Secure Intrusion Detection based on Homomorphic Encryption and Secret Sharing

Peiyin Yao

University of Jinan, Jinan, Shandong, 250000, China

2826314381@qq.com

Abstract. With the increasing complexity of network attack methods, there are serious data leakage risks and system stability problems in traditional Intrusion Detection System (IDS) in data collection, transmission, a1nalysis and storage. Therefore, this paper proposes a Private Secure Intrusion Detection System (PSIDS) that integrates Fully Homomorphic Encryption (FHE) and Shamir secret sharing mechanism. Build an end-to-end data protection and anti-attack system. PSIDS introduces an encryption and decryption layer on the basis of the traditional three-layer architecture, and uses the BFV algorithm to encrypt the original traffic, so that the detection node can directly perform detection and analysis on the encrypted data, achieving "data available but not visible"; At the same time, the Shamir (t, n) threshold secret sharing mechanism is introduced in the system, and the key data of the intrusion detection model are divided into n shares for distributed storage. Only when at least t nodes cooperate, the original information can be reconstructed, which effectively resists single-point attacks and improves the robustness of the system. The experiment compares PSIDS with Centralized IDS, Distributed IDS and Machine Learning based IDS. The results show that PSIDS has achieved breakthroughs in data privacy and system stability. The collaborative application of FHE and secret sharing technology in IDS is realized for the first time.

Keywords: Intrusion Detection System, FHE, BFV, Secret Sharing, Privacy Protection, Network, Data.

1 Introduction

1.1 Research Background

Intrusion Detection System (IDS) [1] is an important network protection measure. It plays a vital role in monitoring network traffic, identifying abnormal behaviors and preventing intrusion attacks. Nowadays, network attack methods [2][4] are becoming increasingly diverse. It seriously threatens users' personal privacy and national key information security [4] through data leakage [4].

For example, in 2023, a bank was attacked by the APT organization Lazarus. And 23 million users' data was leaked (source: FireEye annual report). The direct economic

A. Mallik et al. (eds.), *Proceedings of the 2025 6th International Conference on Management Science and Engineering Management (ICMSEM 2025)*, Atlantis Highlights in Economics, Business and Management 4,
https://doi.org/10.2991/978-94-6463-845-5_98

loss exceeded one billion yuan. Therefore, how to improve the privacy protection ability of IDS in data collection, transmission, storage and analysis has become the core problem to be solved in the field of cybersecurity.

1.2 Privacy and Security Flaws of Traditional IDS

Most of the data in Traditional IDS [4] exists in plaintext form which provides a natural breakthrough for attackers.

Data collection stage: Attackers can steal the original collected data by implanting malware or falsifying data sources, resulting in the leakage of the original data.

Data transmission phase: Unencrypted packets are easily intercepted.

Data storage phase: The database is attacked and the system stability is destroyed.

Detection and analysis stage: If the system rights are not properly managed, sensitive information will also be leaked.

Once IDS is destroyed, and the barrier of network protection disappears, the client will easily receive traffic attacks, which will destroy the confidentiality, integrity and availability of the network. For example, in 2022, the IDS of an internet company failed to identify the JNDI injection attack using the Log4j2 vulnerability due to unencrypted log data and lagging rule base updates. Attackers continuously penetrate the system for 3 months and steal over 50GB of core business data. This example reflects the serious impact when IDS fails. Therefore, improving the data privacy protection capabilities and system stability of IDS has become an important issue to be solved.

1.3 Overview of Technical Solution

In order to cope with the above challenges, this paper proposes an intrusion detection system, which is called Privacy Security Intrusion Detection System (PSIDS), which combines Fully Homomorphic Encryption (FHE) and secret sharing mechanism.

FHE. Based on the RLWE problem, FHE [2] supports arbitrary polynomial operations on ciphertext, and the decryption results are equivalent to plaintext operations. The ideal security state of "invisible" data is realized. We use BFV algorithm to encrypt the data, and the intrusion detection technology based on machine learning is combined for analysis and operation.

Shamir secret sharing mechanism. The basic idea is that the distributor decomposes the secret s into n secrets through the secret polynomial and distributes it to the holder. Any secret not less than t can recover the ciphertext. In this paper, the key data of intrusion detection model are divided into multiple shares, which are stored in different nodes. Only when the threshold conditions are met, the original data can be recovered, and the robustness [5] and anti-attack ability of the system can be enhanced.

Private Secure Intrusion Detection System (PSIDS). The FHE [3] and secret sharing technology [5] in intrusion detection system can achieve double breakthroughs in the dimension of data security. Through FHE, the detection node can directly detect the ciphertext by using machine learning algorithms, thus avoiding the risk of leakage of plaintext data in the process of transmission and analysis. At the same time, the (t, n) threshold secret sharing scheme is applied to divide the key information of the intrusion

detection model into n shares, which are scattered and stored in different detection nodes. Only when any t nodes cooperate can the original information be reconstructed. This way effectively resists single point attacks, greatly improves the robustness of the system and ensures the stable operation of the system.

