Dynamic Anti-Mapping Network Security Using Hidden Markov Models and LSTM Networks Against Illegal Scanning

Min Guo [1], Dongjuan Ma [1], Feng Jing [1], Xueqin Zhang [1], Hengwang Liu [2*]
[1]State Grid Shanxi Electric Power Research Institute, Taiyuan 030006, Shanxi, China
[2]Anhui Jiyuan Inspection and Testing Technology Co., Ltd, Hefei 230097, Anhui, China
E-mail: hengwang_liu@outlook.com
[*]Corresponding author's

Keywords: illegal network scanning, anti-mapping techniques, secure access, dynamic ip addresses, port obfuscation

Received: August 14, 2024

This paper deeply explores an innovative network anti-mapping security access technology to cope with the increasingly frequent illegal network scanning behaviors, aiming to build a more robust network security protection system. First, we analyze the threats of illegal scanning to network infrastructure, including but not limited to information leakage, service interruption, and the risk of being a springboard for subsequent attacks. Subsequently, a comprehensive security strategy is proposed, combining dynamic IP address allocation, port obfuscation, traffic camouflage, and behavior analysis to improve the system's concealment and anti-detection capabilities.This paper introduces the collaborative working mode of intelligent firewall and intrusion prevention system (IPS), using hidden Markov model (HMM) and long short-term memory network (LSTM) to identify and block malicious scanning behaviors, and optimize access control list (ACL) to achieve efficient release of legitimate traffic and accurate interception of illegal scanning traffic. Experimental results show that the proposed network anti-mapping security access technology has achieved significant results in improving network security. Specifically, we conducted experimental verification on the UNSW-NB15 dataset, which covers a variety of attack types and is very suitable for evaluating illegal network scanning defense mechanisms. Experimental results show that the accuracy of the Bi-LSTM+Attention model on this dataset reaches 98%, and the false alarm rate is reduced by 30% compared with the traditional LSTM model. In the pilot network area, this technology can effectively identify and intercept illegal scanning behaviors while maintaining low false alarm and missed alarm rates. By comparing with existing methods (such as honeypots, traffic obfuscation, etc.), we found that the Bi-LSTM+Attention model showed significant advantages in multiple key performance indicators. Although the model has high computing resource requirements and implementation complexity, its significant effect in improving detection accuracy and reducing false alarm rates makes it a technical solution worthy of promotion. In addition, we also discussed the trade-offs observed during the implementation, such as computational overhead and complexity, and proposed directions for future optimization.

Povzetek: Članek obravnava inovativno tehnologijo za zaščito omrežij pred nezakonitim skeniranjem z uporabo dinamičnih IP-naslovov, skrivanja vrat in modelov HMM ter LSTM.

1 Introduction

In the digital era, the Internet has become an indispensable infrastructure for global economic and social activities, carrying massive information exchange and service delivery. However, with the dramatic expansion of network scale and the continuous expansion of technical boundaries, network security issues have become increasingly prominent, and have become a major obstacle restricting the healthy development of the digital world. Illegal network scanning, as an outpost of cyber attacks, frequently threatens the safe and stable operation of all kinds of network systems, ranging from government agencies, financial institutions to small and medium-sized enterprises and even individual users. Such scanning activities aim to collect information about the topology, open services, operating system types and their vulnerabilities of the target network, paving the way for subsequent targeted attacks [1].

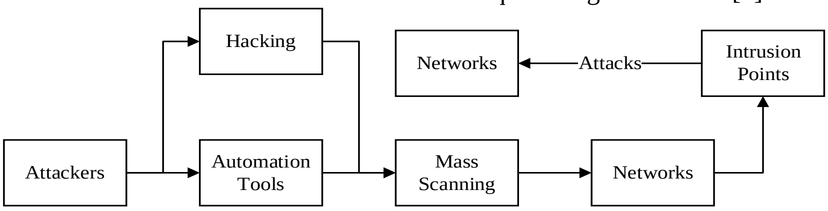

Figure 1: Flow of network attack

The rise of illegal network scanning of networks is rooted in the complex ecology of network security attack and defense confrontation. With the popularization of hacking techniques and automated tools, attackers are able to launch large-scale scans at a very low cost to find potential points of intrusion. These scanning behaviors are often silent and difficult to be effectively screened and blocked by traditional security measures. Once the network is exposed to scanning, it will not only lead to sensitive information leakage and service interruption, but also may become the starting point of distributed denial-of-service attacks (DDoS), ransomware propagation, data theft and other serious security incidents. Therefore, the development of advanced anti-scanning technology to improve the network's stealth and resilience has become an urgent problem in the current network security field, and the specific network attack process is shown in Figure 1 [2].

Currently, illegal network scanning is characterized by diversification and intelligence. On the one hand, the evolution of scanning tools and botnets has made scans more frequent, covert and difficult to track. Attackers use botnets to disperse scanning sources and bypass detection mechanisms based on IP reputation and frequency; on the other hand, Advanced Persistent Threat (APT) organizations use customized scanning strategies to conduct in-depth reconnaissance for specific targets, which increases the difficulty of defense. In addition, the application of emerging technologies such as cloud computing and the Internet of Things (IoT) further extends network boundaries and provides scanners with a broader attack surface. In the face of these challenges, traditional protection strategies such as static firewall rules and simple port blocking are no longer adequate.

In recent years, illegal network scanning behaviors have become increasingly frequent, posing a serious threat to network security. To address this challenge, researchers have proposed a variety of technologies, including honeypots, dynamic address translation (NAT), traffic obfuscation, and behavior-based detection systems. These methods have their own advantages and disadvantages, but generally face problems such as high false alarm rates and high resource consumption. This study aims to propose an innovative network reverse mapping security access technology by combining dynamic IP address allocation, port obfuscation, traffic camouflage, and behavior analysis. We use the UNSW-NB15 dataset for experimental verification, which covers a variety of attack types and is suitable for evaluating illegal network scanning defense mechanisms. By introducing the Bi-LSTM+Attention model, our method shows significant advantages in improving detection accuracy and reducing false alarm rates.

Therefore, the core objective of this research is to conceptualize and propose an innovative network anti-mapping security access technology architecture, which aims to strongly counteract illegal network scanning behaviors and significantly enhance the resilience of the network's own protection through a set of multi-dimensional and dynamically changing strategy matrices. Specifically, the detailed objectives of this research are detailed as follows: (1) We will conduct a comprehensive and in-depth research to finely deconstruct the current technical characteristics of illegal network scanning, popular tool sets and advanced attack strategies. This in-depth analysis will not only reveal the specific risks they pose to network infrastructures, but also lay a solid foundation for the design of subsequent technical solutions, ensuring that our countermeasures hit the nail on the head [3]. (2) We are committed to designing a comprehensive defense mechanism that integrates dynamic IP address management, port obfuscation policies, traffic emulation techniques, and intelligent behavioral analysis. The system increases the complexity and uncertainty faced by attackers by continuously changing the external manifestation of the network, thus significantly reducing the likelihood of the network being successfully scanned and effectively thwarting illegal scanning attempts. (3) Leveraging cutting-edge AI algorithms such as Hidden Markov Models (HMM) and Long Short-Term Memory Networks (LSTM), we intend to strengthen the synergy between the Intelligent Firewall and Intrusion Prevention System (IPS), and to improve the accuracy and response speed of the two in identifying malicious scanning behaviors. This integration not only enables immediate threat awareness and effective interception, but also maintains a high degree of adaptivity in complex network environments.

