. First, personal devices may fail to comply with corporate security policies, which increases the likelihood of data breaches, data leaks, or unauthorized access to sensitive information (Kipchuk et al., 2021). Second, IT departments encounter difficulties monitoring, managing, and updating diverse user-owned devices operating across various platforms. Third, ensuring compliance with data protection regulations such as GDPR (Iavich et al., 2024) and HIPAA becomes complex when data are stored or processed on personal devices. This extends to legal concerns and ethical conflicts regarding potential corporate use of employee and customer personal data, especially when personal and work information coexist on the same device. Fourth, unprotected personal devices may serve as entry points for malware, phishing attacks (Marusenko et al., 2020), or other cyber threats. Thus, although BYOD enhances flexibility and productivity, it simultaneously increases security, compliance, and management challenges.

A review of existing research indicates that many personal devices lack adequate security features, rendering them vulnerable to malware, unauthorized access, and data leaks (Wang et al., 2021; Bahaddad et al., 2022; Downer & Bhattacharya, 2015). Organizational BYOD policies are often incomplete or outdated, resulting in inconsistent security practices and unclear responsibilities (Wang et al., 2021; Kiah et al., 2020; Wani et al., 2022). Employees may not fully understand security risks or may disregard established policies, thereby elevating the likelihood of security incidents (Kiah et al., 2020; Wani et al., 2020; Lian, 2020). Lost or stolen devices also expose sensitive data when insufficiently protected (Kiah et al., 2020).

Common security solutions include firewalls, two-factor authentication, virtual private networks, mobile device management platforms, unified endpoint management systems, and containerization to separate work and personal data (Bahaddad et al., 2022; Downer & Bhattacharya, 2015; Wani et al., 2022). Effective BYOD security requires clear, regularly updated policies addressing device use, data access, and compliance requirements (Wang et al., 2021; Wani et al., 2022; Olson et al.,

https://doi.org/10.36690/ITSC ISBN 978-9916-9320-4-9 (pdf)

2015). Regular user education and active engagement are essential to ensure that employees understand and follow security protocols (Kiah et al., 2020; Lian, 2020; Bhattacharya & Downer, 2022). Recent studies highlight the growing use of supervised machine learning models such as SVM, decision trees, and random forests to detect and mitigate BYOD-related threats, although further research is needed in unsupervised and deep learning approaches (Norman et al., 2023).

Developing a strong security culture and involving users in policy creation contribute to improved compliance and reduced risk (Lian, 2020; Bhattacharya & Downer, 2022). Users are more likely to adopt protective BYOD behaviors when they perceive policies as relevant, understand security threats, and feel confident in implementing protective measures. Achieving consistent adherence to BYOD security requirements remains a challenge shaped by organizational support, user attitudes, and the complexity of security protocols (Kiah et al., 2020; Wani et al., 2022).

Adopting BYOD policies in corporate environments presents significant security and management challenges, as personal devices – often lacking standardized security controls – are granted access to sensitive organizational networks and data. This integration increases the risk of data leakage, malware infection, unauthorized access, and regulatory non-compliance. Traditional security architectures struggle to adapt to BYOD's diverse and dynamic nature, where device heterogeneity, user behavior, and limited administrative oversight further complicate threat detection and policy enforcement. Therefore, there is a critical need for comprehensive BYOD protection strategies that ensure data confidentiality, integrity, and availability while maintaining user flexibility and compliance with international security standards.

Ensuring the security of BYOD in corporate environments requires a multi-faceted approach that addresses both technological and human vulnerabilities. One of the most promising frameworks is ZT architecture, which operates on the principle of "never trust, always verify." In this model, every device and user – regardless of location – is subject to continuous authentication, device health checks, and strict, context-aware access policies. This significantly reduces the risk of unauthorized access and lateral movement within the corporate network. Complementing ZT architecture, mobile threat defense uses machine learning to monitor device behavior in real-time, detecting threats such as malicious apps, phishing attempts, and unsafe networks before they can cause harm.

Another key strategy is containerization and workspace isolation, which separates corporate applications and data from personal content on the

https://doi.org/10.36690/ITSC ISBN 978-9916-9320-4-9 (pdf)

same device. This is often managed through mobile application management, enabling organizations to protect sensitive data without infringing on user privacy or requiring complete control over personal devices. Unified endpoint management platforms further enhance control by integrating mobile device management, application management, and policy enforcement into a single solution supporting various devices and operating systems. These technologies provide the foundation for a consistent and scalable security posture across all endpoints.

Modern BYOD security also relies heavily on intelligent, context-aware access controls. Risk-based and adaptive authentication dynamically adjusts security requirements depending on device trust level, user behavior, and location. This strengthens security and improves user experience by reducing unnecessary authentication steps in low-risk scenarios. Artificial intelligence-driven behavioral analytics are similarly effective, enabling the detection of anomalous activities – such as unusual login patterns or unexpected data transfers – that may indicate compromised credentials or insider threats. These tools allow organizations to respond to incidents quickly and effectively, often before any damage is done.

Equally important are data protection measures and user education. Data loss prevention solutions help monitor and control the flow of sensitive information, using context and content classification to prevent unauthorized data exfiltration. Strong encryption at rest and in transit ensures that even intercepted data remains unreadable. Additionally, organizations must invest in continuous employee training to address the human element of security. Regular, scenario-based training should reinforce phishing awareness, secure device handling, and proper incident reporting. By combining advanced technologies with proactive user engagement, companies can build a resilient BYOD security framework that supports productivity without compromising data integrity or compliance.

This structured classification reflects technological, organizational, and policy-related dimensions often used in academic and industry research (Figure 3.1).

