EPCAD: Efficient and Privacy-Preserving Data Anomaly Detection Scheme for Industrial Control System Networks

Hanjun Gao¹, Liang Yuan², Fei Yin¹ and Gang Shen²*

¹ China Nuclear Power Operation Technology Corporation, LTD, Wuhan Hubei, 430070, China
² School of Computer Science, Hubei University of Technology, Wuhan Hubei, 430068, China
*Corresponding author’s e-mail: shengang@hbut.edu.cn

Abstract. With the integration of Internet and industry, traditional industrial control system (ICS) has faced cyber-security risks and challenges due to interacting with the Internet. In this paper, we propose an efficient and privacy-preserving data anomaly detection scheme (EPCAD) for ICS. The scheme, a combination of a homomorphic cryptosystem and the support vector machine (SVM) algorithm, has the capability of efficiently detecting anomalies in data without compromising data information. Security analysis result shows that the EPCAD scheme has the following advantages: protect the data in the programmable logic controller (PLC); ensure that the classification parameters of anomaly detection server (ADS) are not compromised. Performance evaluation analysis demonstrates that the EPCAD scheme has significant advantages in terms of computational costs and communication overheads.

1. Introduction

In recent years, industrial control system (ICS) has been widely used in the significant domains such as nuclear power, traffic, chemical, public health and financial services. Compared with the traditional ICS, the operation of modern ICS is implemented via distributed control system based on computer and network communication. As shown in figure 1, the comprehensive architecture of ICS is mainly composed of field control layer, process control layer, supervisory control layer and enterprise management layer[1]. Due to the transition from isolated environment to open environment, ICS is exposed to a wide range of malicious network attacks[2]. In the traditional ICS scheme, the encryption and authentication of data are not applied in the communication. Therefore, the attacker can eavesdrop on communication data by parsing the Modbus address and function code[3]. However, the data in ICS contain important information such as PLC instructions. The leaked information will not only cause serious economic losses to the enterprise, but even worse, the adversary may attack the system by manipulating control instructions. Therefore, it is imperative to protect the data’s privacy in ICS.

Support vector machine (SVM), a data classification algorithm, is widely used in different fields[4-7]. SVM mainly includes two phases: training and testing. And the unlabeled data samples can be classified by SVM’s classifier during the testing phase. The classification parameters are obtained by training the characteristics of different types of data sets. Therefore, classifiers trained with normal data sets are used to detect the anomaly of control data in ICS. Although the SVM is widely used in many intrusion detection schemes for ICS[8-9], the confidentiality of data and the efficiency of
abnormal data detection are rarely taken into consideration. Therefore, we propose an efficient and privacy-preserving data anomaly detection scheme for ICS with SVM, which can effectively detect the anomaly of data without compromising data information. The important contributions of this paper are as twofold.

- Firstly, we propose an efficient and privacy-preserving data anomaly detection scheme for ICS, which uses the homomorphic encryption technology to encrypt data, and uses the SVM algorithm to quickly detect anomaly the data without compromising data information. The proposed scheme not only realizes the confidentiality of data and SVM’s classification parameters, but also improves the efficiency of abnormal data detection.

- Secondly, we develop a lightweight method to obtain the ciphertext of the classification label, which greatly reduces the computational cost and communication overhead of ICS. Additionally, the proposed EPCAD scheme adopts a signature technology to ensure the data integrity.

2. Related work
Because intrusion detection technology has the ability to identify potential abnormal behaviors, it has been widely used in ICS. To detect illegal data, Morris et al.[10] proposed a Modbus intrusion detection technology based on detection software. Hong et al.[11] detected abnormal or malicious behavior in multicast messages in substation systems according to the IEC 61850 standards. However, failing to detect unknown attacks and long packet parsing time are the disadvantages of detection method for protocol analysis. Therefore, Stavroulakis and Stamp et al.[12] provided an intrusion detection technology about traffic mining, which can identify the abnormal behaviors and the normal behaviors of the system. Their scheme can detect multiple types of intrusions such as packet tampering, DoS, reply and MITM. In[13], Ashfaq et al. proposed a semi-supervised neural network learning mechanism, in which they used a small amount of labelled data to train a fuzzy classifier. However, training neural network model requires huge computational cost. To solve this problem, Linda et al.
[14-15] proposed a fuzzy logic intrusion detection method, which consumed less computational cost than neural network.