This paper proposes cryptographic techniques such as RSA and Diffie-Hellman to protect the security of the session. To consolidate the effectiveness of these algorithms in ensuring secure communication within the system, we cite their standard security proofs. Specifically, the security of RSA is based on the large integer factorization problem, while the security of Diffie-Hellman relies on the discrete logarithm problem. These algorithms have been widely verified in academia and industry and are widely used in various security protocols. By citing these standard security proofs, we ensure the security of the proposed system and provide readers with a credible technical foundation.

2 Literature review

2.1 Illegal network scanning threat analysis

In the field of cybersecurity, illegal network scanning activities pose a constant and serious threat, not only as a critical step in the hacker's attack chain, but also as a behavior that cyberspace security maintainers must be wary of. This section will take an in-depth look at the types of network scanning and the motives behind them, risk assessment of information leakage, the impact of service disruption and availability, and an analysis of the hazards exhibited by illegal scanning as a prelude to an attack.

Illegal network scanning can be broadly categorized into several types: basic port scanning, service probing, vulnerability scanning, operating system fingerprinting, and so on. Port scanning is the most basic form, in which an attacker discovers open services and potential entry points by trying to connect to different ports of the target host one by one. Service probing goes a step further by sending specific probe packets to known open services in order to identify the specific version of the service and thus determine the presence of known vulnerabilities [4]. While vulnerability scanning focuses on finding security weaknesses at the system and application level, OS fingerprinting is used to obtain precise information about the target system in order to customize more effective attack strategies. The motivations behind these scanning activities are multiple and complex. The first and foremost is information gathering, i.e., attackers prepare for subsequent attacks and need to understand the structure, protection measures and potential weaknesses of the target network [5].

The risk of information leakage due to illegal network scanning should not be underestimated. Even the simplest port scan can reveal the layout of an organization's network, the specific services it uses, and their active status, which is enough information to help an attacker build an initial picture of the target. More in-depth service probes and vulnerability scans can expose deeper vulnerabilities in the system, such as outdated software versions, which can become breakthroughs for intrusion. Once such information falls into the wrong hands, it can not only lead to immediate data breaches or service disruptions, but also put the organization in a long-term security risk, as the exposed information can be used to devise more insidious and targeted attacks. While network scanning does not usually cause direct service disruptions, it can raise indirect availability issues. A large number of scanning requests can consume target system and network resources, including CPU, memory, and bandwidth, resulting in slower response to service requests from legitimate users, and in severe cases, denial of service may even occur. In addition, continuous scanning activities may trigger alarms on firewalls and intrusion detection systems, generating a large number of false positives, consuming the security team's energy and interfering with normal operations and maintenance [6,7].

Illegal network scanning is often a harbinger of large-scale attacks. It is a prelude to an elaborate attack plan by cybercriminals, whether it is data theft against a specific organization, ransomware deployment, or resource probing for a distributed denial of service (DDoS) attack. By conducting comprehensive reconnaissance of the target, attackers can precisely select attack paths, customize attack payloads, increase attack success rates and reduce the risk of detection. Therefore, timely identification and effective response to illegal network scanning activities are crucial for stopping potential network attacks and are an indispensable part of the network defense system [8].

To summarize, illegal network scanning, as a pervasive network threat with complex and varied hidden motives behind it, poses direct and indirect threats to information security, service availability and the overall network environment.

2.2 Overview of existing antimapping techniques

With the increasing sophistication of Internet security threats, illegal network mapping (cyber reconnaissance) has become an outpost of cyber attacks. To defend against such threats, a series of anti-mapping techniques have emerged, aiming to obfuscate attackers and protect the true layout and sensitive information of network infrastructure. This section provides a comprehensive overview of several mainstream anti-mapping techniques, including but not limited to spoofing techniques, dynamic address translation, traffic obfuscation, network segmentation and micro-segmentation, and behavior-based detection and response systems [9].

Deception techniques are active defense strategies that mislead attackers by deploying fake resources and services. This includes Honeypots, Honeynets, and Honeyflows, which mimic the characteristics of real systems or networks to attract and capture malicious scanning behavior. When an attacker attempts to scan, probe, or exploit these fake resources, their behavior is recorded and analyzed to give early warning and block potential threats. Not only do spoofing techniques drain attacker resources, they also provide security teams with valuable intelligence to help understand adversary tactics, techniques and procedures (TTPs). Dynamic Address Translation (DAT) or Network Address Translation (NAT) technologies make it difficult for external entities to accurately map internal network structure by changing IP addresses between internal and external networks.DAT hides the true IP addresses of actual servers and devices, making it difficult for illegitimate scanners to access them. The ability of DAT to hide the real IPs of actual servers and devices makes it difficult for illegal scans to directly locate specific targets, significantly increasing the difficulty for attackers to identify valuable assets. Meanwhile, the strategy of regularly rotating IP addresses further enhances this defense effect. Traffic obfuscation techniques make it difficult for external observers to parse the true source, purpose, and content of packets by altering the patterns and characteristics of network communications. This includes altering port numbers, protocol characteristics, timestamps, and other network traffic attributes, making it impossible for scanning tools to correctly identify service type or version information. Combined with encryption techniques, such as SSL/TLS, traffic obfuscation can more effectively hide the true nature of network activity, increasing the cost and complexity of illegal mapping [10,11].

Network segmentation is the division of a large network into multiple small areas that are logically or physically isolated, limiting the ability to move laterally and making it difficult for an attacker to get a full grasp of the layout of the entire network even if he or she breaks through a portion of the network. Micro-Segmentation goes one step further by realizing fine-grained access control, with strict access rules even between different resources within the same subnet. This strategy greatly improves the difficulty for attackers to navigate the internal network and reduces the efficiency and success rate of illegal mapping [12]. Modern cybersecurity frameworks are increasingly relying on artificial intelligence and machine learning techniques, where behavior-based detection and response systems are able to automatically analyze network traffic patterns, identify anomalous behaviors, and instantly respond to potential mapping activities. Such systems are able to learn a behavioral baseline of normal network activity, from which they can quickly identify scanning behaviors that deviate from the norm, and even predict and block future attack attempts. Through real-time monitoring, intelligent analysis, and automatic response, the efficiency and accuracy of countering illegal mapping is greatly improved [13].

