Methodology for local corporate network security based on a multi-level approach

Valerii Dudykevych[1,*,†], Halyna Mykytyn[1,†] and Taras Murak[1,†]

[1]Lviv Polytechnic National University, Stepan Bandera Str.,12, Lviv, 79000, Ukraine

Abstract

The strategy of the EU Agency for Cybersecurity (ENISA) and Ukraine's Cybersecurity Strategy are aimed at developing and practically implementing new approaches, methodologies, and technologies in addressing cybersecurity challenges within the infrastructure of society, particularly in ensuring data confidentiality in corporate networks. An analytical review has been conducted on well-known methods and technologies for corporate network security in the following areas: secure data exchange and storage; enhancement of security models, security tools, and information protection systems; and the application of machine learning methods and neural network technologies for anomaly detection in corporate networks. A methodology for local corporate network (LCN) security based on a multi-level approach has been presented. This includes the seven-layer OSI model, the "defense-in-depth" model, and an integrated LCN security system within the "threat–security technologies" framework. This methodology is universal for different network topologies and enables the design of information security systems at each OSI layer in accordance with regulatory requirements. Software has been developed for cryptographic protection of information at the OSI transport network level based on the symmetric block algorithm AES-256, using the Python programming language. This is practically implemented through the OpenVPN protocol and TLS transport layer technology, ensuring a high level of information confidentiality in local corporate networks.

Keywords

corporate network, security methodology, multi-level approach, OSI reference model, "defense-in-depth" model, integrated security system, random and targeted threats, transport layer, data encryption

1. Introduction

Effective cooperation between Ukraine and the European Union in the field of cybersecurity, particularly through the interaction of the State Service of Special Communications and Information Protection of Ukraine, the National Cybersecurity Coordination Center, and the EU Agency for Cybersecurity (ENISA), serves as a foundation for developing Ukraine-EU cyber dialogues. These efforts are specifically focused on comprehensive counteraction to cyber threats and ensuring a high level of cyber resilience and protection [1, 2]. A crucial aspect is the implementation of the EU NIS 2 Directive [3], which applies to critical infrastructure companies and systems in sectors such as energy, transport, digital infrastructure, ICT service management, environmental protection, healthcare, and space. Compliance with the DSTU ISO/IEC 27001:2023 standard (Information Security, Cybersecurity, and Privacy Protection – Information Security Management Systems – Requirements, ISO/IEC 27001:2022, IDT) introduces a structured approach to cybersecurity. This helps Ukrainian companies operating in the EU market meet the NIS 2 requirements regarding incident notification, corporate security policies, business continuity planning, responsible partnership selection, multi-factor authentication, and cybersecurity training. The progressive trends of the international cyberspace serve as a foundation for developing Ukraine-EU cyber dialogues aimed at creating a universal cybersecurity platform. This platform is designed to counter threats in the context of hybrid warfare, establish mechanisms for security implementation,

CH&CMiGIN'25: Fourth International Conference on Cyber Hygiene & Conflict Management in Global Information Networks, June 20–22, 2025, Kyiv, Ukraine

*Corresponding author.

†These authors contributed equally.

valerii.b.dudykevych@lpnu.ua (V. Dudykevych); halyna.v.mykytyn@lpnu.ua (H. Mykytyn); taras.murak.mkbst.2024@lpnu.ua (T. Murak)

0000-0001-8827-9920 (V. Dudykevych); 0000-0003-4275-8285 (H. Mykytyn); 0009-0005-7588-9945 (T. Murak)

and integrate cutting-edge security technologies, including new approaches to securing local corporate networks.

In the study [4], a comprehensive security system for information networks is considered as one of the levels of information technologies based on the "object–threat–protection" concept. Within the framework of comprehensive corporate network security, study [5] examines network security mechanisms and corresponding tools. Article [6] analyzes known threats and vulnerabilities in information networks, methods of counteracting them, and proposes effective approaches to ensuring the security of information and telecommunication networks using efficient vulnerability detection methods. The enhancement of information protection systems in computer networks has been further developed through the application of network firewalls such as "Fortigate" and "Cisco ASA" [7]. Network security trends based on the OSI model have been explored in various works. Study [8] investigates major attacks on the data link layer of computer networks and methods to neutralize them using Cisco network equipment tools. Research in [9, 10] examines threats to computer networks at the physical, data link, network, transport, and application layers, analyzing protection methods and technologies. Study [11] provides a brief analysis of the use of machine learning methods and neural network technologies for anomaly detection in corporate networks. Based on this analysis, a neural network-based method utilizing LSTM and FFN architectures is proposed, along with an algorithmic and software implementation for detecting software and technical impacts on critical infrastructure systems in the context of cyber warfare. A comprehensive approach to the optimal selection of enterprise network security systems, based on an objective comparison of various criteria and their impact on overall security levels and protection reliability, is presented in [12]. The authors of [13] describe the most common Internet attack methods and other threats in modern computer networks, as well as highlight contemporary Internet security technologies and network intrusion detection systems. In the field of incident management and information security risk management, the work [14] examines an approach to developing a management system that ensures the necessary control measures to prevent common cyber threats in various infrastructure segments.

