A Hybrid Intrusion Detection System Based on Machine Learning under Differential Privacy Protection

Jibo Shi[1],Yun Lin[1],Zherui Zhang[1,*],Shui Yu[2]
[1,*]*College of Information and Communication Engineering, Harbin Engineering University, Harbin, China*
[2]*School of Software Engineering, University of Technology Sydney, NSW 2007, Australia*
E-mail:{jiboshi,linyun,zhangzherui}@hrbeu.edu.cn,Shui.yu@uts.edu.au

2021 IEEE 94th Vehicular Technology Conference (VTC2021-Fall) | 978-1-6654-1368-8/21/$31.00 ©2021 IEEE | DOI: 10.1109/VTC2021-FALL52928.2021.9625540

***Abstract*—With the development of network, network security has become a topic of increasing concern. Recent years, machine learning technology has become an effective means of network intrusion detection. However, machine learning technology requires a large amount of data for training, and training data often contains privacy information, which brings a great risk of privacy leakage. At present, there are few researches on data privacy protection in the field of intrusion detection. Regarding the issue of privacy and security, we combine differential privacy and machine learning algorithms, including One-class Support Vector Machine (OCSVM) and Local Outlier Factor(LOF), to propose an hybrid intrusion detection system (IDS) with privacy protection. We add Laplacian noise to the original network intrusion detection data set to get differential privacy data sets with different privacy budgets, and proposed a hybrid IDS model based on machine learning to verify their utility. Experiments show that while protecting data privacy, the hybrid IDS can achieve detection accuracy comparable to traditional machine learning algorithms.**

***Index Terms*—Privacy security, IDS, machine learning, differential privacy**

I. Introduction

With the commercialization of 5G and the rapid development of the Internet, the hidden dangers of network security have become serious. Due to the increasingly close integration of the Internet and life, network security is particularly important. In the increasingly serious field of network information security, IDS plays an important role in detection and defense. IDS's core technology is to accurately identify various attacks in the network. Compared with traditional static detection, such as firewalls and vulnerability scanners, IDS can identify intrusions that have occurred or are occurring. IDS has become a key object of research in the field of network information security.

Nowadays, with the progress of big data and hardware technology, applying machine learning to network security has very important research value. Many researchers have applied deep learning to the field of intrusion detection. However, machine learning requires a large amount of data for training. The training data may contain quite a lot of private data, which brings a great risk of privacy leakage. This makes data privacy security become the focus of people's concern. For example, the European Union's "General Data Protection Regulation" (GDPR) was implemented in May 2018 [1]. But there is little work to consider the data privacy of machine learning training in the field of network intrusion detection. Based on this problem, we use the popular differential privacy method to protect the network data privacy.

At present, many researchers have tried to combine the differential privacy mechanism with machine learning, using its rigorous mathematical proof and flexible combination theorem to protect the privacy of data. Therefore, as a rigorous and efficient privacy protection method, differential privacy can be applied to the field of IDS, combined with machine learning technology, to efficiently process massive amounts of data while protecting the privacy of network users.

Our contribution is summarized as follows:

- In order to solve the problem of data privacy security in intrusion detection, we apply differential privacy theory to intrusion detection, and use laplace mechanism to construct differential privacy data sets with different privacy budgets. Different IDS models are used to verify the utilities of these differential privacy data sets.
- We propose a hybrid intrusion detection model based on One-class Support Vector Machine (OCSVM) and Local Outlier Factor(LOF). The hybrid IDS can detect intrusion traffic effectively even if it only uses normal traffic for training.

The rest of this paper is organized as follows. In Section II, we describe the work done by predecessors in the fields of intrusion detection and differential privacy. After we describe the proposed hybrid IDS model and its implementation process in Section III, the simulation results are presented in Section IV. Finally, this paper is summarized in Section V.

II. Related Works

Since 2014, many researchers have applied deep learning to the field of intrusion detection. Gao et al. began to use deep belief networks for intrusion detection [2], compared with the support vector machine (SVM) model, the deep belief network model has better performance on KDD99 dataset. In 2017, Vinayakumar et al. applied Convolutional Neural Network (CNN) to intrusion detection [3]. They modeled the network traffic as a time series and proved the effectiveness of its network structure in intrusion detection on the KDD99 data set. In 2020, Yan et al. combined the autoencoder with

RNN for intrusion detection and achieved 92% accuracy on the UNSW-NB15 dataset [4]. But they did not consider the data privacy problem in machine learning training. Based on this problem, we use the popular differential privacy method to protect the network data privacy.