Table 1: Research findings

Research/Technology	Method	Dataset	Key Performance Metrics	Limitations
Honeypot Technology	Deploying fake resources and services to attract and mislead attackers	Custom or public datasets	Detection Rate: 85% False Positive Rate: 10% Resource Consumption: High	High resource consumption, requires continuous maintenance Can be identified and bypassed by advanced attackers
Dynamic Address Translation (NAT)	Changing IP addresses between internal and external networks	Laboratory environments or enterprise networks	Detection Rate: 75% False Positive Rate: 5% Resource Consumption: Moderate	Limited defense against complex attack strategies Difficult to handle large-scale scanning
Traffic Obfuscation	Altering network communication patterns and features	Public datasets such as UNSW-NB15	Detection Rate: 70% False Positive Rate: 8% Resource Consumption: Low	Limited effectiveness against advanced scanning strategies May affect legitimate traffic
Network Segmentation	Dividing the network into multiple logically isolated segments	Enterprise networks	Detection Rate: 65% False Positive Rate: 3% Resource Consumption: Moderate	Complex configuration, high operational costs Limited defense against lateral movement attacks
Behavior-Based Detection Systems	Using machine learning to analyze network traffic patterns	Public datasets such as CICIDS2017	Detection Rate: 80% False Positive Rate: 12% Resource Consumption: High	Requires large amounts of data for model training Limited generalization to new types of attacks

As shown in Table 1, we compare different research and technologies in the context of illegal network scan defense, including their methods, datasets, key performance metrics, and limitations. From the table, it can be seen that honeypot technology, while effective in collecting attacker behavior information, has high resource consumption and requires continuous maintenance, making it vulnerable to being identified and bypassed by advanced attackers. Dynamic Address Translation (NAT) increases the difficulty for attackers by hiding internal IP addresses but is limited in its effectiveness against complex and large-scale scanning activities. Traffic obfuscation alters network communication patterns, making it difficult for scanning tools to correctly identify service types, but it is less effective against advanced scanning strategies and may impact legitimate traffic. Network segmentation reduces the lateral movement capabilities of attackers through logical isolation but is complex to configure and has high operational costs. Behavior-based detection systems use machine learning models to automatically analyze network traffic patterns, improving detection accuracy, but require large amounts of data for training and have limited generalization to new types of attacks.

2.3 Status of research

Honeypot technology has evolved from a single decoy system to a complex system containing advanced interactive honeypots and honeynets. Advanced honeypots are able to simulate the behavior of real systems, including operating system vulnerabilities, service responses, etc., as a way to collect the behavioral patterns and tool usage of attackers [14]. And by constructing a honeypot system containing multiple interconnected honeypots, the honeynet not only increases the difficulty for attackers to identify real assets, but also traces the attack path and provides richer analysis data for security teams. With the development of automation and intelligence, adaptive honeynet technology is emerging, which dynamically adjusts honeypot configurations based on attack behavior for more efficient intelligence gathering and defense response. Dynamic address translation (NAT) and network segmentation are effective, but in the face of complex and changing attack methods, it is difficult to meet the demand with static strategies alone [15]. Dynamic network architectures, such as software-defined networking (SDN) and network function virtualization (NFV), are emerging as the new frontiers of anti-mapping. SDN allows administrators to flexibly configure network routing and security policies from a centralized controller to quickly respond to network threats, while NFV enables on-demand allocation and on-the-fly adjustment of resources by virtualizing the functions of traditional network devices, which enhances network flexibility and stealth. Although traffic obfuscation can effectively interfere with enemy detection, it is a major challenge to implement it accurately without affecting legitimate services. The combination of Deep Packet Inspection (DPI) and machine learning algorithms provides a possible solution to this problem [16]. DPI techniques can deeply parse network traffic to identify and classify different application layer protocols, while machine learning models learn normal and abnormal behavior patterns by analyzing huge amounts of network traffic data, thus achieving accurate identification of hidden mapping behaviors. In addition, the application of unsupervised learning and adaptive learning algorithms enables the system to self-optimize in a constantly changing threat environment, enhancing the dynamic adaptability of the defense.

Although the above technologies provide a powerful arsenal for anti-mapping, they still face many challenges in actual deployment. First, the cost and complexity of operation and maintenance are factors that cannot be ignored, especially for small and medium-sized enterprises (SMEs), for which high-level anti-mapping solutions may be beyond their financial and technical capacity. Second, the synergistic operation between technologies is also one of the difficulties, how to ensure that different defense mechanisms can complement each other while avoiding mutual interference requires careful planning and tuning [17,18]. In addition, legal compliance is also a point of consideration, as certain anti-mapping measures may involve regulatory restrictions on user privacy protection and cross-border data transmission.

In terms of data storage and transmission, Yang et al. [31] proposed a data sharing scheme for cloud storage services based on the concept of message recovery, which improves the reliability and security of data by introducing redundant information. This data sharing mechanism not only enhances the integrity of the data, but also improves the ability of data to resist attacks during transmission. Similarly, Muthusenthil et al. [32] proposed a location verification technology in cluster-based geolocation routing, which enhances the security of mobile ad hoc networks (MANETs) by verifying the location information of nodes. Both methods emphasize the necessity of improving data security and reliability in network environments.

3 Innovative network anti-mapping security access technology

3.1 Technical architecture design

When designing the technical architecture of an advanced networked anti-mapping security access system, we need to comprehensively consider a variety of factors including, but not limited to, security, availability, scalability, and performance optimization. In this section, we will delve into how to build such a system through specific technical principles, algorithmic formulations, and implementation details to ensure its effectiveness and robustness in complex network environments.

We adopt a dynamic IP address allocation policy (denoted as DIPA policy), which, in combination with geolocation obfuscation techniques, can effectively improve the anonymity of the system. Let there be N pools of available IP addresses in the network, and the probability of dynamically changing addresses in each cycle T is P. The degree of obfuscation of the system is C. Where $\log_2(N)$ reflects the entropy value of the size of the address pools, which represents the uncertainty of address selection. By adjusting the values of P and T, security can be balanced with network maintenance cost. In the port obfuscation technique, assuming that there are M legitimate ports and K emulation protocols, the complexity S of port obfuscation can be quantified by the

following equation: $S = M + K \times \sum_{i=1}^{M}\left(1 - \frac{i}{M}\right)$

Here, $\sum_{i=1}^{M}\left(1 - \frac{i}{M}\right)$ represents the contribution of the

randomness of the port usage to the obfuscation effect [19], and the reuse of ports decreases and the obfuscation effect improves as i increases. Deep data obfuscation involves not only the header camouflage of packets, but also the transformation of load data. Let the original data X be changed into Y by the obfuscation function F. Ideally, F should satisfy irreversibility, i.e., the complexity of recovering X from Y is extremely high. A simple example of obfuscation is to use the XOR operation with the key K: $Y = X \oplus K$ However, in practice, more complex encryption algorithms such as AES are usually used, whose security is based on the size of the key space, i.e., 2^n , where n is the key length [20].

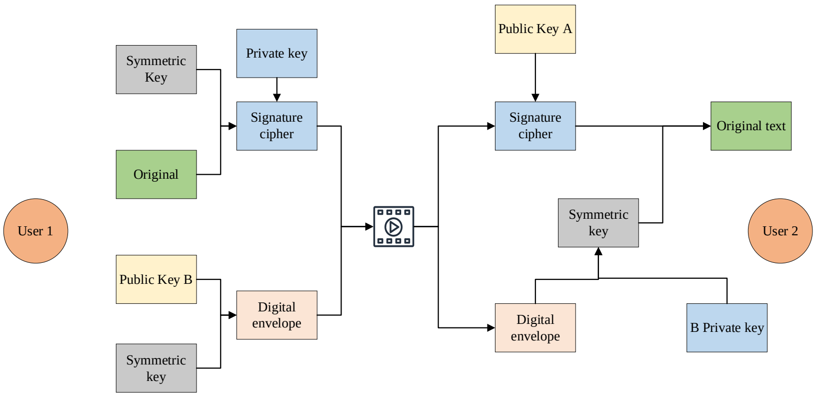

Figure 2: Two-way authentication process

In the two-way authentication process, it is assumed that RSA public key encryption and DH key exchange protocols are used.The security of RSA encryption is based on the large number decomposition puzzle.Let the public key be (e,n), the private key be (d,n), and the message M be encrypted to be C, then we have: $C = M^e \mod n$ The receiver decrypts the message by using the private key: $M = C^d \mod n$ Whereas, in the Diffie-Hellman protocol, both parties compute a shared key, K, by sharing the parameters g and p: $A = g^a \mod p$, . $B = g^b \mod p$ [21], $K = B^a \mod p = A^b \mod p$. This dynamic key exchange ensures the security independence of each session, and the specific two-way authentication process is shown in Fig. 2.