In addition, SVM algorithm is also widely used in the detection system based on traffic mining [8-9]. Maglaras and Jiang[8] presented an intrusion detection scheme for ICS based on One-Class SVM. In this scheme, it can achieve off-line training, but does not need any prior knowledge of attack categories and labelled training data. In[9], Usha and Kavitha proposed a MAC intrusion detection method based on normalized gain. With the optimal set of features, they use the SVM algorithm to detect and classify MAC 802.11 intrusions, thus achieving a better tradeoff between detection accuracy and learning time.

3. System model and security requirements

3.1. System model
As shown in figure 2, two entities anomaly detection server and operator station are involved in our scheme. The specific description is as follows:

- **Anomaly Detection Server (ADS):** ADS, an untrusted entity with a large number of data sets, is mainly responsible for detecting whether the data from OS to PLC is abnormal, and feedback the abnormal behavior to OS.

- **Operator Station (OS):** To prevent the damage caused by the abnormal data in PLC to the actuator of the field control layer, ADS is used to detect the data. Additionally, the data should be encrypted by OS before it is sent, which can prevent the leakage of data information.

3.2. Security requirements
The proposed EPCAD scheme should meet the following two security requirements:

- **Data Confidentiality:** The data in PLC can reflect the operating state of the system, which shall be protected. Even if ADS or an adversary obtains the data, they cannot identify the PLC’s instructions. In addition, since the training data sets and the parameters of ADS are obtained by consuming financial resources and a lot of time[16], these parameters are important private data for ADS. Even if the adversary receives the detection result from ADS, he/she will not learn any information of these parameters.

- **Data Integrity:** To prevent the data from being tampered with during the transmission, the data shall remain intact, that is, ADS shall know whether the data is sent by a valid OS.

4. Preliminaries

4.1. Homomorphic cryptosystem
In this paper, we use the Paillier cryptosystem which is a fully homomorphic encryption scheme proposed by Paillier[17]. Specifically, the Paillier cryptosystem consists of three algorithms: key generation, message encryption and message decryption. The additive homomorphic property of Paillier cryptosystem is as follow:
$$D(E(m_1) \cdot E(m_2)) = D(g^{m_1+m_2} h^{n+i_2}) = D(E(m_1 + m_2))$$

4.2. Support vector machine
SVM is a large margin classifier to process data classification, which is developed by Vapnik [18]. As a two-classification model, SVM is designed to solve the separation hyperplane which can correctly divide the training data sets and has largest geometric interval. However, most of the data are not linearly divisible, so it is necessary to use the kernel function to map the sample from the original space to a higher dimensional feature space, so that the sample can be linearly separated in this feature space. Therefore, the decision function is described as

$$f(x) = w^T x + b = \sum_{i \in S} \alpha_i y_i k(x_i, x) + b$$  \hspace{1cm} (1)

where $\alpha_i$ and $x_i$ are Lagrangian variables and support vectors, respectively. $w$ and $b$ are the classification parameters, $k$ is a kernel function, and $y_i \in \{-1, +1\}$ is the class label of sample $x_i$ for $i = 1$ to $|S|$.

5. The proposed EPCAD scheme
In this section, we propose the concrete EPCAD scheme, which includes three parts: system initialization, data processing and data anomaly detection.

In EPCAD scheme, we assume that the data packet $\overrightarrow{d}$ contains $n$-dimensional features $(\overrightarrow{d_1}, \overrightarrow{d_2}, \ldots, \overrightarrow{d_n})$, where $\overrightarrow{d} \in \mathbb{R}^n$, $i = 1, \ldots, n$. Suppose ADS owns the feature training data sets of points $\overrightarrow{t_i} \in \mathbb{R}^n$, $i = 1, \ldots, n$, where $\overrightarrow{t_i} = (t_{i1}, t_{i2}, \ldots, t_{in})$ and each point $\overrightarrow{t_i}$ belongs to one of the two classes denoted by the label $y_i \in \{-1, +1\}$, $i = 1, \ldots, n$. Additionally, since the test samples and variables in SVM classification are continuous values, the training data shall be normalized to keep the numeric values of training samples on the same scale. We use $\overrightarrow{t_i} = (t_{i1}, t_{i2}, \ldots, t_{in})$ represent normalized training feature samples.