BYODs, as shown in Figure 3.1, can be divided into five levels:

1. Ownership models define who owns the device and set the context for responsibilities.
2. Management models classify the technical tools used to control device behavior and protect data.
3. Access levels reflect how deeply a device can interact with corporate resources.
4. Policy enforcement indicates the strength of security policies applied.

https://doi.org/10.36690/ITSC ISBN 978-9916-9320-4-9 (pdf)

5. Risk profiles are dynamic and reflect the real-time posture of each device based on security assessments.

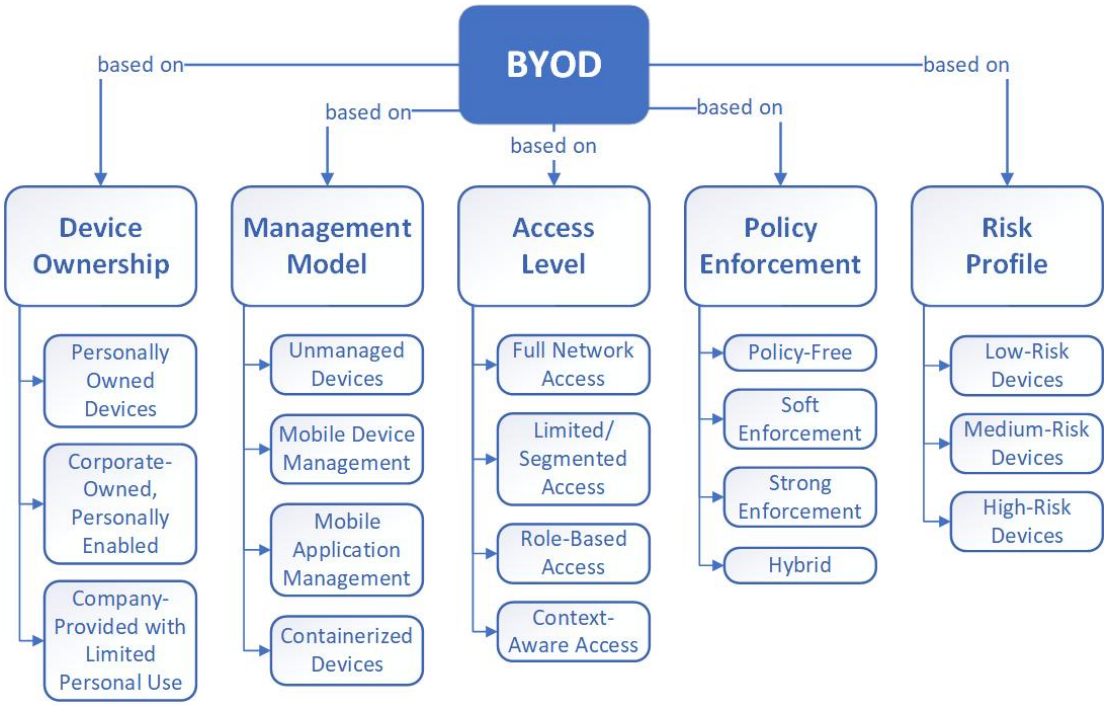

Figure 3.1. Bring your own device classification hierarchical scheme
Source: systematized by the authors

2. Bring Your Own Device Security Threats Analysis. The adoption of BYOD in corporate environments presents a complex, multi-dimensional challenge that requires a coordinated approach involving technology, policy development, and user behavior management (Figure 3.2). While technological advancements – particularly in areas like machine learning – have improved threat detection and response, the effectiveness of BYOD security still heavily depends on addressing human and organizational factors through well-defined policies and continuous user education.

One of the most pressing concerns in BYOD settings is the vulnerability to malware and malicious applications. Mobile devices are increasingly targeted by trojans, spyware, ransomware, and other threats tailored to exploit mobile platforms. This risk is significantly elevated when users sideload applications from untrusted sources, potentially introducing harmful software that can compromise both the personal device and the broader corporate network.

In addition to malware, BYOD environments are exposed to various network security threats. Devices that connect to public or unsecured Wi-Fi

https://doi.org/10.36690/ITSC
ISBN 978-9916-9320-4-9 (pdf)

networks are particularly susceptible to man-in-the-middle attacks, where communications can be intercepted and manipulated. DNS poisoning is another critical threat, capable of redirecting traffic to malicious servers without user awareness. Compromised devices may also be used for unauthorized network scanning and reconnaissance, revealing exploitable corporate infrastructure vulnerabilities.