In the realm of network security based on the Zero Trust model (CISA, Cybersecurity and Infrastructure Security Agency), several key approaches have been proposed: A targeted traffic segmentation method that enables analysis of interactions between applications, users, and corporate network infrastructure, enhancing the detection of complex threats [15]; The "never trust, always verify" concept, which requires users to confirm their credentials for every access request, whether inside or outside the company's network perimeter [16]. Effective security segments for computer systems and networks include comprehensive protection of hardware and software, secure data exchange, and data storage security through access control technologies, data encryption, and network isolation [17]. A notable area of interest is the design of secure network architecture for manufacturing companies. Study [18] explores the application of effective security technologies, such as firewalls and IDS, to enhance system resilience. Modern network security trends encompass methods for detecting distributed network attacks, software-defined networking (SDN), and machine learning techniques [19, 20]. In the field of intrusion detection systems (IDS), a new approach based on a long short-term memory neural network (p-LSTM) has been developed, reducing false alerts and improving detection reliability [21]. Security approaches for LAN and WAN networks continue to evolve. Research has examined VPN application scenarios in corporate WAN networks [22] and proposed the use of firewalls, obfuscation technologies, and port forwarding to establish a robust security policy [23]. A novel risk assessment (RS) approach has emerged, based on risk weighting in accordance with NIST CSF and ISA/IEC 62443 standards. This approach modifies RS by introducing new risk metrics—risk, risk reduction, risk prioritization, and risk reduction prioritization—to formulate a specialized probability model for assessing risks in broadband WAN networks used in operational technology infrastructure [24]. A relevant segment in the development of secure intellectualization of society's infrastructure is the systemic security model of the Internet of Things (IoT) architecture. In this model, security technologies are deployed according to the levels of the OSI network model—physical, transport, and application—considering the impact of potential threats [25, 26]. The effective principles embedded in the organization of pseudo-random sequence generator structures [27], namely, the additive Fibonacci generator (AFG) and its modified

version (MAFG) with prime number moduli—ensure their efficient hardware implementation while meeting all statistical characteristic requirements. These generators can be utilized in cryptographic information protection devices, including ensuring the security of a local corporate network [28]. The monograph [29] presents a methodology for analyzing the quality of the validation mechanism for identified vulnerabilities in a corporate network, enhancing the effectiveness of security analysis. The efficiency of conservative information security systems and their integration into corporate environments has been thoroughly analyzed in [30], offering a multicriterial approach to system assessment. Furthermore, the design of secure services for authentication, authorization, and accounting has been addressed in [31], emphasizing the importance of identity management and controlled access within Zero Trust frameworks.

The reviewed methods and network security tools serve as the foundation for developing LCN security approaches, which are currently relevant in the context of ensuring the secure intelligentization of various societal domains.

2. Problem statement

Based on the conducted analysis, the objectives of this study are as follows: 1) Propose a multi-layered security approach for local corporate networks (LCN) based on the OSI reference model and the "defense-in-depth" model; 2) Develop a comprehensive LCN security system within the framework of the "threats – security technologies" concept; 3) Implement a software solution for cryptographic data protection at the transport layer of the OSI model using the AES-256 symmetric block encryption algorithm in Python. The goal of this article is to establish a security methodology for local corporate networks, leveraging a multi-layered approach and a comprehensive security system. Based on this methodology, a software implementation of the AES-256 encryption algorithm will be developed for OpenVPN and TLS technology, serving as an effective mechanism for information protection and ensuring a high level of data security at the transport layer.

3. Multi-layered approach in local corporate network security

3.1. Local corporate networks in societal infrastructure domains

Local corporate networks (LCNs) are widely used in various infrastructure domains of society. Their key characteristics include short-distance data transmission and high reliability in communication. Among the commonly adopted network topologies, hybrid topology is the most frequently implemented in LCNs due to its numerous advantages: structural flexibility; enhanced reliability and fault tolerance; scalability; segmentation and high security levels; efficiency and high-speed data exchange.

Key Characteristics of Local Corporate Networks (LCNs):

1. Location: LCNs cover a limited geographical area to ensure communication between offices and branches.

2. Size and Scale: They consist of a restricted number of computers and devices within a specific organization.

3. Data Transmission Speed: LCNs provide high-speed data transfer between connected devices, enhancing operational efficiency and information exchange.

4. Communication Technologies: Various technologies, such as Ethernet, Wi-Fi, and Bluetooth, are used to establish device connectivity.

5. Security: Effective protection measures are essential, including firewalls, antivirus software, and other security tools to prevent unauthorized access and mitigate cyber threats.

3.2. Features of Local Corporate Network (LCN) usage

These features include:

1. Data and Resource Sharing: LCNs enable shared access to information and resources within an organization, facilitating efficient data exchange among employees.