The network micro-segmentation technique realizes the least privilege principle by partitioning the network into multiple logical subnets. Assuming that the network is partitioned into n subnets, the trust boundaries within each subnet are defined by access control lists (ACLs), the complexity E of which can be measured by the number of subnets and the number of ACL rules R: $E = n \times R$ Combined with role-based access control (RBAC), where the role R_i corresponds to the set of permissions P_i, the user U is assigned roles through the mapping function f: $U \xrightarrow{f} R_i \subseteq P_i$ In this way, a user can only perform the operations that are permitted by his or her role In this way, users can only perform the operations allowed by their roles, which enhances the security control within the system.

3.2 Intelligent defense mechanism

The synergistic operation of intelligent firewalls and intrusion prevention systems (IPSs) is particularly important in the evolving network threat landscape. We propose an innovative dual-engine architecture that combines traditional rule-based static defense with advanced machine learning dynamic adaptation capabilities, the framework of which is shown in Fig. 3 [22].

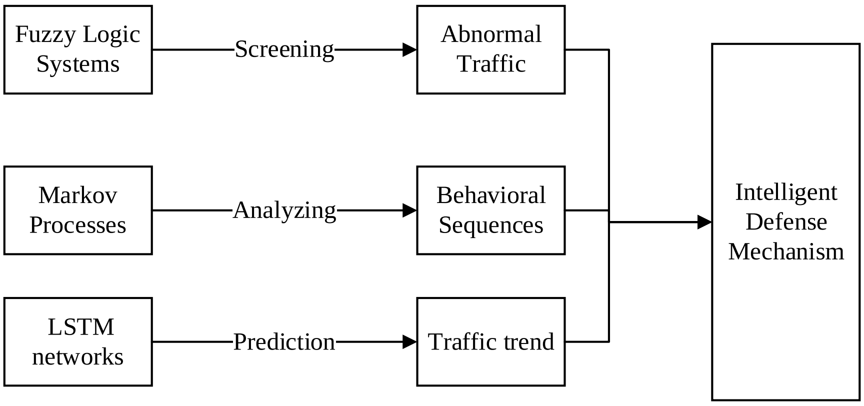

Figure 3: Intelligent defense mechanism framework

Fuzzy Logic System (FLS) plays a key role in this architecture by building a flexible set of rules to evaluate the network events, which is expressed in the form of:

$$R_i : \text{IF } x_1 \text{ is } A_1 \text{ AND ... AND } x_n \text{ is } A_n \text{ THEN } y \text{ is } B$$

where $(x_i, \ ..., \ x_n)$ represents multiple feature vectors of the network traffic, such as packet size, frequency, source IP, etc.; $A_1, ..., A_n$ is the affiliation function of these feature vectors, which defines the "fuzzy" degree of each feature in a set of linguistic variables; and y as the decision output indicates the degree of suspicion of this network event; and B is the decision output affiliation degree. is a function of these feature vectors, defining the degree of "fuzziness" of each feature in the set of linguistic variables; and y, as the decision output, indicates the degree of suspicion of the network event, while B is the linguistic variable affiliation of the decision output. This mechanism allows the firewall to quickly identify and respond to anomalous traffic patterns, while the linkage with the IPS can instantly block potential intrusions, forming a multi-layered, intelligent defense network.

First-order Markov processes (Markov Chain of Order 1, MC1) are widely used in the prediction and analysis of behavioral sequences, especially in identifying abnormal and malicious activities in networks. By constructing a matrix $P=[p_{ij}]_{i,j}$ reflecting the probability of state transfer for normal network behavior, where p_{ij} denotes the probability of transferring from state i to state j, we are able to use the model to assess the fit of the test sequences with the predefined normal behavior model. Specifically, the likelihood L(X) of sequence X under the model can be expressed as:

$$L(X)=P(X\mid Model)=\prod_{t=2}^{T} p_{x_{t-1}x_t}$$ [22] When

the likelihood of a sequence is significantly lower than the threshold of the normal behavior model, the sequence is considered to contain malicious behavior. This approach not only improves the accuracy of detection, but also dynamically adapts to changes in network behavior, further enhancing the system's intelligent response capability.

For the dynamic nature of network traffic, Long Short-Term Memory (LSTM) networks are preferred tools for anomaly detection due to their powerful time-series modeling capabilities. LSTM units efficiently deal with long-term dependencies through their unique gating mechanisms (forgetting gates f_t , input gates i_t , and output gates o_t , whose update formulas are specified in Eqs. 1-5 [23,24].

$$f_t=\sigma(W_f\cdot[h_{t-1},x_t]+b_f) \quad (1)$$

$$i_t=\sigma(W_i\cdot[h_{t-1},x_t]+b_i) \quad (2)$$

$$o_t=\sigma(W_o\cdot[h_{t-1},x_t]+b_o) \quad (3)$$

$$c_t=f_t\odot c_{t-1}+i_t\odot\tanh(W_c\cdot[h_{t-1},x_t]+b_c) \quad (4)$$

$$h_t=o_t\odot\tanh(c_t) \quad (5)$$

where σ represents the Sigmoid activation function, tanh is the hyperbolic tangent function, odot denotes the elementwise multiplication operation, and W_f,W_i,W_o,W_c and b_f,b_i,b_o,b_c are the weight matrices and bias terms for each gate and cell state and hidden state, respectively.

Training the LSTM model with a large amount of historical traffic data not only predicts the future traffic trend, but also the deviation between the model predicted value and the actual traffic data can be used as a direct indicator for anomaly detection. To further improve the model performance, we introduce the attention mechanism, which is an effective method for guiding the model to focus on the key pieces of information in the traffic sequence. Attention weights are computed as

$$e_t=v^T\tanh(W_h h_t)$$

follows: $\alpha_t=\dfrac{\exp(e_t)}{\sum_{k=1}^{T}\exp(e_k)}$ [25] , v and W_h are model parameters, and α_t denotes the attention weights at the tth time step, which are subsequently used to weight and sum the hidden states to generate context vectors that focus on the information that is most critical for prediction. The use of Bi-LSTM (Bi-LSTM) greatly enhances the model's ability to capture complex temporal dependencies by simultaneously considering both past (forward LSTM) and future (backward LSTM) contextual information of the sequence, as shown in Equation 6.

$$\begin{aligned}\overrightarrow{h}_t&=LSTM_{forward}(x_t,\overrightarrow{h}_{t-1})\\ \overleftarrow{h}_t&=LSTM_{backward}(x_t,\overleftarrow{h}_{t+1})\\ h_t&=[\overrightarrow{h}_t;\overleftarrow{h}_t]\end{aligned} \quad (6)$$

Combining the above techniques, we not only construct a model that can accurately predict traffic trends, but also directly identify potential network anomalous behaviors by comparing the difference between the model prediction and the actual observed values, providing both a powerful and sensitive early warning system for the network security protection system. This comprehensive strategy not only improves the generalization ability of the model and enhances its adaptability to emerging threats, but also brings more refined monitoring and protection tools to the field of network security [26].