2 Methods

2.1 System Architecture

On the basis of the traditional three-layer architecture of intrusion detection system, data acquisition layer, detection and analysis layer, and response processing layer, PSIDS proposed in this paper adds encryption layer and decryption layer, and introduces distributed monitoring factor access mechanism to achieve higher level of data privacy protection and system stability.

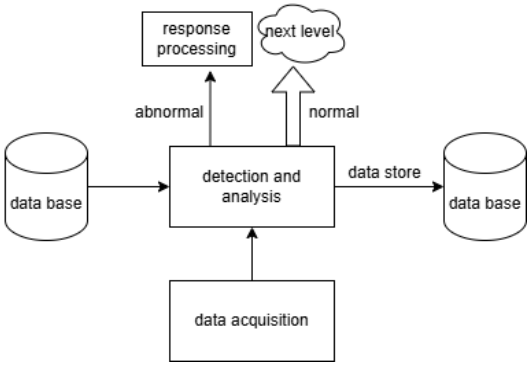

Fig. 1. Traditional Intrusion Detection System

As shown in Fig. 1, the traditional IDS is divided into three layers, the data acquisition layer, the detection and analysis layer and the response processing layer [4].

Data acquisition layer: This layer collects original data from the network. Data sources include network traffic, system logs, etc. In the aspect of network traffic collection, the data packets flowing through devices are obtained through the network interface, and the data packets are analyzed to capture the details of network activities.

Detection and analysis layer: Its main task is to conduct in-depth analysis of the preprocessed data according to the preset method to determine whether there is intrusion behavior. Common detection methods include feature-based detection and anomaly-based detection. Now, intrusion detection methods based on machine learning have been developed, which greatly improves the detection accuracy and efficiency.

Response processing layer: Once the detection and analysis layer find a intrusion behavior, the response processing layer will take measures to prevent the further spread of the attack. Response measures include sending alerts to notify system administrators, recording details of intrusion events, etc. In addition, the response processing layer can automatically adjust the security policy of the system according to the severity of the intrusion event to improve the overall security of the system.

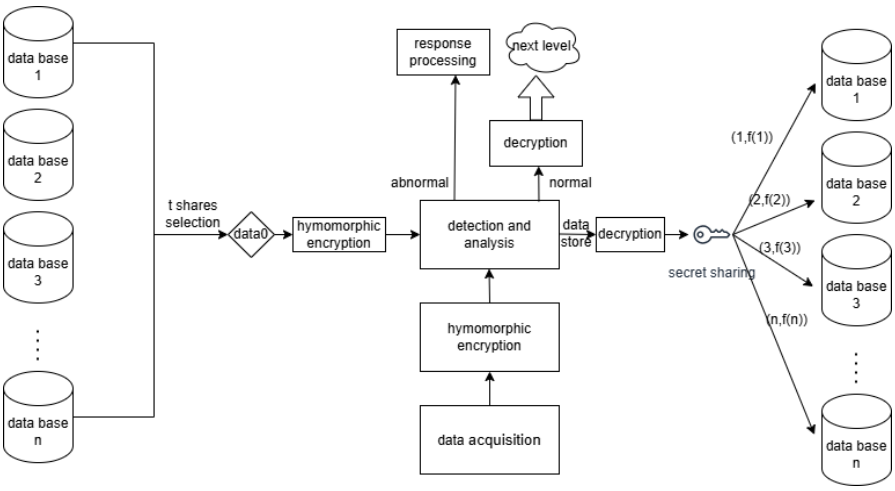

Fig. 2. The improved intrusion detection system: PSIDS

As shown in Fig. 2, PSIDS encrypts the data using BFV fully homomorphic encryption scheme after data extraction, and then performs the operation of detection and analysis layer. If the detection result is normal, it is decrypted by fully homomorphic encryption algorithm, and finally passe to the next layer.

When the data is taken from the database to participate in the operation of detection and analysis. The data divided in t-threshold databases are retrieved to jointly derive the original data, and use the same homomorphic encryption operation on the data to achieve the consistency of calculation.

When the data written in the database is to be updated by the detection and analysis layer, the homomorphic encrypted data is decrypted to obtain the original data, and the original data S is divided by Shamir algorithm, and the divided secrets are stored in n databases respectively, so as to realize the distributed secret storage [5] of data.

The detection and analysis layer of this system uses intrusion detection technology based on machine learning [1], so as to adapt to the encrypted data processing.