2. Centralized Management: They allow centralized control over hardware, software, and security policies, simplifying administration and ensuring network consistency.

3. Access to Shared Services: LCNs support the use of shared services such as printers, file servers, and other resources, promoting collaboration across departments.

4. Use of Specialized Equipment: They enable the deployment of specialized hardware, including servers and switches, to optimize network performance and ensure high productivity.

5. Data Security: LCNs play a crucial role in maintaining data confidentiality and integrity through security tools such as encryption, authentication, and activity monitoring.

6. Real-Time Operation Support: They facilitate real-time data exchange for critical applications, including production lines, security systems, and other essential infrastructure components.

3.3. Multilevel security approach for local corporate networks: basic OSI reference model and "defense in depth" model

To create a comprehensive security system for local corporate networks, we will consider a multilevel approach that involves applying the layered basic OSI reference model and the multilayered "defense in depth" model. This approach ensures a high level of information confidentiality.

3.4. Basic OSI reference model

Figure 1 presents the multilevel basic OSI reference model (DSTU ISO/IEC 7498-1:2004 Information Technology. Open Systems Interconnection. Basic Reference Model. Part 1: Reference Model).

Physical Layer (Ethernet cable, fiber optics, Wi-Fi, Bluetooth). The security of the physical layer is aimed at ensuring secure physical access to equipment, cables, and data transmission channels. Common threats include theft, unauthorized access to equipment, cable damage/disconnection, and signal interception. Security measures to counter threats include physical access control (electronic locks, video surveillance systems), the use of protected cables (shielded, fiber-optic), uninterruptible power supplies (UPS), and protection against power failures.

Data Link Layer (Protocols: Ethernet, PPP (Point-to-Point Protocol), MAC addresses). Ensures data transmission between adjacent nodes; Implements bit-to-packet conversion; Enables error detection and correction in the transmission medium.

Network Layer (Protocols: IPv4, IPv6, ICMP (Internet Control Message Protocol)). Handles packet routing from sender to receiver; Uses logical addressing for communication.

Transport Layer (Protocols: TCP (Transmission Control Protocol), UDP (User Datagram Protocol), TLS/SSL for encryption). Ensures reliable data exchange between network endpoints; Controls data integrity and transmission order; Manages segmentation, flow control to prevent congestion, error handling, and retransmission in case of data loss.

Session Layer (Protocols: NetBIOS, PPTP (Point-to-Point Tunneling Protocol)). Establishes, maintains, and terminates communication sessions between devices; Manages synchronization and reconnection in case of interruptions; Implements user authentication.

Presentation Layer (Formats: JPEG, MP3, GIF). Converts data into a format understandable by the recipient; Implements data encryption for secure transmission.

Application Layer (Protocols: HTTP (for web access), FTP (for file transfer), SMTP (for email); applications: web browsers, email clients, file managers). Provides interfaces and services for user interaction with network applications; Processes user requests and server responses.

3.5. "Defense in depth" model

Figure 2 presents the structure of the "Defense in Depth" model for local corporate networks [32]. The "Defense in Depth" model ensures resilience against cyber threats based on multiple security layers:

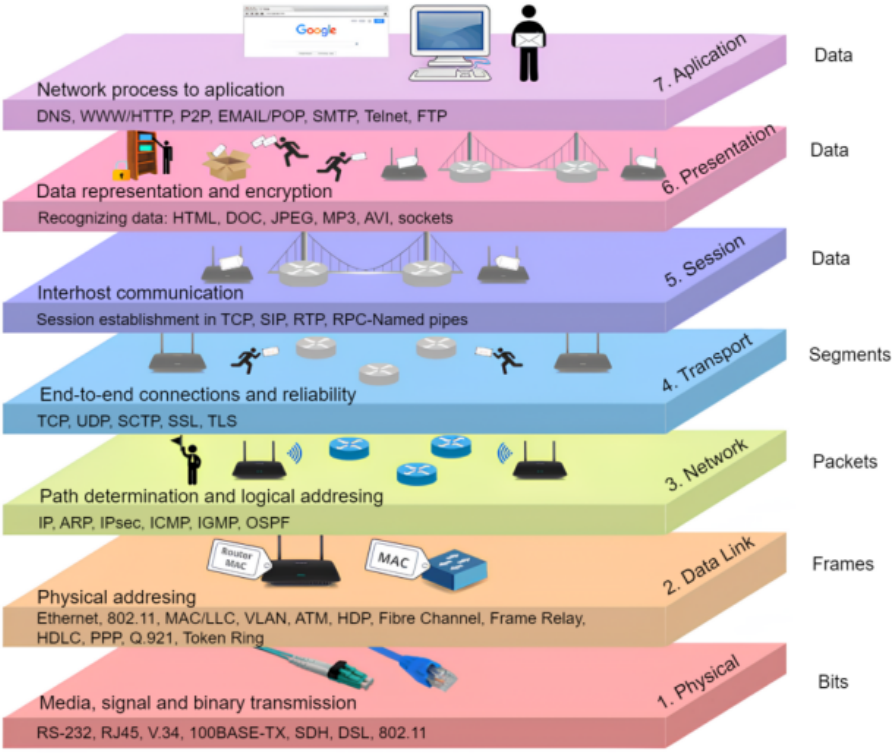

Figure 1: OSI multi-layered basic reference model.