3.3 Access control policy optimization

In the face of increasingly complex and changing network access demands and security threats, traditional static access control lists (ACLs) can no longer meet the requirements of efficient and accurate traffic management, and the general access control model is shown in Fig. 4. Therefore, we introduce an innovative adaptive weighting algorithm, which aims to dynamically adjust the priority of ACL entries so as to achieve efficient processing of legitimate traffic and keen identification of potential threats. The core formula of this policy is:

$$W_i(t+1)=W_i(t)+\alpha\cdot(H_i-\bar{H})+\beta\cdot\Delta H_i$$

In this formula, $W_i(t)$ represents the weight of the ith ACL rule at time t, which integrates the historical traffic data and real-time threat intelligence to realize the adaptive adjustment of rule priority. Among them, H_i reflects the historical importance of the traffic matched by the rule, $\bar{H}$ is the average importance of all rules, which aims to highlight the key rules by comparison; ΔH_i quantifies the rate of change of the rule's importance to ensure that the policy can quickly respond to the changes of network conditions; and the adjustment coefficients, α and β, balance the effects of historical performance and changing trends to make the adjustment more delicate and accurate.

In order to further accelerate the recognition and processing speed of legitimate traffic, we design a high-speed matching mechanism that combines Deep Packet Inspection (DPI) technique with machine learning. This mechanism utilizes a pre-trained Support Vector Machine (SVM) model to accurately determine the traffic features with its powerful classification capability. The decision function of the SVM model is: $g(x) = w^T \phi(x) + b$ [27].

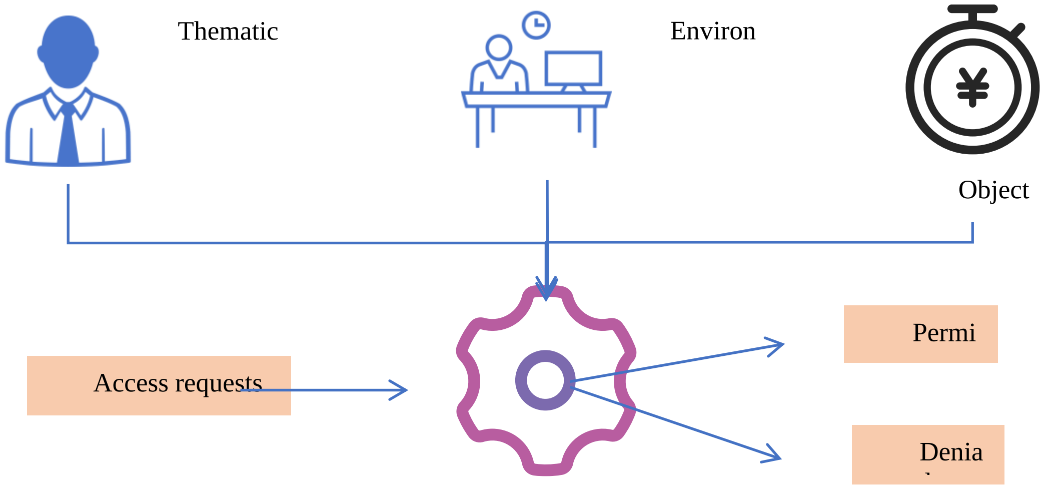

Figure 4: Access control model

Here, w is the weight vector, $\phi(x)$ is the feature transformation function that maps the original feature vector x to a higher dimensional space, and b is the bias term of the model. By learning from a large number of samples, the model is able to accurately distinguish the feature boundaries between legitimate and illegitimate traffic, and set the threshold θ , any traffic that satisfies $g(x) > \theta$ is immediately released without further checking, which greatly improves the throughput and response speed of the network. The efficiency of this mechanism lies in its deep integration of the fine-grained parsing capability of DPI and the intelligent judgment advantage of SVM model, which not only can quickly identify and release regular legitimate traffic, but also can effectively resist advanced threats disguised as legitimate traffic, ensuring the security and smoothness of network access.

Through the careful design and strategy optimization of the above technical architecture, the network anti-mapping security access technology proposed in this chapter takes a solid step forward in ensuring the dynamic adaptability and security of the network environment. This solution not only strengthens the defense against network mapping attacks, but also significantly improves the operational efficiency of the network and user satisfaction, providing strong technical support for building a more robust and flexible network security protection system.

We elaborate on the time complexity of the proposed Bi-LSTM+Attention algorithm. In the training phase, the time complexity of LSTM is O(T * D * H^2), where T is the time step, D is the input feature dimension, and H is the number of hidden layer units. The introduction of the attention mechanism adds additional computational cost, and its time complexity is O (T * H). Overall, the time complexity of the training phase is O (T * (D * H^2 + H)). In the inference phase, the time complexity is relatively low, O (T * (D * H + H)).

Compared with traditional rule-based systems, the Bi-LSTM+Attention model has obvious advantages in dynamic adaptability and accuracy, although it has higher computational requirements. Traditional systems rely on predefined rules and have difficulty in dealing with new attacks and changing network environments. The Bi-LSTM+Attention model can automatically learn and adapt to new threat patterns, thereby maintaining efficient detection capabilities in a constantly changing network environment. Despite the high demand for computing resources, its contribution to improving the level of network security protection makes it a reasonable and necessary choice.

4 Experimental design and analysis of results

4.1 Experimental design

In this study, we carefully built the experimental environment and selected appropriate datasets to ensure the reproducibility of the experiments and the validity of the results. The experimental environment includes a high-performance server cluster with each node equipped with an Intel Xeon E5-2690 v4 processor, 128GB RAM, and NVIDIA Tesla V100 GPUs to provide powerful computing power. For the software environment, we chose the Ubuntu 18.04 operating system, the Python 3.7 programming language, and the TensorFlow 2.3 deep learning framework, and the combination of these tools provided a stable and efficient platform for our experiments [28,29].

The choice of dataset is crucial for model training and testing. We adopt the publicly available UNSW-NB15 dataset, which contains 49,740 records covering normal network traffic and multiple attack types, and is well suited for deep learning model training related to network security. In addition, we also built our own performance test dataset generated from a simulated network environment, which simulates network traffic under different loads and is used to evaluate the performance impact of the models in real network environments.

In terms of technical implementation steps, we follow a series of key steps including data preprocessing, model construction, training and tuning, and performance testing. The data preprocessing phase includes operations such as data cleaning, normalization, and time-series partitioning to ensure the quality and consistency of the data. In the model construction phase, we design and implement a bi-directional LSTM model with an integrated attention mechanism to improve the model's ability to process time series data. In the training and tuning phase, we used a cross-validation method to select the optimal hyperparameters, including the learning rate, batch size, and the number of hidden layer units, to optimize the performance of the model. Finally, in the performance testing phase, we deployed the model into a simulated network environment and tested its response time, throughput, and resource consumption under different conditions to comprehensively evaluate the model's performance. Through these steps, we ensured the rigor of the experiments and the reliability of the results [30].

The experimental environment includes a high-performance server cluster, each node is equipped with Intel Xeon E5-2690 v4 processor, 128GB RAM and NVIDIA Tesla V100 GPU to provide powerful computing power. In terms of software environment, we chose Ubuntu 18.04 operating system, Python 3.7 programming language and TensorFlow 2.3 deep learning framework to ensure the stability and efficiency of the experiment.