The differential privacy technology proposed by Dwork et al. [5] has been widely used in data publishing [6], data analysis [7] and other fields. Bindschaedler et al. proposed a standard of plausible deniability to ensure the privacy of sensitive data [8]. Huang et al. proposed an ADMM distributed learning algorithm based on differential privacy(DP-ADMM) [9]. Wang et al. proposed a new local differential privacy mechanism to Collect numerical attributes and extend them to multi-dimensional data that can contain both number and category attributes [10]. Their experiments proved that the algorithm can support many important machine learning tasks and is more effective than current solutions. However, in the field of intrusion detection, there is little research on using differential privacy for data privacy protection, so this paper uses Laplace mechanism to build differential privacy data set, and verifies their utilities on different intrusion detection models.

III. System Model

Considering the privacy security problems in the field of network intrusion detection, we propose a hybrid intrusion detection model based on OCSVM and LOF under differential privacy protection.

A. One-class Support Vector Machine

The OCSVM algorithm is developed on the basis of the traditional SVM algorithm.

Assuming that the training sample data set $X = \{x_i, i = 1, 2, 3, ..., l\}, x_i \in R^N$, there is a high-dimensional feature space H, so that the training sample data is mapped into H through a non-linear mapping ϕ, $s.t. \phi(x_i) \in H$. Establish a classification hyperplane $\omega \cdot \phi(x) - \rho = 0$ with ω as the normal vector and ρ as the intercept in the high-dimensional feature space to separate the sample points from the origin.

The secondary planning problems solved by OCSVM are as follows:

$$min_{\omega,\xi,\rho}\ \frac{1}{2}\omega^T\omega - \rho + \frac{1}{vl}\sum_{i=1} r\xi_i$$
$$s.t.\ \begin{cases} \omega^T\phi(x_i) \geq \rho - \xi_i \\ \xi_i \geq 0, i = 1, ..., l \end{cases} \quad (1)$$

where x_i is the training sample, $i = 1, 2, ..., l$, l is the number of training samples, $\phi(\cdot)$ is the mapping from the original space to the feature space, ω is the normal vector of the classification hyperplane, and ρ is the compensation of the classification hyperplane , $v \in [0, 1]$ is a trade-off parameter. ξ_i is the slack variable, which is used to punish deviations from the hyperplane. The detection process of IDS based on OCSVM is shown as Algorithm 1.

Firstly, we introduce Lagrange vector to solve the quadratic programming problem, calculate the partial derivatives of ω, ρ, ξ_i respectively. Then, Gauss kernel function is introduced to transform the OCSVM optimization problem into dual form, as shown in formula(4). Choose any α^* that satisfies $0 \leq \alpha^* \leq \frac{1}{vl}$, calculate the offset $\rho = \sum_i^l \alpha_i^* K(x_i, x_j)$, and the vector x_i corresponding to α_i is the support vector. Finally, the decision function of OCSVM classification can be obtained. After the training, we input the test data into the trained IDS, and use the decision function to detect the intrusion sample.

Algorithm 1 Detection Process of IDS Based on OCSVM

1: ***Data Preprocess***.
2: ***Train:***
3: Input the train dataset: $X = \{x_i, i = 1, 2, 3, ..., l\}, x_i \in R^N$.
4: Introduce the Lagrangian vector $\alpha = [\alpha_i, ..., \alpha_l]^T$.
5: Solve the above quadratic programming problem:

$$L(\omega, \xi, \rho, \alpha, \beta) = \frac{1}{2}||\omega||^2 - \sum_i^l \alpha_i(\omega \cdot x_i - \rho + \xi_i) + \frac{1}{vl}\sum_i^l \xi_i - \rho - \sum_i^l \beta_i\xi_i \quad (2)$$