1. Network Security Plan - 1.1 Identifying communication channels within the network of the management system; 1.2 Conducting a full audit of devices in the network; 1.3 Recording security parameters of each device; 1.4 Creating a detailed network diagram.

2. Network Partition - 2.1 Organizing the necessary infrastructure for seamless network information transmission (servers that collect and distribute data within management systems); 2.2 Managing software updates; 2.3 Implementing an antivirus server; 2.4 Deploying a web access server; 2.5 Setting up a wireless access point; 2.6 Configuring remote access.

3. Network Perimeter Protection - 3.1 Implementing firewalls to perform packet filtering; 3.2 Filtering network traffic; 3.3 Using a proxy gateway.

4. Network Segmentation: Benefits - 4.1 Prevents malicious traffic infiltration by limiting it to a single network segment; 4.2 Enhances security by making network nodes invisible to unauthorized networks; 4.3 Mitigates attacks from intruders scanning deeper network layers before selecting a target; 4.4 Prevents data leaks in case of a security breach; 4.5 Improves network performance and reduces load.

5. Enhancing Device Security - 5.1 Password management, including encryption; 5.2 Disabling unused services; 5.3 Access control; 5.4 Network Intrusion Detection Systems (NIDS); 5.5 Strong authentication.

6. Monitoring/Update - 6.1 Packet logging monitoring; 6.2 Event log monitoring; 6.3 Authentication interception; 6.4 Using Intrusion Detection Systems (IDS).

4. Comprehensive security system for local corporate networks in subject areas

The comprehensive security system for a local corporate network in a specific subject area is built based on the OSI and "Defense in Depth" models. It is deployed within the framework of the "Threats – Security Technologies" concept.

1. The OSI model: Physical.

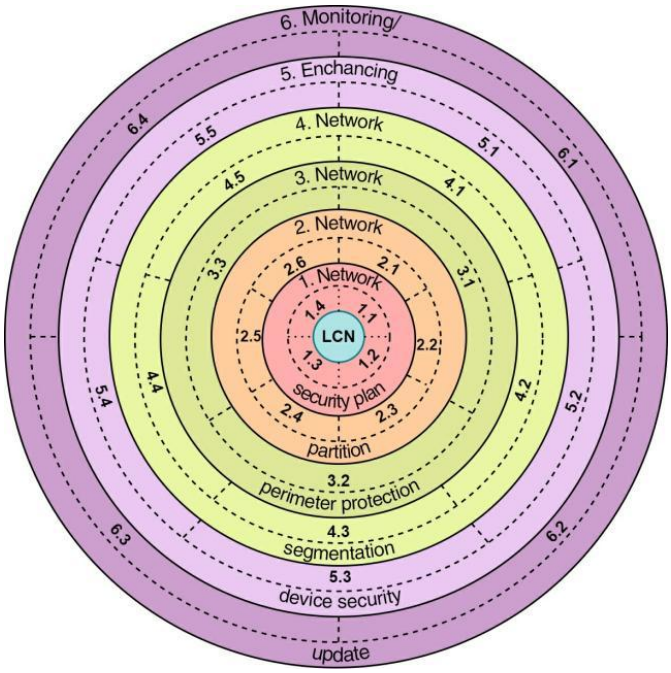

Figure 2: Multy-layered "defense-in-depth" model of local corporate networks.

In this case the possible threats are random (electromagnetic interference, damage to cables or connections, failure in the power supply) and targeted (physical intrusion attempts to gain access to equipment, attacks on cables and infrastructure, temperature attacks).

Security technologies with elements of "defense-in-depth" (hardware) include physical hardware intrusion detection mechanisms, use of secure cables and connectors, and use of controlled access to server and communication rooms

2. The OSI model: Data link.

In this case the possible threats are random (noise or interference that may lead to false perception of bits, influence of internal electrical noise band, interference in the wireless channel) and targeted (poisoning the ARP cache, DHCP attacks (DHCP Spoofing), MAC address flooding).

Security technologies with elements of "defense-in-depth" include hardware (control access to the switch ports, IEEE 802.1X Authentication (A mechanism that requires authentication of devices connecting to the network before gaining access), MAC Address Filtering: Restricts devices from connecting to the network based on their MAC address) and software(Software-Based Access Control (Using programs to configure access control policies and assign rights to interact with network ports), Dynamic ARP Inspection Software (Use programs to detect and block invalid ARP responses and prevent ARP attacks), Port Security Software (Port security policies on switches to restrict access to the network)) tools.