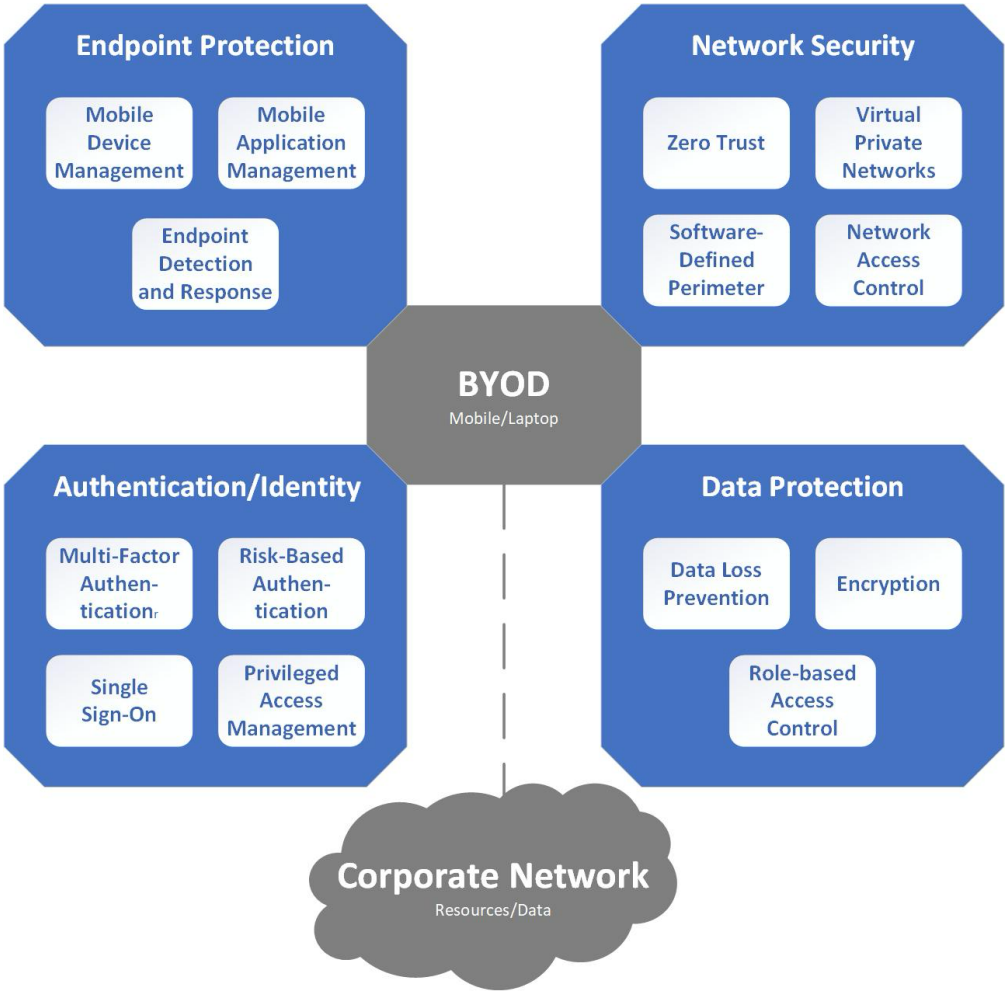

Figure 3.2. Diagram of the bring your own device security solutions architecture

Source: systematized by the authors

Authentication and access control represent further weak points in BYOD security. Inadequate password policies, weak biometric protections, and poorly implemented authentication mechanisms can create easy entry points for attackers. Once access is gained, adversaries may hijack active sessions using stolen authentication tokens or escalate privileges to reach sensitive systems and data. Identity spoofing also poses a serious risk,

https://doi.org/10.36690/ITSC
ISBN 978-9916-9320-4-9 (pdf)

enabling attackers to masquerade as legitimate users or devices and evade detection.

Physical security threats add another layer of complexity to BYOD risk management. Lost or stolen devices, especially those lacking encryption, can lead to significant data breaches. Users are also vulnerable to low-tech threats like shoulder surfing, where nearby attackers observe and record sensitive information. Moreover, using untrusted USB ports or public charging stations can facilitate malicious code injection, while social engineering tactics may deceive users into unintentionally exposing confidential information or granting unauthorized access. These diverse risks underscore the need for comprehensive, multi-layered BYOD security strategies.

3. Risk Assessment Model. To develop an effective and adaptive security strategy for BYOD environments, organizations must first understand and quantify the risks associated with allowing personal devices to access corporate resources. A systematic risk assessment enables security teams to prioritize mitigation efforts based on the severity and likelihood of various threats. One widely accepted approach involves using a quantitative risk model that incorporates multiple factors such as threat probability, impact severity, and vulnerability exposure. This allows for a structured evaluation of overall BYOD-related risk and supports informed decision-making regarding resource allocation, policy adjustments, and technological safeguards.

The proposed risk assessment model evaluates the overall risk associated with BYOD implementations by summing the risk contributions of each identified threat. Each threat is assessed individually based on three primary dimensions: the probability of occurrence, the impact severity if the threat materializes, and the organization's level of vulnerability to that specific threat. This structured approach provides a comprehensive view of the threat landscape and highlights which areas require immediate attention.

The equation for calculating the overall BYOD risk is as follows:

$$R = \sum_{i=1}^{n} P(T_i) \cdot I(T_i) \cdot V(T_i), \qquad (3.1)$$

where T_i is a threat I, representing each threat identified in the assessment; $P(T_i)$ is a probability of threat I occurring, usually expressed as a value between 0 (no chance) and 1 (certainty); $I(T_i)$ is an impact severity of threat I, often rated on a scale (e.g., 1–5 or 1–10) depending on the potential damage to confidentiality, integrity, and availability of corporate resources; $V(T_i)$ is a vulnerability level to threat I, representing how exposed the organization is to this threat (e.g., due to lack of controls or unpatched systems); n is the total number of identified threats relevant to the BYOD environment.

https://doi.org/10.36690/ITSC ISBN 978-9916-9320-4-9 (pdf)

This formula enables organizations to compute a numerical risk value that reflects the aggregate security posture of their BYOD implementation. Higher relative risk values indicate greater overall risk and the need for more urgent or extensive security interventions. The model can also be adapted over time as new threats emerge or as improvements in policy and technology reduce the probability, impact, or vulnerability associated with existing risks.

4. Multi-Factor Authentication Security Model. Authentication is a critical component of any security strategy, especially in BYOD environments where various devices and contexts make identity verification more complex. Traditional single-factor authentication methods, such as passwords, are increasingly inadequate due to their susceptibility to guessing, theft, or phishing. MFA enhances security by requiring users to present two or more independent credentials – typically combining something they know (e.g., a password), something they have (e.g., a smartphone or security token), and something they are (e.g., biometric data).

To quantify the effectiveness of MFA implementations, the MFA security model provides a mathematical representation of the cumulative security strength achieved by combining multiple authentication factors. The model considers the probability that each factor could be compromised and calculates the likelihood that all aspects could be simultaneously defeated.