6: Introduce the Gaussian kernel function:

$$K(x_i, x_j) =< \Phi(x_i), \Phi(x_j) >= exp(-g||x_i - x_j||^2 \quad (3)$$

7: Bring in the OCSVM optimization problem and convert it into a dual form:

$$\begin{cases} min_\alpha \frac{1}{2}\sum_i^l \sum_j^l \alpha_i\alpha_j K(x_i, x_j) \\ s.t.\ 0 \leq \alpha_i \leq \frac{1}{vl}, \sum_i^l \alpha_i = 1 \end{cases} \quad (4)$$

8: Obtain the decision function:

$$y = sgn(f(x)) = sgn(\sum_{i=1}^{l} \alpha_i K(x_i, x) - \rho) \quad (5)$$

9: ***Test:***
10: Input the test data into trained IDS to get the corresponding output y.
11: **if** $y > 0$ **then**
12: Judged as normal sample.
13: **else**
14: Judged as abnormal sample.
15: **end if**

B. Local Outlier Factor

The LOF algorithm is one of the typical density-based local outlier detection algorithms. The main principle is: each data point is given a local outlier factor lof that characterizes the outlier degree of the object. By calculating the outlier degree of each data point in the data set, the first n points with the largest value are found and judged as Outliers. The detection process of IDS based on LOF is shown as Algorithm 2.

Most of the intrusion detection algorithms before LOF were based on statistical methods. However, statistics-based anomaly detection algorithms usually need to assume that the data obey a specific probability distribution. In comparison, the

Algorithm 2 Detection Process of IDS Based on LOF

Data Preprocess.

Train:

Input the train dataset: $P = \{p_i, i = 1, 2, 3, ..., l\}, p_i \in R^N$.

Calculate the $k - distance$ of object p,which is defined as the distance between p and an object o, the conditions that the object o needs to meet are: (a) There are at least k objects $o' \in D\backslash\{p\}$, satisfying $s.t.\ d(p, o') \leq d(p, o)$. (b) There are at most $k-1$ objects $o' \in D\backslash\{p\}, s.t.\ d(p, o') < d(p, o)$.,where $d(p, o)$ represents the distance between data element p and data element o.

Seek the $k-th$ distance field of object p., which is defined as:

$$N_{k-distance}(p) = \{q | d(p, q) \leq k - distance(p)\} \quad (6)$$

Calculate the reachable distance of data p relative to data:

$$reach - dist(p, o) = max(k - distance(o), d(p, p)) \quad (7)$$

For each data object p, calculate the local reachable density:

$$lrd_k(p) = 1/[\frac{\sum reach - dist_k(p, o)}{|N_{k-distance}(p)|}] \quad (8)$$

Solving the local anomaly factor of object p:

$$LOF_k(p) = \frac{\sum_{o \in N_k(p)} \frac{lrd_k(o)}{lrd_k(p)}}{|N_k(p)|} \quad (9)$$

Test:

Calculate the local anomaly factors of the sample p: lof_p.

Set the threshold value C of local abnormal factor.

if $lof_p < C$ **then**

    Judged as normal sample.

else

    Judged as abnormal sample.

end if

density-based LOF algorithm is simpler and more intuitive. It does not require too much data distribution, and it can also quantify the outlierness of each data sample.

C. Differential Privacy

Differential privacy's principle is to perturb the data by adding random noise that obeys a specific distribution to the original data set. After adding noise to the data set, these data can still maintain statistical significance, but achieve the goal of privacy protection for a single data.

Definition 1: Adjacent data set:If two data sets D and $D'$with the same structure and attributes are the same except for one piece of data, the rest of the data are the same, then we can call the data sets D and D'as adjacent data sets.

Definition 2: Differential privacy: For any two adjacent data sets D and D', given a random algorithm A, if any output result of A satisfies:

$$Pr[A(D) = S] \leq exp(\epsilon) \cdot Pr[A(D') = S] \quad (10)$$

where ϵ is the privacy budget parameter of the differential privacy algorithm, and the algorithm A satisfies $\epsilon-$ differential privacy.

Definition 3: Global sensitivity: Assume a function $f : D \rightarrow R^d$, data set D be the input of f, and output be a vector of dimension d.

The global sensitivity of function f is defined as follows:

$$\triangle f = max_{D,D'} ||f(D) - f(D')||_1 \quad (11)$$

where D and D' are any adjacent data sets.