3. The OSI model: Network.

Random threats are IP address leakage due to configuration errors or insufficient security, routing table overflow due to a large number of requests, faulty network cards or ports. Targeted threats are IP address spoofing, man-in-the-middle attack, packet sniffing, Denial of Service (DoS) or Distributed Denial of Service (DDoS), TCP hijacking (session hijacking).

Security technologies with elements of "defense-in-depth" include hardware (Network Firewalls (Specialized hardware for filtering network traffic based on predefined security rules to block unwanted connections and protect against external threats), IPS (Intrusion Prevention Systems) (The use of hardware accelerators to effectively detect and block intrusions at the network traffic level), use of switches and routers that support various encryption protocols, VPNs, authentication and other security features) and software(Firewall systems (Software for configuring packet filtering rules at the network level to control access and block unwanted connections), IPS (Intrusion Prevention System) and IDS

(Intrusion Detection System) (Software systems for detecting and preventing network intrusions by analyzing network traffic for anomalies and intrusions), proxy servers (Software that allows you to control and filter traffic between a local network and the Internet, as well as provides security features)) tools.

4. The OSI Model: Transport.

Random threats are low throughput due to technical malfunctions, buffer overflow at the transport layer, temporary loss of connection due to anomalies in the operation of switches or routers. Targeted threats are TCP SYN/ACK Flooding attacks (SYN/ACK Flooding), UDP Flood attacks, TCP Hijacking (Session Hijacking).

Hardware security technologies include use of special hardware devices for encryption and decryption of traffic at the transport layer to help ensure data confidentiality during transmission (e.g., Thales n Shield Connect), use of specialized hardware devices to monitor network traffic and respond to potential threats at the transport layer (e.g., Cisco Firepower Next-Generation Firewall (NGFW)), use of hardware devices to control access to the network and resources at the transport layer, which allows you to manage access rights and user identification (for example, Fortinet FortiGate Next-Generation Firewall).

Software security technologies include openVPN is a software for creating VPN connections that uses TLS for encryption and transport layer protection, Transport Layer Security (TLS) / Secure Sockets Layer (SSL) (TLS/SSL software provides encryption and protection at the transport layer to ensure data confidentiality, use of IDS and IPS.

Regulatory support includes:

1. DSTU ISO/IEC 27033:2013 - Information technology. Methods of protection. Network security. Part 3. Reference network scenarios. Threats, design methods and management issues.

2.DSTU ISO/IEC 18033-1:2017 - Information technology. Methods of protection. Encryption algorithms. Part 1: General provisions.

3. DSTU ISO/IEC 15408-1:2022 - Information security, cybersecurity and privacy protection. Evaluation criteria for IT security.

4. DSTU ISO/IEC 27001:2023 - Information security, cybersecurity and privacy protection. Information security management systems. Requirements.

5. DSTU ISO/IEC 27033-7: 2023 - Information technology - Network security. Guidelines for network virtualization security.

5. Cryptographic data protection at the transport layer of the OSI model in a local corporate network based on: the OpenVPN protocol, TLS technology, and the AES-256 algorithm

To implement the proposed comprehensive security system for local corporate networks, we utilize elements of the OSI reference model and the "defense-in-depth" model within the space of effective security tools. These include the OpenVPN protocol, transport layer security (TLS) technology, and the AES-256 symmetric block encryption algorithm, collectively ensuring a high level of information confidentiality, data exchange speed, and connection security.

Among well-known VPN protocols (OpenVPN, WireGuard, IKEv2/IPSec, L2TP/IPSec, PPTP), which manage the creation and encryption of VPN connections, OpenVPN stands out as a universal solution. It is compatible with all platforms and efficiently leverages AES-256, providing a high level of cryptographic resilience when transmitting confidential data within corporate networks.

TLS technology ensures security at the transport layer of the OSI model within a local corporate network by providing user authentication, data confidentiality, and transmission integrity. The advantages of using the AES-256 symmetric block encryption algorithm include: 1) High speed – the algorithm operates efficiently on both hardware and software levels; 2) Reliable security – its structure is resistant to many types of attacks, making it one of the most secure encryption algorithms; 3) Flexibility – support for different key lengths allows for adjustable security levels based on specific needs. The

encryption algorithm is effectively used for: secure exchange of confidential data in corporate networks, secure data storage, cryptographic data protection in cloud environments and on mobile devices.

For the software implementation of data protection at the transport layer of the OSI model in a local corporate network, the Python programming language was used. It features a clear syntax, a large number of standard and third-party libraries. All of this makes the language universal.

The developed program is a specialized proxy server that can handle the most sensitive data, providing an additional layer of encryption on top of standard TLS protection. In addition to SSL, the proxy server uses AES-256 to ensure an extra level of security for confidential data such as passwords, logins, keys, tokens, etc.

The program's logic is as follows: the client connects to the proxy server via a standard TLS connection. The proxy then determines whether additional encryption is required for a specific request. If needed, the data is encrypted using AES-256 with a unique session key. The encrypted data is then transmitted through the TLS tunnel to the target server. On the server side, a similar proxy decrypts the data before passing it to the final application.