The goal is to determine the authentication strength is a value between 0 and 1 that reflects the system's resilience against unauthorized access:

$$AS = 1 - \prod_{i=1}^{k}(1 - S_i), \qquad (3.2)$$

where S_i is the security strength of authentication factor i, expressed as a probability between 0 and 1 (exclusive), representing the chance that this factor alone would prevent unauthorized access; k is the number of independent authentication factors used.

The combined authentication strength represents the probability that the system will successfully block unauthorized access attempts. This formula operates on the principle that the probability of all factors failing simultaneously decreases as more strong and independent factors are introduced. As k increases, and assuming reasonably high values of S_i, the product $\prod(1 - S_i)$ becomes smaller, making the value of AS approach 1.

In other words, the more secure and diverse the authentication factors, the closer the system gets to maximum authentication strength.

This model is beneficial for organizations assessing or designing MFA

https://doi.org/10.36690/ITSC ISBN 978-9916-9320-4-9 (pdf)

configurations. By assigning realistic values to each factor's strength, security teams can simulate different combinations and determine whether the current or proposed authentication scheme meets the required security thresholds. It also provides a foundation for comparing traditional two-factor authentication setups with more advanced, context-aware, or risk-based MFA implementations.

5. Zero Trust Network Access Control Model. In modern BYOD environments, traditional perimeter-based security models are no longer sufficient to protect corporate resources. Devices and users now frequently operate outside the corporate firewall, increasing the risk of unauthorized access and lateral threat movement. To address these challenges, the ZT architecture has emerged as a leading security paradigm [14]. Its central principle – "never trust, always verify" – mandates continuous evaluation of users, devices, and contextual information before granting access to resources, regardless of whether the request originates inside or outside the network.

The ZT network access control model formally represents how access decisions are made in such an architecture. Rather than relying solely on user identity or network location, this model evaluates the user's trustworthiness in context and enforces policy-driven access rules. The decision to allow or deny access is based on a combination of a dynamically calculated trust score, predefined resource-specific thresholds, and a contextual policy evaluation that assesses the user's device, behavior, location, and access time. The defining the access decision function is as follows:

$$AD(u,r,c) = \begin{cases} \text{ALLOW} & \text{if Trust}(u,c) \geq T(r) \\ & \wedge \text{Policy}(u,r,c) = \text{TRUE}, \\ \text{DENY} & \text{otherwise}, \end{cases} \qquad (3.3)$$

where u is the user identity, representing the authenticated user requesting access; r is the requested resource, such as a file, application, or internal service; c is the contextual attributes, including device compliance status, location, time of access, and behavioral patterns; $Trust(u,c)$ *is a calculated trust score for the user under the given context, derived from factors such as device health, login history, and behavioral risk indicators;* $T(r)$ *is the required trust threshold for accessing resource r, defined based on the sensitivity or criticality of the resource;* $Policy(u,r,c)$ *a boolean function evaluates whether the user, resource, and context meet specific access policies (e.g., device must be encrypted, login must occur during business hours).*

This model ensures that access is only granted when both trust and policy conditions are satisfied, offering a layered and adaptive defense mechanism. For instance, a user with high trust may still be denied access if their device is non-compliant or if the access request violates organizational

https://doi.org/10.36690/ITSC ISBN 978-9916-9320-4-9 (pdf)

policy. Conversely, a lower-trust user may be granted limited or conditional access depending on contextual risk and resource sensitivity.

This model enables granular control over resource access in a BYOD setting by integrating real-time trust assessment with dynamic policy enforcement. It reduces reliance on static credentials and network location, helping organizations minimize risk, prevent insider threats, and enforce regulatory and security standards compliance.

6. Encryption Security Model. Protecting sensitive corporate data across various devices, networks, and applications in BYOD environments is a fundamental security requirement. Encryption is central to ensuring data confidentiality and integrity, both at rest and in transit. However, the effectiveness of encryption is not determined solely by key length or algorithm strength. It also depends on resistance to cryptanalytic attacks and the secure implementation of encryption mechanisms on various platforms, including potentially insecure personal devices.

The encryption security model presented here quantitatively assesses the overall strength of an encryption scheme used in a BYOD context. This model considers three primary components: the key space size (a proxy for brute-force resistance), the probability of successful cryptanalysis, and the likelihood of exploited implementation vulnerabilities (e.g., due to poor coding practices or insecure hardware environments). By combining these factors into a single metric, the model helps security professionals evaluate the valid Data Protection Level (DPL) provided by a given encryption strategy:

$$DPL = f(K, A, I) = \log_2 K \left(1 - P(A)\right)\left(1 - P(I)\right), \quad (3.4)$$

where K is the key space size, representing the total number of possible keys (e.g., for a 256-bit key, $K = 2^{256}$); the logarithm base 2 reflects the adequate key strength in bits; $P(A)$ is the probability of a successful cryptanalytic attack, such as differential or linear cryptanalysis; this reflects the theoretical weaknesses of the encryption algorithm; $P(I)$ is the probability of implementation vulnerability exploitation, accounting for risks from insecure libraries, flawed code, or poorly protected encryption keys; $f(K, A, I)$ is the combined security function, yielding the DPL as a weighted, risk-adjusted metric.

The product $\left(1 - P(A)\right)\left(1 - P(I)\right)$ serves to discount the theoretical key strength by the practical risks posed by known attack vectors and implementation flaws. A high DPL value indicates strong resistance to theoretical and practical attacks. At the same time, a lower DPL suggests that encryption may not adequately protect sensitive data – regardless of the nominal key size.

https://doi.org/10.36690/ITSC ISBN 978-9916-9320-4-9 (pdf)

This model is particularly valuable in the BYOD context, where encryption solutions may be deployed inconsistently across devices with varying levels of security hardening. It encourages organizations to go beyond basic key length requirements and consider the full lifecycle and environment of cryptographic implementation – from algorithm selection to software and hardware integration – ultimately leading to more robust data protection across diverse BYOD deployments.