The method of Laplace mechanism to achieve differential privacy protection is to add random noise that obeys Laplace distribution to the output result $f(D)$. If the probability density of a random variable x is $Pr(x, \lambda, a) = \frac{1}{2\lambda} e^{-\frac{|x-a|}{\lambda}}$, then x satisfies the Laplace distribution, where λ is the scale parameter and a is the mean value.

Definition 4: Laplace mechanism: Given a query function f, the input is data set D, and algorithm A satisfies:

$$A(D) = f(D) + \xi \quad (12)$$

then A satisfies a $\epsilon-$differential privacy protection. Where ξ is random noise that obeys the Laplace distribution, $\xi \sim Lap(\lambda), \lambda = \frac{\triangle f}{\epsilon}$, $\triangle f$ is the global sensitivity of the data set. It can be seen that the amount of noise is inversely proportional to ϵ.

The datasets used in this paper are multi feature datasets, and the attribute and numerical difference between features is large, so it is difficult to add Laplacian noise directly. Therefore, we normalize and standardize the datasets, the characteristic value of the datasets falls within the range of $[0, 1]$, so that the global sensitivity of the datasets we use is 1 and we can add the differential privacy noise of different privacy budgets to the dataset as a whole. Specifically, for the CICIDS2018 dataset, we add Laplacian noise with privacy budget of 1, 10, 100 and 200 respectively. For UNSW-NB15 dataset, we add Laplacian noise with privacy budget of 1, 10 and 100 respectively.

D. Hybrid IDS

The hybrid IDS combines the advantages of LOF and OCSVM algorithms. In the actual experiment, we found that the OCSVM-based IDS has a high accuracy in detecting normal flow. Therefore, in the detection stage, if the input flow data is detected as normal flow, it will be directly output, and it does not need to be input to the LOF-based IDS for detection, which shortens the detection time. Since the LOF-based IDS has high accuracy when detecting abnormal traffic, if the input flow data is detected as abnormal traffic, LOF-based IDS will perform a second detection, thereby increase the robustness of the model, detect abnormal traffic more efficiently, and reduce the false alarm rate. The structure of hybrid IDS is shown in Fig.1.

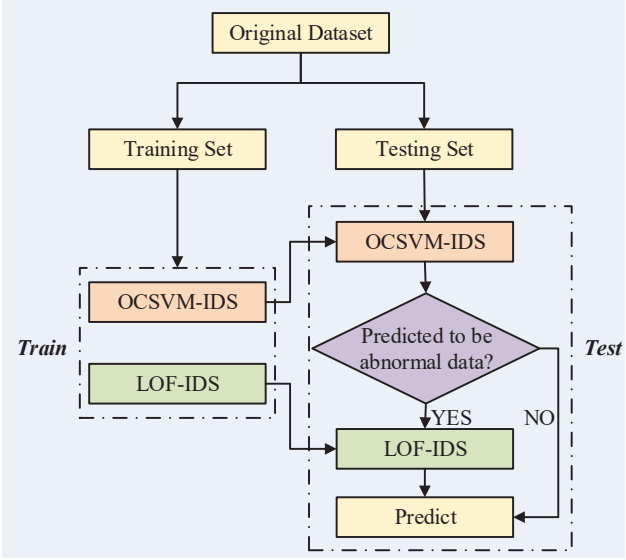

Fig. 1. The structure of hybrid IDS

The operation process of our hybrid IDS model is shown in Fig. 2. Firstly, we preprocess the original network intrusion detection data set, including data cleaning, data normalization, data standardization and other operations. The purpose of data cleaning is to delete the data with incomplete information, redundant information and duplicate information, while data normalization and data standardization are helpful to solve the global sensitivity of differential privacy. In addition, in order to further enhance the privacy protection level of the differential privacy dataset, we delete some privacy sensitive features from the original dataset. Then, we perform differential privacy processing on the training data set, and add Laplacian noise with different privacy budget to the original data set by using the Laplacian mechanism described above. After the differential privacy step is completed, we use the obtained differential privacy data set to train IDS model based on OCSVM and LOF. Finally, we feed the test dataset which only has data preprocessing but not differential privacy processing into the trained hybrid IDS to test the network intrusion detection performance.