The main structure of the program code includes the following elements:

1. Importing necessary modules:

socket – for network operations (creating a server socket). threading – for handling multiple connections simultaneously. ssl – for establishing a secure connection via TLS. json – for processing JSON data. logging – for event logging. base64 – for encoding/decoding data. os – for generating random keys. cryptography.hazmat – for implementing AES-256 encryption.

2. Server parameters:

PROXY_HOST = '127.0.0.1'

PROXY_PORT = 8443

TARGET_HOST = '127.0.0.1

TARGET_PORT = 8444

The proxy server listens for connections on 127.0.0.1:8443 and forwards traffic to 127.0.0.1:8444 (acting as an intermediary between the client and the server).

3. Initializing SSL certificates to establish a secure TLS connection:

CERT_FILE = 'server.crt'

KEY_FILE = 'server.key'

4. List of sensitive data patterns that trigger additional encryption by the proxy server:

SENSITIVE_PATTERNS = ['password', 'token', 'credit', 'ssn', 'secret', 'account', 'personal', 'confidential']

5. Sensitive data encryption:

The proxy server encrypts/decrypts data using AES-256 in CBC mode and exchanges the key between the parties. The following functions are used:

def__init__(self): Generates a random key.

def encrypt(self, data): Encrypts sensitive data.

def decrypt(self, data): Decrypts data.

def get_key(self), def set_key(self, key): Handles key exchange between parties.

6. Classifying sensitive data in functions:

def__init__(self, patterns=None) - Detects sensitive data based on keywords and patterns. If suspicious keywords are found, the data is considered sensitive and encrypted before transmission and def is_sensitive(self, data) - Checks JSON data. If the input data is JSON, the server parses it into a flat dictionary and verifies all keys and values against patterns from self.patterns. If JSON parsing fails, the proxy server processes the data as plain text.

7. Main server that establishes a connection between two network points and intercepts data:

def start(self): Launches the proxy server and connects the client.

def handle_client(self, client_socket, client_address): Connects to the target server and creates two threads for data transmission.

def transfer_data(self, source, destination, direction, is_request): Handles data transmission and detects sensitive information.

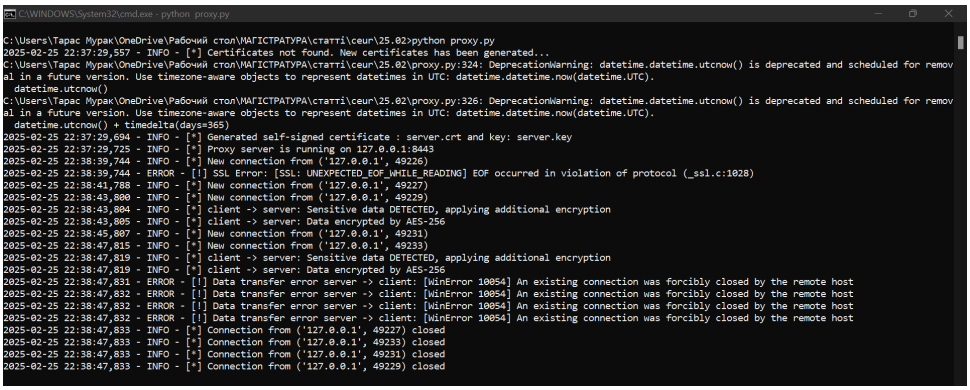

Figure 3: Proxy server logs.

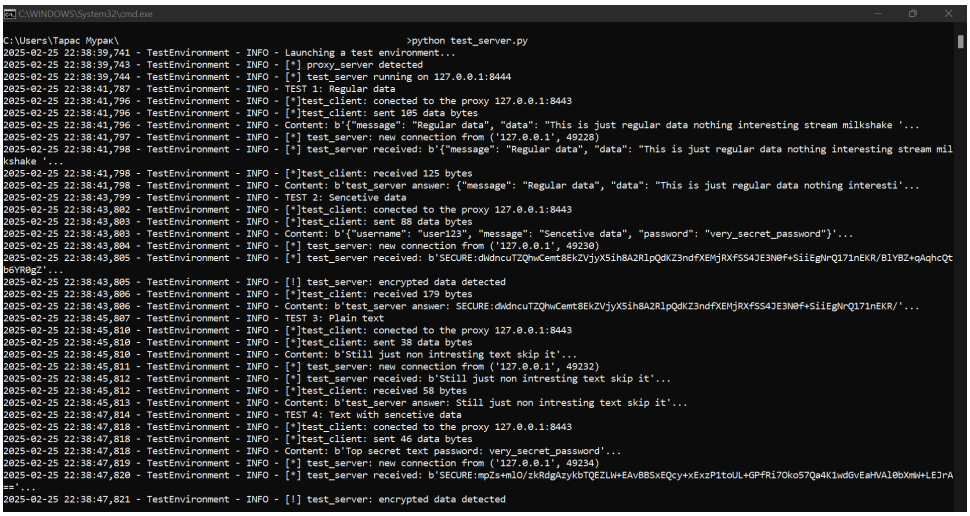

Figure 4: Test environment logs (client and target server) with test data exchange result.