7. Network Segmentation Security Model. In BYOD-enabled corporate environments, effective network segmentation is essential to limit the spread of threats from compromised personal devices. Unlike traditional perimeter-focused models, modern security frameworks must assume that breaches can and will occur. The goal, therefore, is to contain potential damage by isolating sensitive systems, services, and data into controlled zones or segments. Proper segmentation prevents attackers from freely moving across the network – a tactic known as lateral movement – and ensures that a compromise in one area does not jeopardize the entire system's integrity.

To quantitatively assess the effectiveness of such segmentation strategies, the network segmentation security model introduces the concept of Containment Effectiveness (CE). This metric reflects the degree to which a network's segmentation limits the potential impact of security breaches. It considers the likelihood of lateral movement from compromised segments and the value of assets distributed across the network. A higher CE score indicates better containment and lower overall risk exposure, particularly in environments where mobile and personally owned devices pose an increased risk due to weaker endpoint controls:

$$CE = 1 - \frac{\sum_{i=1}^{m} C_i P_i}{\sum_{j=1}^{n} A_j}, \qquad (3.5)$$

where C_i is the compromise impact in segment i, representing the potential damage or data loss if that segment is breached; P_i is the probability of lateral movement into segment i from a compromised node or device; A_j is the asset value in segment j, representing data sensitivity, system criticality, or operational importance; m is the number of segments potentially affected by lateral movement; n is the total number of network segments. CE is expressed as a value between 0 and 1, with 1 indicating perfect containment (no risk of lateral compromise).

The numerator of the fraction calculates the weighted expected damage from segments that could be compromised after an initial breach. The denominator represents the total value of assets across all segments, effectively normalizing the risk about what is at stake. The subtraction from

https://doi.org/10.36690/ITSC ISBN 978-9916-9320-4-9 (pdf)

1 converts this risk measure into a CE score – i.e., how much of the network remains protected in the face of potential breaches.

This model provides security architects a tool to evaluate and improve segmentation strategies in real-world deployments. For example, increasing segmentation granularity, adding access controls, or reducing inter-segment connectivity can directly reduce P_i, thereby improving CE. Similarly, placing the most valuable assets in highly secure, isolated segments can reduce the potential impact C_i, further enhancing containment.

In the context of BYOD, where user-controlled devices may bypass traditional perimeter defenses, CE becomes a crucial metric for ensuring resilient network design and limiting breach scope when device security cannot be guaranteed.

8. Security Monitoring and Response Model. Rapid threat detection and timely incident response are critical to minimizing damage in a BYOD-driven corporate environment, where devices of varying trustworthiness regularly access internal resources. Traditional security monitoring systems often struggle to balance detection speed with resource constraints, leading to either false positives from overly aggressive detection or delayed responses due to conservative alerting. The security monitoring and response model provides a quantitative framework for optimizing this balance by minimizing the total cost associated with detection and delayed response.

The core objective of this model is to optimize Detection Time (DTO) across multiple threat scenarios, ensuring that security teams detect incidents early enough to mitigate their consequences without overwhelming systems with noise. It incorporates two cost dimensions: (a) the cost incurred from delays in detecting a threat and (b) failing to respond to a threat within an acceptable timeframe. This allows organizations to assess trade-offs and fine-tune their monitoring infrastructure for better responsiveness and cost-effectiveness:

$$DTO = \arg\min \sum_{i=1}^{t} (C_d t_i + C_r \max(0, t_i - t_r)), \qquad (3.6)$$

where C_d is the cost of detection delay per unit of time, representing the operational or security impact of not detecting a threat promptly; C_r is the cost of response delay per unit time, applicable only when the detection time t_i exceeds the response threshold; t_i is the time to detect a threat i, i.e., how long the system or team takes to identify the incident; t_r is the response time threshold, the maximum acceptable delay before the response becomes disproportionately costly; t is the total number of threat scenarios considered in the model; arg min is the optimization function that identifies the set of detection times t_i that minimize the overall cost function.

https://doi.org/10.36690/ITSC ISBN 978-9916-9320-4-9 (pdf)

The cost function contains two parts for each threat scenario:

1. $C_d t_i$ captures the increasing cost of delayed detection, such as greater exposure time for malware or data exfiltration.

2. $C_r \max(0, t_i - t_r)$ adds additional penalties only if detection occurs after the critical response window, modeling the potentially catastrophic impact of late remediation (e.g., ransomware encryption or data breaches).

By minimizing this total cost across all anticipated threats, the DTO model helps security teams and system architects design and calibrate detection systems (e.g., security information and event management, endpoint detection and response, and intrusion detection system) to achieve a practical, cost-efficient balance between speed and accuracy.

This model becomes essential in BYOD environments where uncontrolled endpoints can introduce unpredictable risks. It supports the configuration of adaptive detection thresholds, prioritization of alerts, and resource allocation for response teams – all tailored to ensure timely and effective threat management without incurring unnecessary costs.

9. User Behavior Analytics Model. In BYOD environments, where traditional perimeter-based security is weakened by the diversity and autonomy of personal devices, identifying insider threats, compromised accounts, or policy violations becomes especially challenging. Conventional access controls often cannot detect subtle indicators of misuse or compromise. This is where UBA becomes a powerful tool – profiling regular user activity and detecting deviations that may indicate malicious intent or account compromise.