2.2 BFV Fully Homomorphic Encryption Scheme

BFV scheme is one of the most widely used fully homomorphic encryption frameworks at present, and its theoretical basis is based on Ideal Lattices and Ring Learning With Errors (RLWE). BFV is more suitable for the computing resource limitation of real-time traffic detection because it supports low-degree polynomial operations and has a smaller key size.

When the BFV algorithm is applied to the data processing of the intrusion detection system, the data is transmitted in ciphertext. The system can directly detect and analyze the encrypted data. This prevents data leakage during system operation and best ensures data privacy.

The BFV scheme mainly consists of four core algorithms: Key generation, encryption, homomorphic operation, decryption.

Key Generation.

Define a polynomial ring.

$$R = Z[x]/(x^N + 1) \tag{1}$$

N is a power of 2.

Choose the modulus q and the noise distribution χ.

Randomly generate the private key: $s \in \chi^N$. N elements are sampled from the noise distribution.

Compute public key component. Random sampling from R_q: $a \in R_q$

Sampling from the noise distribution: $e \in \chi$

$$b = -(a \cdot s + e) \bmod q \tag{2}$$

Output public key and private key: PK = (b, a). SK=s.

Generate the relinearization key: RLK

$$t = s^2 \tag{3}$$

$$b' = -(a' \cdot s + e' + q \cdot t) \bmod q^2 \tag{4}$$

$$RLK = (b', a') \tag{5}$$

Encryption.

Input: plaintext m $\in$ {0, 1} ^ N, public key PK = (b, a)

Output: ciphertext c = (c_0, c_1)

Encoding m as a polynomial: m (x) $\in$ R_q

Sampling random polynomial: u $\in$ {0, 1} ^ N

Sampling noise polynomials: e_0, e_1 $\in$ χ

Calculation:

$$c_0 = b \cdot u + e_0 + m \bmod q \tag{6}$$

$$c_1 = a \cdot u + e_1 \bmod q \tag{7}$$

Output: ciphertext c = (c_0, c_1)

Homomorphic Operation.

Homomorphic addition.

Input: ciphertext $c_1 = (c_{10}, c_{11})$, $c_2 = (c_{20}, c_{21})$

Output: ciphertext $c_{sum} = (c_{sum0}, c_{sum1})$

Calculation:

$$c_{sum0} = c_{10} + c_{20} \bmod q \tag{8}$$

$$c_{sum1} = c_{11} + c_{21} \bmod q \tag{9}$$

Output: $c_{sum} = (c_{sum0}, c_{sum1})$

Homomorphic multiplication.

Input: ciphertext $c_1 = (c_{10}, c_{11})$, $c_2 = (c_{20}, c_{21})$, relinearization key RLK
Output: ciphertext $c_{prod} = (c_{prod0}, c_{prod1})$
Calculation:

$$c_1 \cdot c_2 = (c_{10} \cdot c_{20}, c_{10} \cdot c_{21} + c_{11} \cdot c_{20}, c_{11} \cdot c_{21}) \tag{10}$$

Re-linearization using RLK to convert triples to binaries.
Output: $c_{prod} = (c_{prod0}, c_{prod1})$

Decryption.

Input: ciphertext $c = (c_0, c_1)$, private key SK = s
Output: plaintext m
Calculation:

$$m' = c_0 + c_1 \cdot s \; mod \; q \tag{11}$$

Decode m' to plaintext m.

2.3 Detection Factor Access Scheme

Based on the storage mode of Shamir secret sharing scheme, some key detection factors are split and stored in various databases in multiple directions and distributed.

Shamir secret sharing algorithm: Assume that the secret value to be shared is S as a constant a_0 of a polynomial of degree $t - 1$, the polynomial is:

$$f(x) = a_{t-1}x^{t-1} + \cdots + a_1 x + a_0 \tag{12}$$

Where a_i is a randomly selected coefficient on the finite field GF (p) ($i = 0, 1, \cdots, t - 1$). Here, p needs to be a large prime number to ensure the safety and uniqueness of polynomial operations. Then, n different points $x_1, x_2, \cdots, x_n$ ($n > t$) are selected on the finite field GF (p), and n secret shares (x_i, y_i) are obtained by calculating $y_i = f(x_i)$ ($i = 1, 2, \cdots, n$). These shares are scattered and stored in different nodes, and the original secret cannot be derived from a single or less than t shares, thus realizing "t-threshold" security. When the secret needs to be restored, t shares are arbitrarily selected and the Lagrange interpolation formula is used:

$$f(x) = \sum_{i=1}^{t} y_i \frac{\prod_{j \neq i}(x - x_i)}{\prod_{j \neq i}(x_i - x_j)} \tag{13}$$

The original polynomial can be reconstructed. Since the secret value S is the constant term a_0 of the polynomial, S can be directly obtained after the polynomial is reconstructed.