To demonstrate the program's functionality, a test environment was also created. It includes a client that sends various test data and a target server that receives data transmitted through the proxy server. The client sends both plain text and potentially sensitive data. In the proxy server logs, we can observe information about detecting sensitive data and applying additional AES-256 encryption. Meanwhile, in the target server logs, we can see the received data. For clarity, encrypted sensitive data is marked with the prefix "SECURE:".

As shown in Figure 3, four test connections were made, transmitting different types of data. During the first and third connections, regular data was sent, while in the second and fourth connections, typical confidential information was transmitted, such as a login, password, and a secret message. Upon detecting sensitive data, the proxy server logs the event and applies additional encryption: client -> server: Sensitive data DETECTED, applying additional encryption; client -> server: Data encrypted by AES-256.

In Figure 4, we can see the data sent by the client and what was received by the target server. During the first and third connections, the data was received in the same form as it was sent. During the second and fourth connections, the target server received the data in an encrypted format, marked with the "SECURE:" prefix. For example: sent data - {"username": "user123", "message": "Sensitive data", "password": "very_secret_password"}; received data - SECURE: dwdncuTZQhwCemt8EkZVjyX5ih8A2R1pQdKZ3ndfXEMjRXfSS4JE3NØf+SiiEgNrQ171nEKR/B1YBZ+qAqhcQt.

6. Conclusions

The proposed methodology for ensuring information confidentiality in local corporate networks, which: 1) is presented as a multi-level approach based on the OSI reference model and the "defense-in-depth" model; 2) is deployed as a comprehensive security system within the "threat – security technologies" concept, addressing both random and targeted threats; 3) is practically implemented in the information protection mechanism at the transport layer of the OSI model using the AES-256 algorithm in Python, the OpenVPN protocol, and TLS technology, enabling a high level of cybersecurity resilience and protection.

Declaration on Generative AI

The authors have not employed any Generative AI tools.

References

[1] International strategy of the EU agency for cybersecurity, 2021. URL: https://www.enisa.europa.eu/sites/default/files/all_files/2022-02-16%20ENISA%20International%20Strategy.pdf.

[2] Cybersecurity strategy of Ukraine (2021-2025), 2021. URL: https://www.rnbo.gov.ua/files/2021/STRATEGIYA%20KYBERBEZPEKI/proekt%20strategii_kyberbezpeki_Ukr.pdf.

[3] NIS 2: Overview of the EU cybersecurity directive, 2021. URL: https://gigacloud.ua/blog/navchannja/nis-2-ogljad-direktivi-es-pro-kiberbezpeku.

[4] Y. Bobalo, V. Dudykevych, H. Mykytyn, Information technologies for data collection: concept, methodological approaches, security, Spolom, Lviv, 2024. 148 p.

[5] D. Chinchyk, T. Korobeynikova, S. Zakharchenko, Methods and means of complex protection of the corporate network, in: Scientific Collection «InterConf», with the Proceedings of the 5th International Scientific and Practical Conference «Theory and Practice of Science: Key Aspects», 84, 2021, pp. 433–450. doi:10.51582/interconf.7-8.11.2021.043.

[6] A. Ilienko, S. Ilienko, D. Kvasha, Y. Mazur, Practical approaches to identifying vulnerabilities in information and telecommunication networks, Cybersecurity: education, science, technology (2023) 96–108. doi:10.28925/2663-4023.2023.19.96108.

[7] O. Androschuk, O. Kovalenko, V. Titova, V. Cheshun, A. Polyakov, Improvement of information protection systems in computer networks of the state border guard service of Ukraine, Military Sciences (2021) 5–21. doi:10.32453/3.v85i2-3.828.

[8] O. Polotai, N. Fedynets, N. Kukharska, Research on information security threats and methods of their resolution in computer networks at the channel level, Bulletin of the Ukrainian State University of Railways (2024) 65–71. doi:10.32447/20784643.29.2024.07.

[9] P. Kuchernyuk, Methods and technologies for protecting computer networks (physical and channel levels), Microsystems, Electronics and Acoustics 22 (2017) 64–70.

[10] P. Kucherniuk, Methods and technologies for protecting computer networks (network, transport and application levels), Microsystems, Electronics and Acoustics 23 (2018) 52–58.

[11] O. Lebid, S. Kiporenko, V. Vovk, Detection of cyberattacks and improvement of information security based on neural network technologies in cyberwarfare conditions, Science and Technology Today (2023) 238–256. doi:10.52058/2786-6025-2023-1(15)-238-256.

[12] V. Savchenko, O. Rybalchenko, Building an effective enterprise network security system based on the method of analyzing hierarchies of quality indicators, Modern Information Protection (2024) 6–14. doi:10.31673/2409-7292.2024.010001.