Considering the huge amount of network data, and the magnitude of network normal traffic data is far greater than that of network intrusion traffic data, it is very difficult to obtain intrusion data from a large number of normal data in the actual scene. To solve this problem, we only use normal traffic data for unsupervised training of hybrid IDS to enhance the practicability of hybrid IDS.

IV. SIMULATION RESULTS

A. Data Preprocessing

In order to enhance the persuasiveness of our proposed IDS, we use two relatively novel and comprehensive open source data sets for experimental verification, which are the UNSW-NB15 data set and the CICIDS2018 data set.

In order to further protect data privacy, we have deleted the 'label', 'attack_cat','proto', 'service', 'state' and other features in the UNSW-NB15 data set, and 'typeName', 'src_ip', 'dst_ip', 'whitelist', 'persist', 'guid' and other features in the CICIDS2018 data set. In addition to deleting privacy-sensitive features, we also performed data preprocessing operations such as data cleaning, data standardization, and data normalization.

We add Laplacian noise to the two data sets to obtain differential privacy data sets. The training set of the UNSW-NB15 data set in this article is 56,000 data samples with 39-dimensional features. The normal flow test set consists of 37,000 data samples and 39-dimensional features. The abnormal flow test set consists of 45,332 data samples and 39-dimensional features. Similarly, the training set of the CICIDS2018 data set in this article is 40,000 data samples with 44-dimensional features. The normal flow test set consists of 20,000 data samples and 44-dimensional features. The abnormal flow test set consists of 120,000 data samples and 44-dimensional features.

B. Simulation Results

We first use OCSVM, LOF, and hybrid IDS to conduct experiments on the CICIDS2018 data set without differential privacy processing.

OCSVM's detection accuracy of normal flow samples on CICIDS2018 was 82.285%, and the detection accuracy of abnormal flow samples was 99.932%. The detection accuracy of LOF on CICIDS2018 for normal flow samples is 77.055%, and the detection accuracy for abnormal flow samples is 100%. The detection accuracy of double-layer IDS on CICIDS2018 for normal flow samples is 87.505%, and the detection accuracy for abnormal flow samples is 100%.

Next, we use OCSVM, LOF and hybrid IDS to conduct experiments on the CICIDS2018 data set after differential privacy processing. According to the different privacy budgets, we conducted experiments on three CICIDS2018 data sets processed with differential privacy. The global sensitivity $\triangle f$ of the 4 data sets is approximately 1, and the privacy budget ϵ is 1, 10, 100 and 200, respectively.

- When the privacy budget $\epsilon = 1$. OCSVM's detection accuracy of normal flow samples on DP-CICIDS2018($\epsilon = 1$) is 0, and the detection accuracy of abnormal flow samples is 100%. The detection accuracy of LOF on DP-CICIDS2018($\epsilon = 1$) for normal flow samples is 0, and the detection accuracy for abnormal flow samples is 100%. The detection accuracy of double-layer IDS on DP-CICIDS2018($\epsilon = 1$) for normal flow samples is 0, and the detection accuracy for abnormal flow samples is 100%.
- When the privacy budget $\epsilon = 10$. OCSVM's detection accuracy of normal flow samples on DP-CICIDS2018($\epsilon = 10$) is 52.7%, and the detection accuracy of abnormal flow samples is 99.928%. The detection accuracy of LOF on DP-CICIDS2018($\epsilon = 10$) for normal flow samples is 0, and the detection accuracy for abnormal flow samples is 100%. The detection accuracy of double-layer IDS