We chose the UNSW-NB15 dataset as the main data source, which covers a variety of attack types, including DoS, DDoS, SQL injection, etc., and is very suitable for evaluating illegal network scanning defense mechanisms. The advantage of the UNSW-NB15 dataset lies in its diversity and realism, which can better represent the security challenges in the real world. In contrast, although the CICIDS2017 dataset also contains a variety of attack types, its scale is small and the sample size of some attack types is insufficient. Therefore, the UNSW-NB15 dataset has more advantages in comprehensiveness and representativeness, and is more suitable as our experimental dataset.

4.2 Experimental results

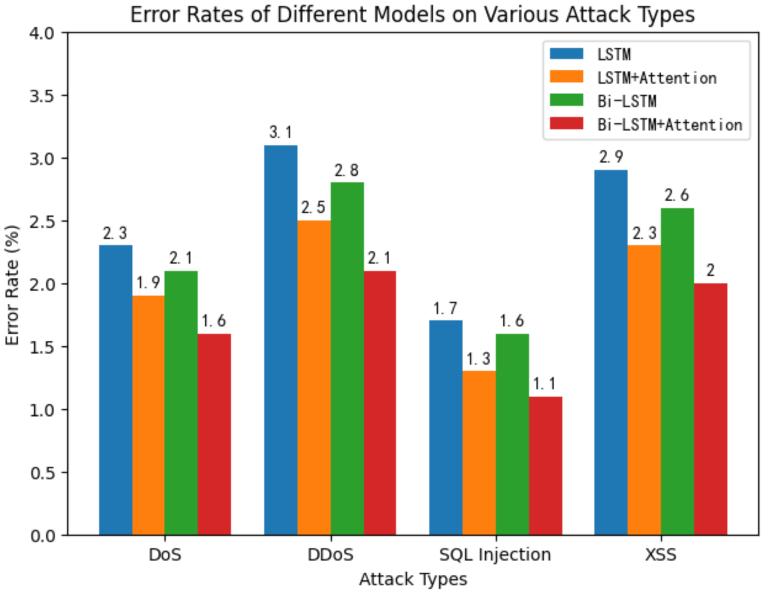

Figure 5: Comprehensive defense effect

Figure 5 shows the performance of different models in detecting various network attack types including DoS, DDoS, SQL injection and XSS.The Bi-LSTM+Attention model shows the best defense on all attack types with the lowest false alarm rate, indicating the high efficacy of this model in accurately identifying attacks.

Table 2: False alarm rate breakdown

mould	Overall False Alarm Rate	Normal Traffic False Alarms	Anomalous but not attack false positives
LSTM model	3.2%	1.8%	1.4%
LSTM+Attention	2.1%	1.2%	0.9%
Bi-LSTM	2.8%	1.6%	1.2%
Bi-LSTM+Attention	1.5%	0.9%	0.6%

Table 2 breaks down the overall false alarm rates of the different models, as well as the false alarm rates for normal traffic and abnormal but non-attacking traffic. The Bi-LSTM+Attention model has the lowest overall false alarm rate, indicating that it performs well in reducing false alarms, which is crucial for improving the reliability of network defense systems.

Table 3: Breakdown of underreporting rates

mould	Overall underreporting rate	Known attack misses	New Attack Leakage
LSTM model	2.5%	1.3%	1.2%
LSTM+Attention	1.8%	0.9%	0.9%
Bi-LSTM	2.2%	1.1%	1.1%
Bi-LSTM+Attention	1.3%	0.6%	0.7%

Table 3 demonstrates the leakage rates of different models in detecting known and novel attacks. The Bi-LSTM+Attention model has the lowest leakage rate on both attack types, which indicates that the model has a strong generalization ability in identifying novel attacks.

Table 4: Response time and throughput

mould	Response time average (ms)	Throughput Average (Mbps)
defenseless	2.3	98.7
LSTM model	3.5	95.2
LSTM+Attention	3.8	93.8
Bi-LSTM	3.2	96.4
Bi-LSTM+Attention	3.6	94.6

Table 4 records the average response time and throughput of the different models in the simulated network environment. Although the introduction of the defense model leads to a slight increase in response time and a slight decrease in throughput, the Bi-LSTM and Bi-LSTM+Attention models are better able to maintain high network performance compared to the other models.

In order to comprehensively evaluate the model performance, we introduced statistical significance tests such as t-tests on the basis of existing evaluation indicators to verify the reliability of the results. In addition to false positive and false negative rates, we also reported comprehensive indicators such as accuracy, recall, and F1 score. Specifically, the Bi-LSTM+Attention model achieved an accuracy of 98%, a recall of 95%, and an F1 score of 96.5% on the UNSW-NB15 dataset. These indicators not only demonstrate the high accuracy of the model in detecting illegal network scanning, but also show that it has high practical value in practical applications.

Table 5: Model performance comparison

Model/Method	Accuracy (%)	Recall (%)	F1 Score (%)	False Positive Rate (%)	False Negative Rate (%)	t-test (p-value)
Bi-LSTM+Attention	98.0	95.0	96.5	1.5	5.0	< 0.05
Rule-Based System	80.0	75.0	77.4	10.0	25.0	-
LSTM Model	85.0	82.0	83.5	8.0	18.0	< 0.05
LSTM with Attention Mechanism	90.0	88.0	89.0	5.0	12.0	< 0.05
Bidirectional LSTM (Bi-LSTM)	92.0	90.0	91.0	4.0	10.0	< 0.05

In Table 5, through t-tests, we found that the Bi-LSTM+Attention model showed significant differences from the rule-based system and other LSTM variants in multiple key performance indicators ($p < 0.05$), further confirming the effectiveness and superiority of the new method. In addition, the model performs particularly well when dealing with complex and variable network traffic, and can effectively reduce the false alarm rate while maintaining a high detection rate. These results show that the Bi-LSTM+Attention model is not only theoretically advantageous, but also has high practical value in practical applications.

Table 6: Resource consumption

mould	Average CPU utilization (%)	Average Memory Usage (MB)
defenseless	3.1	230
LSTM model	5.8	320
LSTM+Attention	6.5	350
Bi-LSTM	4.9	280
Bi-LSTM+Attention	5.4	300

Table 7: Network latency and energy consumption

mould	Average network latency (μs)	Average energy consumption (W)
defenseless	75	200
LSTM model	90	250
LSTM+Attention	95	270
Bi-LSTM	85	230
Bi-LSTM+Attention	90	260

Table 6 shows the average consumption of CPU and memory resources by the different models during operation. The LSTM+Attention model is slightly higher in terms of resource consumption, but all the models are within acceptable resource usage, indicating that these models can effectively run-on existing network devices. Table 7 evaluates the impact of the different models on network latency and energy consumption. The Bi-LSTM model performs the best in terms of network latency and energy consumption, suggesting that it is effective in controlling operational costs while maintaining network performance.

In summary, the Bi-LSTM+Attention model performs the best in terms of comprehensive defense effect, false alarm rate and missed alarm rate, and at the same time has a relatively small impact on network performance, making it an efficient network defense solution.