5.1. System initialization
- Given the security parameter $\kappa$, OS generates $(p, q, G_1, G_2, e)$ by running $Gen(\kappa)$, and then calculates the Paillier cryptosystem’s private key $sk$ and the corresponding public key $pk$. OS also selects a signed key $\varepsilon$ and computes $Y = \varepsilon \cdot g$ as the public key of signature verification. Finally, OS publishes the public parameters and keeps the private key and signed key secretly.
- A decision function with linear kernel function $f(d) = \sum_{i \in S} \alpha_i y_i t^T \overrightarrow{d} + b$ is used by ADS, where $\alpha_i$ are Lagrangian variables, $y_i \in \{+1, -1\}$ is the class label of sample $\overrightarrow{t_i}$. Here, $(\alpha_i, y_i, t_i, b)$ are the classification parameters. Additionally, ADS randomly chooses two integers $U$ and $V$, where $U > V$ and $|U \cdot f(d) + V| << \frac{q}{2}$. To make the variables in the decision function be quantized to the nearest integer value, ADS randomly chooses a sufficiently large positive number $\xi$ as the scaling factor. Finally, ADS keeps the parameters $(\alpha_i, y_i, t_i, b, \xi, U, V)$ secretly.

5.2. Data processing
First, OS encrypts the data $\overrightarrow{d}$ using Paillier cryptosystem to generate encrypted data as $[[\overrightarrow{d}]]$. Then, OS uses BLS technology[19] to generate a signature $\sigma$ for $[[\overrightarrow{d}]]$. 
5.3. Data anomaly detection

In this scheme, ADS only considers whether the data is abnormal or not, and gives the corresponding results. In general, the data in ICS is high-dimensional, so we use the linear kernel function $(\xi_t^T, \xi_d)$ in equation (1). The specific detection processes are as follows:

- After receiving $[|d_t|]$, ADS uses public key $Y = \xi \cdot g$ to verify the validity of the signature.
- ADS calculates the normalized value of each element in $[d_t]$ individually as follows:

\[
[f(d)] = [\xi^3 \sum_{i \in S} \alpha_i y_i (t_i^T d + b)]
\]

\[
= [\sum_{i \in S} \xi^3 (\alpha_i y_i) (t_i^T d + \xi b)]
\]

\[
= [\sum_{i \in S} \xi^3 (\alpha_i y_i) (t_i^T d)]
\]

\[
= [\xi^3 b] \cdot \prod_{i \in S} [([\xi t_i^T \cdot \xi d])^{\xi (a_i, y)}]^{\xi (a_i, y)}
\]

where $[\xi d]$ denotes the element of scaled data $[\xi d]$. ADS can calculate the ciphertext of the classification label using integers $U$, $V$ and $f(d)$ as

\[
[\text{flag}] = [f(d)] = [f(d)]^{\xi} = [U \cdot f(d) + V]
\]

- Upon receiving $[\text{flag}] = [f(d)]$, OS can decrypt the $[\text{flag}]$ with private key $sk$ and obtain the detection result.

6. Security analysis and performance evaluation

6.1. Security analysis

In our scheme, since the data and ADS’s parameters are encrypted by Paillier homomorphic cryptosystem, the adversary cannot obtain them without the private key. Although OS can decrypt the classification label, he/she cannot identify ADS’s parameters. The reason is that the decision function $f(d)$ in equation (4) is blinded by two random numbers $U$ and $V$. In addition, the encrypted data is signed by BLS technology, which prevents the data from being maliciously tampered with by adversary.

6.2. Computational cost

We perform the evaluations on Intel Core i7-7500U @2.70 GHz with 8 GB RAM. A security parameter with 512-bit is selected. The computational cost of the proposed EPCAD scheme is shown in Table 1.
Table 1. Computational cost of the proposed EPCAD scheme

| Phase | Data processing phase | Data anomaly detection phase | Total |
|-------|-----------------------|----------------------------|-------|
| OS    | $2nT_e + T_m$         | -                          | $(4n+|S|+1)T_e + T_m +$ |
| ADS   | -                     | $(2n+|S|+1)T_e + 2T_b$     | $2T_b$ |

- No operation

Figure 3 shows that the computational cost of OS is so low that even if there are 10 data types, its execution time is no more than 120 ms. As shown in figure 4, when the number of support vector is the same, the higher the dimension of the data, the greater the computational cost of ADS.

6.3. Communication overhead

In this subsection, we mainly consider the communication overhead between OS and ADS. Table 2 shows that the proposed EPCAD scheme has low communication overhead.