Using an anomaly score, the UBA model introduces a mathematical approach to quantify such deviations. This score helps security systems determine whether a user's behavior at a given time significantly deviates from their historical norms. It relies on a statistical comparison of behavioral features – such as login times, file access patterns, or application usage – against a user's baseline. When the aggregate deviation exceeds a defined threshold, the system can trigger alerts, enforce step-up authentication, or isolate the user session:

$$AS(u,t) = \sum_{i=1}^{n} w_i \frac{|x_i(u,t) - \mu_i|}{\sigma_i}, \qquad (3.7)$$

where u is the specific user being monitored; t is the time of observation; $x_i(u,t)$ is the observed value of behavioral feature i for user u at time t; μ_i is the mean (average) value of feature i based on the user's historical behavior; σ_i is the standard deviation of feature i, reflecting how much variability the user typically exhibits for that behavior; w_i is the weight assigned to feature i, indicating its relative importance or sensitivity in the risk model; n is the number of behavioral features being evaluated.

https://doi.org/10.36690/ITSC ISBN 978-9916-9320-4-9 (pdf)

Each term in the sum quantifies how much the user's current behavior deviates from their norm for a particular feature, scaled by the variability of that feature and its assigned weight. Features with high sensitivity or low historical variance (e.g., logins from unusual geolocations) will contribute more significantly to the total anomaly score. This allows the model to adapt to individual behavioral baselines and reduce false positives.

This model is especially valuable in BYOD contexts, where security controls may be inconsistent and users operate in diverse environments. It can detect anomalous behaviors that static policies would miss – such as a user accessing corporate resources at an unusual hour, from a new location, or with a device exhibiting a previously unseen pattern. Integrating this anomaly scoring model into a broader security information and event management system enhances threat detection and supports more dynamic, behavior-aware access control.

10. Composite Security Score Model. This version combines the output of all individual models into a unified risk-based security score, which can be used to assess the overall security posture of a BYOD-enabled system in real-time.

$$\begin{aligned} CSS = {} & \upsilon_1(1-R) + \\ & + \upsilon_2 \cdot AS_{\text{MFA}} + \\ & + \upsilon_3 \cdot \overline{AD} + \\ & + \upsilon_4 \cdot DPL + \\ & + \upsilon_5 \cdot CE + \\ & + \upsilon_6 \cdot \overline{DTO} + \\ & + \upsilon_7 \cdot (1 - AS_{\text{UBA}}), \end{aligned} \tag{3.8}$$

where R is the overall BYOD risk from (1), inverted to reflect "security level"; AS_{MFA} is the authentication strength from (2); $\overline{AD}$ is the normalized access decision value, e.g., 1 for allow, 0 for deny from (3); DPL is the data protection level from encryption model from (4); CE is the containment effectiveness from network segmentation from (5); $\overline{DTO}$ is the normalized inverse of detection cost from (6), lower cost equals as higher score; AS_{UBA} is the anomaly score from (7), inverted to reflect "normality;" υ_i is the weights representing the relative importance of each domain ($\Sigma\upsilon_i = 1$).

This formula yields a score between 0 and 1, where values close to 1 represent strong security across all BYOD dimensions. It's useful for continuous risk scoring and dynamic policy enforcement.

The integrated BYOD security architecture illustrated in the diagram brings together seven critical models that work in tandem to provide comprehensive protection. The system begins with the Risk Assessment Model, which quantifies potential threats based on their likelihood, impact,

https://doi.org/10.36690/ITSC ISBN 978-9916-9320-4-9 (pdf)

and system vulnerability. This risk profile drives decisions in other layers, including MFA and ZT network access control, ensuring that users and devices are assessed appropriately based on context and potential danger (Figure 3.3). The MFA model strengthens authentication by requiring multiple verification factors, and its output directly affects trust scores used in access control decisions.

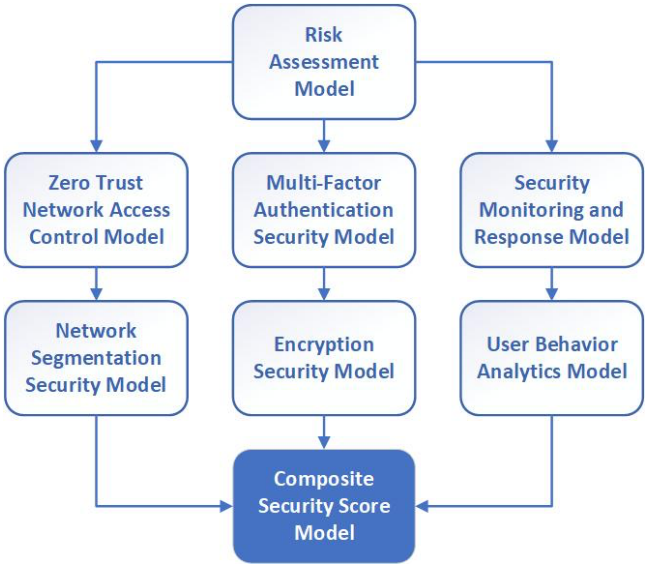

Figure 3.3. Model interaction diagram

Source: systematized by the authors

The ZT model plays a central role by continuously verifying user, device, and contextual integrity before allowing access to network resources. It draws on inputs from the risk model, MFA, and UBA to determine whether access should be granted. Once access is allowed, encryption ensures that data is protected at rest and in transit, while Network Segmentation isolates systems to prevent lateral movement by potential intruders. These technical controls limit the scope of a breach, and risk levels and access decisions influence their configuration.

The final layer, security monitoring and response, minimizes detection and response times by analyzing data from encryption, segmentation, and behavioral anomalies. The UBA model detects deviations from established behavior patterns and feeds insights into monitoring and access control systems, enabling adaptive and proactive responses. The system is inherently cyclical and self-adjusting: real-time data flows between layers to ensure that each component evolves based on ongoing threats, user behavior, and policy enforcement outcomes. This layered approach embodies a defense-in-depth

https://doi.org/10.36690/ITSC
ISBN 978-9916-9320-4-9 (pdf)

strategy that strengthens organizational resilience in dynamic BYOD environments.