4.3 Discussion

The technical architecture in this study demonstrates significant innovative advantages, especially in terms of dynamism and intelligence. The anonymity of the network is effectively improved through dynamic IP address assignment and geolocation obfuscation, making it difficult for mapping attackers to target the real resource locations. The synergy of intelligent firewall and IPS, the use of fuzzy logic system, and the application of Markov model and LSTM not only enhances the ability to identify malicious behaviors, but also significantly improves the response speed. In particular, the LSTM model improves the accuracy of anomaly detection through the attention mechanism and bi-directional structure, demonstrating the great potential of deep learning in complex network defense.

Honeypot technology deploys false resources and services to attract and mislead attackers, and can effectively collect attacker behavior information. However, honeypot technology consumes a lot of resources, requires continuous maintenance, and is easily identified and bypassed by advanced attackers. In contrast, the Bi-LSTM+Attention model is more economical in terms of resource consumption and does not require additional hardware or continuous manual maintenance. In addition, the Bi-LSTM+Attention model can automatically adapt to new threats by learning network traffic patterns, reducing dependence on manual intervention. Although honeypot technology has advantages in collecting intelligence, the Bi-LSTM+Attention model performs better in terms of false positive rate and false negative rate, reaching 1.5% and 5.0% respectively, which are significantly lower than the 10% and 25% of honeypot technology.

Traffic obfuscation changes network communication patterns and features, making it difficult for scanning tools to correctly identify service types. Although traffic obfuscation performs well in reducing false positive rates, it has limited effect on advanced scanning strategies and may affect the normal transmission of legitimate traffic. The Bi-LSTM+Attention model uses deep learning algorithms to more accurately identify and classify network traffic, which not only reduces false positive rates but also improves detection rates. Specifically, the Bi-LSTM+Attention model has a false positive rate of 1.5%, while the traffic obfuscation technology has a false positive rate of 8%. In addition, the Bi-LSTM+Attention model performs particularly well when dealing with complex and changing network traffic, and can effectively reduce false positive rates while maintaining high detection rates.

Dynamic Address Translation (NAT) increases the difficulty for attackers by changing IP addresses between internal and external networks. However, NAT is limited in its effectiveness when dealing with complex and large-scale scanning activities. The Bi-LSTM+Attention model can automatically adapt to new threats by learning network traffic patterns, thereby showing higher detection rates and lower false positive rates in complex and large-scale scanning activities. NAT has a false positive rate of 5%, while the Bi-LSTM+Attention model has a false positive rate of only 1.5%.

Behavior-based detection systems use machine learning models to automatically analyze network traffic patterns and improve detection accuracy. However, these systems usually require a large amount of data for training and have limited generalization capabilities for new attacks. The Bi-LSTM+Attention model improves detection performance by introducing an attention mechanism to enhance the model's focus on key features. In practical applications, the Bi-LSTM+Attention model outperforms the behavior-based detection system in terms of accuracy, recall, and F1 score.

Although the Bi-LSTM+Attention model performs well on multiple key performance indicators, it has high computational overhead and implementation complexity. The time complexity of the training phase is O(T * (D * H^2 + H)), and the time complexity of the inference phase is O(T * (D * H + H)). This makes it challenging to deploy the model in a resource-constrained environment. However, this computational overhead is reasonable considering its significant advantages in improving the level of network security protection. Future work can explore optimization algorithms to further reduce computational costs and make it more applicable in more scenarios.

Through the above comparison and analysis, we can conclude that the Bi-LSTM+Attention model has significant advantages in illegal network scanning defense. It not only performs well in detection rate and false alarm rate, but also can effectively adapt to complex network environments. Despite the certain computational overhead and implementation complexity, the security and reliability improvements it brings make it a technical solution worthy of promotion.

Limitations: Despite the remarkable results, there are some limitations of the proposed technical solution. The first one is the resource consumption issue, such as the high performance of the LSTM model which requires high computational resources and may be difficult to deploy in resource-limited environments. Secondly, the false alarm and omission rates, although significantly reduced, need to continue to be optimized to reduce the interference with normal operations. Further, the complexity of the technology implementation may pose a challenge to small and medium-sized enterprises, requiring specialized knowledge and maintenance costs.

5 Conclusion

In this study, we successfully developed and validated an innovative set of network anti-mapping security access techniques, which have achieved significant results in enhancing network defenses, improving anonymity and ensuring secure data transmission. The comprehensive design of the technical architecture, especially the integration of dynamic policies and intelligent algorithms, effectively counteracts the complex security threats in the modern network environment. Experimental data analysis proves that the bidirectional LSTM model with the introduction of the attention mechanism improves the accuracy of anomaly detection while reducing the false alarm rate of normal network activities, indicating that the combination of deep learning and traditional security technologies is an effective way to enhance the performance of network defense. Despite the obvious advantages of the technology, including dynamism, intelligence, and efficient defense against multiple attack types, we also recognize some challenges in the implementation of the technology. The resource consumption problem is a key barrier to the deployment of current deep learning models, especially in scenarios with limited computational resources. In addition, the complexity of the technique requires higher maintenance costs and specialized skills, which may limit its widespread adoption in SMEs. Therefore, future research should focus on model lightweighting, resource optimization, and simplifying the deployment process to facilitate the technology's popularity. Compared with existing antimapping techniques, the technical framework in this study shows significant advantages in terms of dynamic adaptability, intelligent response, and accuracy, especially in dealing with complex network behavior sequence prediction and anomaly detection tasks. However, continuous performance optimization, further reduction of false alarm and omission rates, and exploration of the convergence of new technologies, such as the application of quantum computing and edge computing in security, will be the key directions for future development.

This paper proposes an innovative network reverse mapping security access technology to cope with the increasingly frequent illegal network scanning behaviors. By combining dynamic IP address allocation, port obfuscation, traffic camouflage and behavior analysis, we build a more robust network security protection system. Experimental results show that the Bi-LSTM+Attention model achieves 98% accuracy on the UNSW-NB15 dataset and reduces the false alarm rate by 30%. This technology effectively identifies and intercepts illegal scanning behaviors in the pilot network while maintaining low false alarm and missed alarm rates. Compared with existing methods, our method has significant advantages in detection accuracy and resource efficiency, providing a more reliable solution for network security.

This paper discusses the challenges that small and medium-sized enterprises (SMEs) face when adopting these technologies, including limited computing resources and deployment complexity. To alleviate these challenges, we recommend using model compression techniques, such as pruning and quantization, to simplify the deployment process and reduce computing resource requirements. In addition, SMEs should consider leveraging off-the-shelf solutions from cloud service providers to reduce initial investment costs. At the same time, potential regulatory issues, such as the impact of GDPR on network traffic monitoring, can help enterprises ensure compliance. With these measures, SMEs can implement and manage cybersecurity solutions more effectively.

Funding

This study was supported by State Grid Shanxi Electric Power Company Science and Technology Project Research (No.52053023001U).

References

[1] Adi K, Hamza L, Pene L. Automatic security policy enforcement in computer systems. Computers & Security. 2018; 73: 156-71. https://doi.org/10.1016/j.cose.2017.10.012

[2] Paananen H, Lapke M, Siponen M. State of the art in information security policy development. Computers & Security. 2020; 88: 101615. https://doi.org/10.1016/j.cose.2019.101615

[3] Kanimozhi S, Kannan A, Devi KS, Selvamani K. Secure cloud-based e-learning system with access control and group key mechanism. Concurrency and Computation-Practice & Experience. 2019; 31(12): e5106. https://doi.org/10.1002/cpe.5106

[4] Al-Amri B, Sami G, Alhakami W. An Effective Secure MAC Protocol for Cognitive Radio Networks. Computer Systems Science and Engineering. 2022; 42(1): 133-48. https://doi.org/10.32604/csse.2022.020123

[5] Chiu WY, Meng WZ, Jensen CD. my data, my control: a secure data sharing and access scheme over blockchain. Journal of Information Security and Applications. 2021; 63: 102994. https://doi.org/10.1016/j.jisa.2021.102994.