When an individual database is destroyed, the original data can be recovered as long as the threshold t of recovered data can still be reached, which can greatly improve the robustness of the system.

3 Result

This paper aims to construct a more secure intrusion detection system. In order to verify the progress of this scheme, the experiment through the methods of investigation, analysis and comparison. The intrusion detection systems currently used in the network are compared from the aspects of data security and system security, and clear results are shown in Table 1.

Table 1. Comparison results of each system

System Type	Data Privacy	Database Robustness	Accuracy
Ordinary IDS	×	×	Baseline
Distributed IDS	×	✓	Higher
ML-based IDS	×	×	Even Higher
PSIDS	✓	✓	Even Higher

Data privacy assessment, Ordinary IDS, Distributed IDS and Machine Learning-based IDS (ML-based IDS) do not protect the data flowing through the system, but the PSIDS in this paper realizes the whole process of ciphertext transmission and analysis by FHE on the original traffic, which significantly reduces the risk of data leakage.

Database robustness evaluation, Ordinary IDS and ML-based IDS can't continue to run stably when the database is destroyed, while Distributed IDS and PSIDS in this paper have strong robustness. PSIDS can tolerate the damage of up to $n - t$ database nodes, and can still recover the original data and maintain the detection function even if some nodes are lost.

In terms of detection accuracy, Ordinary IDS is used as the benchmark for comparison, Distributed IDS has higher accuracy, and ML-based IDS has higher accuracy. Because the detection module of PSIDS in this paper combines the detection method of machine learning, it has higher accuracy similar to ML-based IDS.

Although the encryption overhead of PSIDS has increased compared to other systems, it is worthwhile to sacrifice a certain amount of computing efficiency in exchange for data privacy in scenarios with high data privacy requirements. In terms of performance trade-offs, the system can optimize operational efficiency through methods such as hardware acceleration or approximate homomorphic operations.

In applications, PSIDS will play an important role in areas with higher privacy requirements such as medical care and finance. For example, in financial transactions, if the detection system's database is damaged, the attack cannot be accurately prevented, critical transaction information may be stolen. Alternatively, transaction data leaks during system operation could lead to severe financial losses.

4 Conclusions

In the research of network intrusion detection system, traffic data is faced with this crisis of data leakage in the process of system processing traffic, and it is difficult for the system to maintain stability in the attack on database of intrusion detection system, this paper proposes a double security reinforcement scheme for intrusion detection system, that is, homomorphic encryption method to ensure the privacy of data in intrusion detection system and prevent the data flowing through intrusion detection system from being leaked; The secret sharing method ensures the security of data storage in intrusion detection system and enhances the robustness of the system.

For the first time, FHE and Shamir threshold scheme are jointly applied to IDS to achieve end-to-end privacy protection. Experimental research shows that this scheme can effectively detect intrusion behavior, and at the same time, it can significantly improve the privacy protection ability of data, strengthen the stability of the system, and provide a reliable solution for network security protection.

Future-oriented research, based on the scheme of this paper. We can conduct research on lightweight encryption algorithms to adapt to the performance requirements of real-time monitoring scenarios. Research and build a cross-agency federated IDS network to improve collaborative defense capabilities against new attacks such as zero-day vulnerabilities. We can also migrate and expand the ideas proposed in this paper and try to apply them to wider cybersecurity domains such as the Industrial Internet and the Internet of Vehicles.

References

1. Zhang, X., Wang, X.F., Wang, Y.Z., Shang, Y., Wang, F.M., Zeng, Y.M. (2024) Overview of network intrusion detection technology based on machine learning. Cyber Security and Data Governance, 43: 1-18. 10.19358/j.issn.2097-1788.2024.12.001.
2. Li, R.Q., Yi, Q., Huang, Y.X., Jia, C.F. (2024) Privacy-preserving convolutional neural network inference scheme based on homomorphic ciphertext transformation. Journal on Communications, 45: 12-23. 10.11959/j.issn.1000-436x.2024216.
3. Wu, T., Zhang, S.S. (2025) Scalable blockchain privacy protection scheme based on homomorphic encryption and zero-knowledge proof. Application Research of Computers, 42: No.7. 10.19734/j.issn.1001-3695.2025.01.0002.
4. Ceviz, O., Sadioglu, P., Sen, S., Vassilakis, V.G. (2025) A novel federated learning-based IDS for enhancing UAVs privacy and security. Internet of Things, 31: 1-20. https://doi.org/10.1016/j.iot.2025.101592.
5. Hineman, A., Blaum, M. (2022) A Modified Shamir Secret Sharing Scheme With Efficient Encoding. IEEE COMMUNICATIONS LETTERS, 26: 758-762. 10.1109/LCOMM.2022.3144375.