Table 2. Communication overhead of the proposed EPCAD scheme

|                  | OS to ADS | ADS to OS | Total     |
|------------------|-----------|-----------|-----------|
| 1024×$n+210$ bits| 1024 bits | 1024×$n+1234$ bits |

7. Conclusion

In this paper, we have proposed an efficient and privacy-preserving data anomaly detection scheme for ICS. With the Paillier homomorphic cryptosystem, signature authentication technology and SVM algorithm, it has the capability of efficiently detecting anomalies in data without compromising data information and preventing the leakage of ADS classification parameters. Additionally, simulation results demonstrate that the proposed EPCAD scheme has lower computational cost so that OS can quickly obtain abnormal data detection results. Therefore, the proposed EPCAD scheme is suitable for the real-time industrial control detection environment.

Acknowledgments

This research is supported by the Scientific Research Program for Young Talents of China National Nuclear Corporation under grant A190686, the Ph.D research startup foundation of Hubei University of Technology BSQD2019023.

References

[1] Kobo, H. I., Abu-Mahfouz, A. M., Hancke, G. P. (2019) Fragmentation-based distributed control system for software defined wireless sensor networks. IEEE Transactions on Industrial Informatics, 15: 901-910.
[2] Cherdantseva, Y., Burnap, P., Blyth A., Stoddart, K. (2016) A review of cyber security risk assessment methods for SCADA systems. Computers & Security, 56: 1-27.

[3] Hu, Y., Yang, A., Li, H., Sun, Y., Sun, L. (2018) A survey of intrusion detection on industrial control systems. International Journal of Distributed Sensor Networks, 14: 1-14.

[4] Qin, J., He, Z. (2005) A SVM face recognition method based on gabor-featured key points. In: International Conference on Machine Learning and Cybernetics. Guangzhou. pp. 5144-5149.

[5] Kaur, P., Pannu, H. S., Malhi, A. K. (2019) Plant disease recognition using fractional-order zernike moments and SVM classifier. Neural Computing and Applications, 31: 8749-8768.

[6] Byvatov, E., Schneider, G. (2003) Support vector machine applications in bioinformatics. Appl Bioinformatics, 2: 67-77.

[7] Tong, S., Koller, D. (2002) Support vector machine active learning with applications to text classification. Journal of Machine Learning Research, 2: 999-1006.

[8] Maglaras, L. A., Jiang, J. (2014) Intrusion detection in SCADA systems using machine learning techniques. In: Science and information conference. London. pp. 626-631.

[9] Usha, M., Kavitha, P. (2016) Anomaly based intrusion detection for 802.11 networks with optimal features using SVM classifier. Wireless Networks, 23: 2431-2446.

[10] Morris, T., Vaughn, R., Dandass, T. (2012) A retrofit network intrusion detection system for MODBUS RTU and ASCII industrial control systems. In 45th Hawaii international conference on system science. Grand Wailea. pp. 2338-2345.

[11] Hong, J., Liu, C., Govindarasu, M. (2014) Detection of cyber intrusions using network-based multicast messages for substation automation. In IEEE PES conference on innovative smart grid technologies conference. Washington. pp. 1-5.

[12] Stavroulakis, P., Stamp, M. (2010) Handbook of information and communication security. Berlin: Springer-Verlag.

[13] Ashfaq, R. A. R., Wang, X., Huang, J. (2017) Fuzziness based semi-supervised learning approach for intrusion detection system. Information Sciences. 378: 484-497.

[14] Linda, O., Manic, M., Vollmer, T. (2011) Fuzzy logic based anomaly detection for embedded network security cyber sensor. In IEEE symposium on computational intelligence in cyber security. Paris. pp. 202-209.

[15] Linda, O., Manic, M., Vollmer, Y. (2012) Improving cyber-security of smart grid systems via anomaly detection and linguistic domain knowledge. In 5th international symposium on resilient control systems. Salt Lake City, pp. 48-54.

[16] Li, X., Zhu, Y., Wang, J., Liu, Z., Liu, Y., Zhang, M. (2018) On the soundness and security of privacy-preserving SVM for outsourcing data classification. IEEE Transactions on Dependable and Secure Computing, 15: 906-912.

[17] Paillier, P. (1999) Public-key cryptosystems based on composite degree residuosity classes. In: International Conference on the Theory and Application of Cryptographic Techniques. Prague. pp. 223-238.

[18] Vapnik, V. N. (1999) An overview of statistical learning theory. IEEE Transactions Neural Network, 10: 988-999.

[19] Boneh, D., Lynn, B., Shacham, H. (2004) Short signatures from the weil pairing. Journal of Cryptology, 17: 297-31.