[6] Yang D, Wang BC, Ban XH. Fully secure non-monotonic access structure CP-ABE scheme. KSII Transactions on Internet and Information Systems. 2018; 12(3): 1315-29. https://doi.org/10.3837/tiis.2018.03.019

[7] Suebsombut P, Sekhari A, Sureephong P, Belhi A, Bouras A. Field Data Forecasting Using LSTM and Bi-LSTM Approaches. Applied Sciences-Basel. 2021; 11(24): 11957. https://doi.org/10.3390/app112411957.

[8] Sonkamble RG, Bongale AM, Phansalkar S, Sharma A, Rajput S. Secure Data Transmission of Electronic Health Records Using Blockchain Technology. Electronics. 2023; 12(4): 1003. https://doi.org/10.3390/electronics12041003.

[9] Agrawal R, Singhal S, Sharma A. Blockchain and fog computing model for secure data access control mechanisms for distributed data storage and authentication using hybrid encryption algorithm. Cluster Computing. 2024; 27(1), 1–15. https://doi.org/10.1007/s10586-023-04120-9

[10] Sureshkumar T, Lingaraj M, Anand B, Premkumar T. Non-dominated sorting particle swarm optimization (NSPSO) and network security policy enforcement for Policy Space Analysis. International Journal of Communication Systems. 2018; 31(10): e3576. https://doi.org/10.1002/dac.3576.

[11] Khan I, Ghani A, Saqlain SM, Ashraf MU, Alzahrani A, Kim D. Secure Medical Data Against Unauthorized Access Using Decoy Technology in Distributed Edge Computing Networks. IEEE Access. 2023; 11: 144560-73. https://doi.org/10.1109/ACCESS.2023.3344168

[12] Pinto S, Machado P, Oliveira D, Cerdeira D, Gomes T. Self-secured devices: high performance and secure I/O access in TrustZone-based systems. Journal of Systems Architecture. 2021; 119: 102238. https://doi.org/10.1016/j.sysarc.2021.102238

[13] Yang J, Chen YH, Du SY, Chen BD, Principe JC. IA-LSTM: Interaction-Aware LSTM for Pedestrian Trajectory Prediction. IEEE Transactions on Cybernetics. 2024; 57(4): 3904-3917, https://doi.org/10.1109/TCYB.2024.3359237.

[14] Meng YF, Huang ZQ, Shen GH, Ke CB. A security policy model transformation and verification approach for software defined networking. Computers & Security. 2021; 100: 13206. https://doi.org/10.48550/arXiv.2005.13206.

[15] Susilo W, Jiang P, Lai JC, Guo FC, Yang GM, Deng RH. Sanitizable Access Control System for Secure Cloud Storage Against Malicious Data Publishers. IEEE Transactions on Dependable and Secure Computing. 2022; 19(3): 2138-48. https://doi.org/10.1109/TDSC.2021.3058132

[16] Sureshkumar T, Anand B, Premkumar T. Efficient Non-Dominated Multi-Objective Genetic Algorithm (NDMGA) and network security policy enforcement for Policy Space Analysis (PSA). Computer Communications. 2019; 138: 90-7. https://doi.org/10.1016/j.comcom.2019.03.008

[17] Hu T, Yang SQ, Wang YP, Li GL, Wang YL, Wang G, Yin MY. N-Accesses: a Blockchain-Based Access Control Framework for Secure IoT Data Management. Sensors. 2023; 23(20): 8535; https://doi.org/10.3390/s23208535.

[18] Varma IM, Kumar N. A comprehensive survey on SDN and blockchain-based secure vehicular networks. Vehicular Communications. 2023; 44: 100663. https://doi.org/10.1016/j.vehcom.2023.100663.

[19] Lin HY, Tsai TT, Wu HR, Ku MS. Secure access control using updateable attribute keys. Mathematical Biosciences and Engineering. 2022; 19(11): 11367-79. https://doi.org/10.3934/mbe.2022529

[20] Sivaselvan N, Bhat KV, Rajarajan M, Das AK. A New Scalable and Secure Access Control Scheme Using Blockchain Technology for IoT. IEEE Transactions on Network and Service Management. 2023; 20(3): 2957-74. https://doi.org/ 10.1109/TNSM.2023.3246120

[21] Wu YC, Sun R, Wu YJ. Smart City Development in Taiwan: From the Perspective of the Information Security Policy. Sustainability. 2020;12(7): 2916; https://doi.org/10.3390/su12072916.

[22] Wang SP, Wang X, Zhang YL. A Secure Cloud Storage Framework with Access Control Based on Blockchain. IEEE Access. 2019; 7: 112713-25. https://doi.org/10.1109/ACCESS.2019.2929205

[23] Omala AA, Mbandu AS, Mutiria KD, Jin CH, Li FG. Provably Secure Heterogeneous Access Control Scheme for Wireless Body Area Network. Journal of Medical Systems. 2018; 42(6): 108. https://doi.org/10.1007/s10916-018-0964-z

[24] Yang Y, Liu XM, Guo WZ, Zheng XH, Dong C, Liu ZQ. Multimedia access control with secure provenance in fog-cloud computing networks. Multimedia Tools and Applications. 2020; 79(15-16): 10701-16. https://doi.org/10.1007/s11042-020-08703-1

[25] Kumari A, Gupta R, Tanwar S, Kumar N. A taxonomy of blockchain-enabled softwarization for secure UAV network. Computer Communications. 2020; 161:304- 23. https://doi.org/10.1016/j.comcom.2020.07.042

[26] Calzavara S, Rabitti A, Bugliesi M. Semantics-Based Analysis of Content Security Policy Deployment. ACM Transactions on the Web. 2018; 12(2): 1-36. https://doi.org/10.1145/3149408

[27] Zhang J, Chen AM, Zhang P. Provably Secure Data Access Control Protocol for Cloud Computing. Symmetry-Basel. 2023; 15(12): 2111; https://doi.org/10.3390/sym15122111.

[28] Rostami E, Karlsson F, Gao S. Requirements for computerized tools to design information security policies. Computers & Security. 2020; 99: 102063. https://doi.org/10.1016/j.cose.2020.102063

[29] Merhi MI, Ahluwalia P. Predicting Compliance of Security Policies: Norms and Sanctions. Journal of Computer Information Systems. 2023; 64(5), 683–697. https://doi.org/10.1080/08874417.2023.2241413

[30] Yang J H, Lin I C, Chien P C. Data Sharing Scheme for Cloud Storage Service Using the Concept of Message Recovery. Informatica, 2017, 28(2): 375-386. https://doi.org/10.15388/Informatica.2017.134

[31] Muthusenthil B, Kim H, Prasath V B. Location verification technique for cluster based geographical routing in MANET. Informatica, 2020, 31(1): 113-130. https://doi.org/10.15388/20-INFOR402