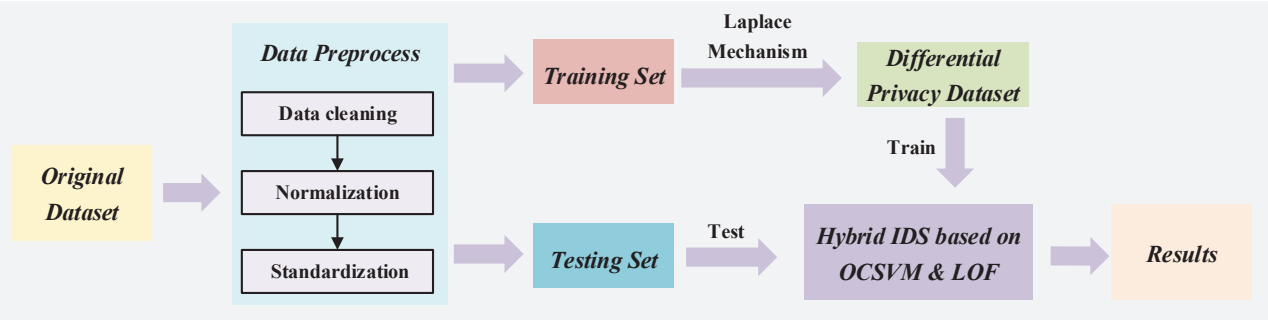

Fig. 2. The operation process of our system model

on DP-CICIDS2018($\epsilon = 10$) for normal flow samples is 52.7%, and the detection accuracy for abnormal flow samples is 100%.

- When the privacy budget $\epsilon = 100$. OCSVM's detection accuracy of normal flow samples on DP-CICIDS2018($\epsilon = 100$) is 80.305%, and the detection accuracy of abnormal flow samples is 99.932%. The detection accuracy of LOF on DP-CICIDS2018($\epsilon = 100$) for normal flow samples is 0.39%, and the detection accuracy for abnormal flow samples is 100%. The detection accuracy of double-layer IDS on DP-CICIDS2018($\epsilon = 100$) for normal flow samples is 80.34%, and the detection accuracy for abnormal flow samples is 100%.
- When the privacy budget $\epsilon = 200$. OCSVM's detection accuracy of normal flow samples on DP-CICIDS2018($\epsilon = 200$) is 82.65%, and the detection accuracy of abnormal flow samples is 99.930%. The detection accuracy of LOF on DP-CICIDS2018($\epsilon = 200$) for normal flow samples is 0.62%, and the detection accuracy for abnormal flow samples is 100%. The detection accuracy of double-layer IDS on DP-CICIDS2018($\epsilon = 200$) for normal flow samples is 82.77%, and the detection accuracy for abnormal flow samples is 100%.

The specific experimental results are shown in Table I and Table II. It can be seen from Table I and Table II that on the CICIDS2018 data set, the OCSVM algorithm performs better than the LOF algorithm when detecting normal traffic, and it performs slightly worse than the LOF algorithm when detecting intrusion traffic. The hybrid IDS we proposed has the best performance in detecting normal traffic and intrusive traffic. On the differential privacy data set DP-CICIDS2018, when the privacy budget is ϵ 1 and 10, the performance of the three IDS is very poor. When the privacy budget ϵ is 100 and 200, the performance of the three IDSs is close to the baseline they reached on the CICIDS2018 data set.

We also did a similar experiment on the UNSW-NB15 dataset without differential privacy processing. OCSVM's detection accuracy of normal flow samples on UNSW-NB15 was 86.9655%, and the detection accuracy of abnormal flow samples was 26.617%. The detection accuracy of LOF on UNSW-NB15 for normal flow samples is 82.295%, and the detection accuracy for abnormal flow samples is 72.469%. The

TABLE I
DETECTION ACCURACY OF ABNORMAL FLOW ON CICIDS2018 AND DP-CICIDS2018

Dataset \ Algorithm	OCSVM	LOF	Hybrid IDS
CICIDS2018	99.932%	100.000%	100.000%
DP-CICIDS2018(ϵ=1)	100.000%	100.000%	100.000%
DP-CICIDS2018(ϵ=10)	99.928%	100.000%	100.000%
DP-CICIDS2018(ϵ=100)	99.932%	100.000%	100.000%
DP-CICIDS2018(ϵ=200)	99.930%	100.000%	100.000%

TABLE II
DETECTION ACCURACY OF NORMAL FLOW ON CICIDS2018 AND DP-CICIDS2018

Dataset \ Algorithm	OCSVM	LOF	Hybrid IDS
CICIDS2018	82.285%	77.055%	87.505%
DP-CICIDS2018(ϵ=1)	0.000%	0.000%	0.000%
DP-CICIDS2018(ϵ=10)	52.700%	0.000%	52.700%
DP-CICIDS2018(ϵ=100)	80.305%	0.390%	80.340%
DP-CICIDS2018(ϵ=200)	82.650%	0.620%	82.770%

detection accuracy of double-layer IDS on UNSW-NB15 for normal flow samples is 95.654%, and the detection accuracy for abnormal flow samples is 76.177%.