11. Weighted Security Effectiveness Aggregate Model. The model is a comprehensive framework designed to evaluate the overall security posture of BYOD environments through a normalized, weighted combination of seven critical security dimensions. This model addresses the fundamental challenge of translating multiple, disparate security metrics into a single, actionable security effectiveness score:

$$E = \sum_{i=1}^{7} v_i \cdot S_i \cdot I_i, \qquad (3.9)$$

where S_i is a security component (see Table 1); I_i is the interaction factor.

Table 3.1. Individual security components

Heading level	Component Definitions
S_1	Risk Assessment Score
S_2	Authentication Strength
S_3	ZT Access Control Effectiveness
S_4	Encryption Protection Level
S_5	Network Segmentation Containment
S_6	Monitoring Response Effectiveness
S_7	Behavioral Anomaly Detection Score

Source: systematized by the authors

The model operates on the principle that security effectiveness is not merely the sum of individual security controls but rather an emergent property arising from multiple security layers' synergistic interaction. The model recognizes that different security components contribute varying levels of protection and that these contributions must be weighted according to their relative importance in the overall security architecture. This model employs a weighted linear aggregation approach enhanced with interaction factors to capture the multiplicative effects of security controls working in concert. This approach ensures that:

– organizations with strong performance across all security dimensions receive higher scores than those with uneven security profiles;
– security interdependencies are properly accounted for through interaction coefficients;
– the final score remains interpretable and comparable across different organizational contexts.

Each security component is normalized to a [0,1] scale, ensuring that components with different natural ranges (e.g., encryption key lengths vs.

https://doi.org/10.36690/ITSC ISBN 978-9916-9320-4-9 (pdf)

detection times) contribute proportionally to the final score. This normalization prevents any single metric from dominating the aggregate score due to scale differences.

The weight assignments reflect industry best practices and empirical evidence regarding the relative impact of different security controls on overall risk reduction. The weights can be adjusted based on organizational risk tolerance, regulatory requirements, industry-specific threat landscapes, and historical incident patterns.

The interaction factor captures the reality that security controls often exhibit positive correlation effects. For example, strong authentication controls enhance the effectiveness of ZT policies, while comprehensive monitoring amplifies the value of behavioral analytics. This multiplicative enhancement prevents the model from treating security controls as independent variables.

12. Dynamic Security Resilience Aggregate Model. The model represents a paradigm shift from traditional static security assessment to a dynamic, adaptive framework emphasizing organizational resilience and learning capabilities. Unlike conventional models that measure security at discrete points in time, the dynamic model continuously evaluates how security systems evolve, adapt, and improve in response to changing threat landscapes and operational experiences:

$$D = \Delta T \cdot CF \sum_{i=1}^{7} S_i^{\beta_i} \cdot R_i, \qquad (3.10)$$

where ΔT is the time decay factor; CF is the confidence factor; β_i are the power coefficients; R_i are the resilience factors (Table 3.2).

Table 3.2. Individual resilience factors

Heading level	Factor Definitions
R_1	Risk Adaptation Factor
R_2	Authentication Resilience
R_3	ZT Adaptation
R_4	Cryptographic Agility
R_5	Network Elasticity
R_6	Response Maturity
R_7	Behavioral Learning Rate

Source: developed by the authors

https://doi.org/10.36690/ITSC ISBN 978-9916-9320-4-9 (pdf)

The dynamic model is built on the fundamental premise that security effectiveness is not a static property but a dynamic capability that emerges from an organization's ability to learn, adapt, and respond to security challenges over time. The model recognizes that in rapidly evolving threat environments, the capacity for continuous improvement and adaptive response often matters more than achieving perfect security at any single moment.

The model incorporates resilience factors R_i that measure each security component's ability to maintain effectiveness under stress, recover from incidents, and improve through experience. This approach acknowledges that security breaches are inevitable and focuses on how quickly and effectively systems can detect, respond to, and learn from security events. The dynamic model employs power functions $S_i^{\beta_i}$ to capture the non-linear relationships inherent in security systems, where incremental improvements in critical areas can yield disproportionate benefits. This mathematical structure reflects that security often exhibits threshold effects – certain minimum levels must be achieved before meaningful protection occurs.

The time decay factor ΔT ensures that the model remains current and relevant by reducing the influence of outdated assessments. This temporal weighting recognizes that security postures can change rapidly and that recent performance generally indicates current capabilities more than historical achievements. Each resilience factor incorporates learning algorithms that track improvement rates, adaptation speeds, and maturity progression. This allows the model to reward organizations that demonstrate continuous security improvement and penalize those that remain static despite changing threat conditions.

The confidence factor addresses the reality that security metrics often involve uncertainty and incomplete information. By incorporating data quality and sample size considerations, the model provides more reliable assessments when data is robust and appropriately conservative estimates when information is limited.

13. Layered Security Decision Framework. This framework can organize the seven models into interdependent functional layers, forming a hierarchical model for policy decisions or threat response:

1. Risk layer:

– Input: R is the risk score from (1).
– Output: determines baseline risk level: low, medium, or high.

2. Identity and access layer:

– Inputs: AS_{MFA} from (2) and $AD(u, r, c)$ from (3).

https://doi.org/10.36690/ITSC
ISBN 978-9916-9320-4-9 (pdf)

– Output: access granted or restricted based on strength of authentication and trust context.

3. Data protection layer:

– Inputs: DPL from (4) and CE from (5).
– Output: determines whether data access requires isolation, encryption, or redirection.

4. Monitoring and response layer:

– Inputs: DTO from (6) and AS_{UBA} from (7).
– Output: real-time alerts, session termination, or further investigation if anomaly score or detection cost crosses thresholds.

This model doesn't produce a single score but instead guides actions (access, isolation, escalation) based on evaluations at each layer. It's ideal for implementation in security orchestration or access policy engines.