[13] A. Yanko, R. Vyhivskyi, Computer network protection system, Control, Navigation and Communication Systems (2022) 91–94. doi:10.26906/SUNZ.2022.2.091.

[14] V. Susukailo, I. Opirsky, O. Yaremko, Methodology of ISMS establishment against modern cyber-

security threats, in: Lecture Notes in Electrical Engineering, Springer International Publishing, Cham, 2021, pp. 257–271. doi:10.1007/978-3-030-92435-5_15.

[15] M. Tolkachov, et al., Development of a method for protecting information resources in a corporate network by segmenting traffic, Eastern-European Journal of Enterprise Technologies (2024) 63–78. doi:10.15587/1729-4061.2024.313158.

[16] R. Habash, M. Ibrahem, Zero trust security model for enterprise networks, Iraqi Journal of Information and Communication Technology 6 (2023) 68–77. doi:10.31987/ijict.6.2.223.

[17] G.-L. Zhang, Analysing computer system security and computer network security, Engineering Technology Trends 2 (2024) 11–15. doi:10.37155/2972-483X-0204-3.

[18] O. Hosam, R. Abousamra, M. Hassouna, R. Azzawi, Security analysis and planning for enterprise networks, in: Industry 4.0 Key Technological Advances and Design Principles in Engineering, Education, Business, and Social Applications, 1, 2024, pp. 69–100. doi:10.1201/9781003343332-5.

[19] M. Lyu, H. Gharakheili, V. Sivaraman, A survey on enterprise network security: Asset behavioral monitoring and distributed attack detection, IEEE Access 12 (2024) 89363–89383. doi:10.48550/arXiv.2306.16675.

[20] J. Al-Azzeh, M. A. Hadidi, R. Odarchenko, S. Gnatyuk, Z. Shevchuk, Z. Hu, Analysis of self-similar traffic models in computer networks. international review on modelling and simulations, International Journal of Computer Network and Information Security 10 (2017) 328–336. doi:10.15866/iremos.v10i5.12009.

[21] M. Sudha, V. Mahesh Kumar Reddy, W. Deva Priya, S. Rafi, S. Subudhi, S. Jayachitra, Optimizing intrusion detection systems using parallel metric learning, Computers and Electrical Engineering 110 (2023) 76–91. doi:10.1016/j.compeleceng.2023.108869.

[22] N. Bhagat, MPLS vs. IPsec VPN: Choosing the right network architecture for enterprise WAN, International Journal of Scientific Research in Engineering and Management 5 (2021). doi:10.55041/ijsrem11326.

[23] A. Taslim, R. Uddin, N. Evan, R. Alam, Enterprise network: Security enhancement and policy management using next-generation firewall, in: Lecture Notes on Data Engineering and Communications Technologies, volume 66, 2021, pp. 753–769. doi:10.1007/978-981-16-0965-7_59.

[24] V. Abergos, F. Medjek, A risk assessment analysis to enhance the security of OT WAN with SD-WAN, Journal of Cybersecurity and Privacy 4 (2024) 910–937. doi:10.3390/jcp4040042.

[25] V. Dudykevych, G. Mykytyn, T. Stosyk, P. Skladannyi, Platform for the security of cyber-physical systems and the iot in the intellectualization of society, in: CEUR Workshop Proceedings, volume 3654, 2024, pp. 449–457.

[26] Y. Averyanova, et al., UAS cyber security hazards analysis and approach to qualitative assessment, in: S. Shukla, et al. (Eds.), Data Science and Security, volume 290 of *Lecture Notes in Networks and Systems*, Springer, Singapore, 2021, pp. 258–265. doi:10.1007/978-981-16-4486-3_28.

[27] V. Maksymovych, et al., Generator of pseudorandom bit sequence with increased cryptographic security, Metallurgical and Mining Industry: scientific and technical journal (2014) 25–29.

[28] V. Maksymovych, et al., Development of additive fibonacci generators with improved characteristics for cybersecurity needs, Applied Sciences (Basel) 12 (2022) 15–19. doi:10.3390/app12031519.

[29] S. Yevseiev, Y. Khokhlachova, S. Ostapov, O. Laptiev, O. Korol, S. Milevskyi, et al., Models of socio-cyber-physical systems security, PC Technology Center, Kharkiv, 2023. doi:10.15587/978-617-7319-72-5.

[30] V. Dudykevych, et al., A multicriterial analysis of the efficiency of conservative information security systems, Eastern-European Journal of Enterprise Technologies (2019) 6–13. doi:10.15587/1729-4061.2019.166349.

[31] D. Shevchuk, et al., Designing secured services for authentication, authorization, and accounting of users, in: CEUR Workshop Proceedings, volume 3550, 2023, pp. 217–225.

[32] C. Onyagu, O. Okonkwo, G. Akawuku, J. John, Enhancing security in Internet of Things (IoT) architecture through defense-in-depth mechanism: A comprehensive study, Newport International Journal of Engineering and Physical Sciences 4 (2024) 17–22.