Conclusions. The study and modeling of BYOD security presented herein reveal the complexity and multidimensionality of protecting corporate environments in the context of personal device usage. The proposed aggregate model, composed of seven foundational sub-models – including risk assessment, MFA, ZT access control, encryption, network segmentation, security monitoring, and UBA – demonstrates that a layered and interconnected security architecture is essential. Each model contributes specific functions, while their integration ensures adaptability, redundancy, and responsiveness to dynamic threats.

Our analysis highlights the central role of risk-based decision-making, context-aware authentication, and continuous trust evaluation, all of which maintain the security posture of a BYOD ecosystem. Notably, UBA and real-time monitoring enable the system to adjust dynamically to evolving threat patterns, while network segmentation and encryption act as core containment and protection mechanisms. Formal mathematical models provide a basis for quantifying security properties such as authentication strength, detection latency, and DPLs, offering a structured framework for implementation and evaluation. The proposed architecture provides a robust and adaptable framework for mitigating BYOD-associated risks. However, the effectiveness of such a system depends not only on technical sophistication but also on policy enforcement, user awareness, and ongoing evaluation of evolving threats and technologies.

Future research should focus on validating the theoretical models through empirical studies, using real-world BYOD deployments in corporate environments to refine probability, impact, and behavior variables. Incorporating cost-benefit analyses into the security models, especially in the

https://doi.org/10.36690/ITSC ISBN 978-9916-9320-4-9 (pdf)

Detection Time Optimization framework, could aid organizations in balancing security investments with operational efficiency.

Funding. The author declare that no financial support was received for the research, authorship, and/or publication of this article.

Conflict of interest. The author declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Generative AI statement. The author declare that no Generative AI was used in the creation of this manuscript.

Publisher's note. All claims expressed in this article are solely those of the author and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References:

1. Kipchuk, F., Sokolov, V., Skladannyi, P., & Ageyev, D. (2021). Assessing Approaches of it Infrastructure Audit. In 2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T), 213–217. IEEE. https://doi.org/10.1109/picst54195.2021.9772181
2. Iavich, M., Kovalchuk, O., Gnatyuk, S., Khavikova, Y., & Sokolov, V. (2024) Classical and Post-Quantum Encryption for GDPR. In Classic, Quantum, and Post-Quantum Cryptography, vol. 3829, 70–78.
3. Marusenko, R., Sokolov, V., & Buriachok, V. (2020). Experimental Evaluation Of Phishing Attack On High School Students. In Advances in Intelligent Systems and Computing: Advances in Computer Science for Engineering and Education III, vol. 1247, 668–680. Springer International Publishing. https://doi.org/10.1007/978-3-030-55506-1_59
4. Wang, Y., Noteboom, C., El-Gayar, O., & Ratchford, M. (2021). BYOD Security Issues: a Systematic Literature Review. Inf. Secur. J. Glob. Perspect., 31, 253–273. https://doi.org/10.1080/19393555.2021.1923873
5. Bahaddad, A., Alghamdi, A., & Almarhabi, K. (2022). Security Management of BYOD and Cloud Environment in Saudi Arabia. Alexandria Eng. J., 63, 103–114. https://doi.org/10.1016/j.aej.2022.07.031
6. Downer, K., & Bhattacharya, M. (2015). BYOD Security: A New Business Challenge. 2015 IEEE International Conference on Smart City/SocialCom/SustainCom (SmartCity), 1128–1133. https://doi.org/10.1109/SmartCity.2015.221
7. Kiah, M., Norman, A., & Palanisamy, R. (2020). Compliance With Bring Your Own Device Security Policies In Organizations: A Systematic Literature Review. Comput. Secur., 98, 101998. https://doi.org/10.1016/j.cose.2020.101998
8. Wani, T., Smolenaers, F., Mendoza, A., & Gray, K. (2022). Status Of Bring-Your-Own-Device (Byod) Security Practices In Australian Hospitals – A National Survey. Health Polic. Technol., 1(3), 100627. https://doi.org/10.1016/j.hlpt.2022.100627

ISBN 978-9916-9320-4-9 (pdf)

9. Wani, T. A., Mendoza, A., & Gray, K. (2020). Hospital Bring-Your-Own-Device Security Challenges And Solutions: Systematic Review Of Gray Literature. JMIR mHealth and uHealth, 8(6), e18175. https://doi.org/10.2196/18175
10. Lian, J. (2020). Understanding Cloud-Based Byod Information Security Protection Behaviour In Smart Business: In Perspective Of Perceived Value. Enterp. Inf. Syst., 15, 1216–1237. https://doi.org/10.1080/17517575.2020.1791966
11. Olson, B., Blessner, P., Zahadat, N., & Blackburn, T. (2015). BYOD Security Engineering: A Framework And Its Analysis. Comput. Secur., 55, 81–99. https://doi.org/10.1016/j.cose.2015.06.011
12. Bhattacharya, M., & Downer, K. (2022). BYOD Security: A Study Of Human Dimensions. Inform., 9, 16. https://doi.org/10.3390/informatics9010016
13. Norman, A., Eke, C., & Mulenga, M. (2023). Machine Learning Approach For Detecting And Combating Bring Your Own Device (Byod) Security Threats And Attacks: A Systematic Mapping Review. Artif. Intell. Rev., 56, 8815–8858. https://doi.org/10.1007/s10462-022-10382-3
14. Syrotynskyi, R., Tyshyk, I., Kochan, O., Sokolov, V., & Skladannyi, P. (2024). Methodology Of Network Infrastructure Analysis As Part Of Migration To Zero-Trust Architecture. In Cyber Security and Data Protection, vol. 3800, 97–105.

https://doi.org/10.36690/ITSC ISBN 978-9916-9320-4-9 (pdf)