Finally, we use three different privacy budgets to perform differential privacy processing on the UNSW-NB15 dataset. Their global sensitivity is approximately 1, and their privacy budgets are 1, 10, and 100 respectively, and conduct experiments on these three data sets.

- When the privacy budget $\epsilon = 1$. OCSVM's detection accuracy of normal flow samples on DP-UNSW-NB15($\epsilon = 1$) is 0, and the detection accuracy of abnormal flow samples is 100%. The detection accuracy of LOF on DP-UNSW-NB15($\epsilon = 1$) for normal flow samples is 0, and the detection accuracy for abnormal flow samples is 100%. The detection accuracy of double-layer IDS on DP-UNSW-NB15($\epsilon = 1$) for normal flow samples is 0, and the detection accuracy for abnormal flow samples is 100%.
- When the privacy budget $\epsilon = 10$. OCSVM's detection accuracy of normal flow samples on DP-UNSW-NB15($\epsilon = 10$) is 15.359%, and the detection accuracy of abnormal flow samples is 89.034%. The detection accuracy of LOF

TABLE III
DETECTION ACCURACY OF ABNORMAL FLOW ON UNSW-NB15 AND DP-UNSW-NB15

Dataset \ Algorithm	OCSVM	LOF	Hybrid IDS
UNSW-NB15	26.617%	72.469%	76.177%
DP-UNSW-NB15(ϵ=1)	100.000%	100.000%	100.000%
DP-UNSW-NB15(ϵ=10)	89.043%	99.656%	100.000%
DP-UNSW-NB15(ϵ=100)	56.998%	75.375%	79.173%

TABLE IV
DETECTION ACCURACY OF NORMAL FLOW ON UNSW-NB15 AND DP-UNSW-NB15

Dataset \ Algorithm	OCSVM	LOF	Hybrid IDS
UNSW-NB15	86.965%	82.295%	95.654%
DP-UNSW-NB15(ϵ=1)	0.000%	0.000%	0.000%
DP-UNSW-NB15(ϵ=10)	15.359%	0.408%	13.705%
DP-UNSW-NB15(ϵ=100)	88.446%	71.832%	95.873%

on DP-UNSW-NB15($\epsilon = 10$) for normal flow samples is 0.408%, and the detection accuracy for abnormal flow samples is 99.656%. The detection accuracy of double-layer IDS on DP-UNSW-NB15($\epsilon = 10$) for normal flow samples is 13.705%, and the detection accuracy for abnormal flow samples is 100%.

- When the privacy budget $\epsilon = 100$. OCSVM's detection accuracy of normal flow samples on DP-UNSW-NB15($\epsilon = 100$) is 80.305%, and the detection accuracy of abnormal flow samples is 88.446%. The detection accuracy of LOF on DP-UNSW-NB15($\epsilon = 100$) for normal flow samples is 71.832%, and the detection accuracy for abnormal flow samples is 75.375%. The detection accuracy of double-layer IDS on DP-UNSW-NB15($\epsilon = 100$) for normal flow samples is 95.873%, and the detection accuracy for abnormal flow samples is 79.173%.

The specific experimental results are shown in Table III and Table IV. It can be seen from Table III and Table IV that the OCSVM algorithm on the UNSW-NB15 data set is not as good as the LOF algorithm in detecting normal traffic and intrusive traffic, while our proposed hybrid IDS performs best in detecting normal traffic and intrusive traffic. On the DP-UNSW-NB15 data set, as the privacy budget ϵ increases, the performance of the three IDSs also improves. When the privacy budget ϵ is 100,the performance of our proposed hybrid IDS exceeds its performance on the UNSW-NB15 dataset.

V. CONCLUSION

In this article, we propose a hybrid IDS based on differential privacy and machine learning algorithms. In order to further protect the privacy, we deleted the privacy-sensitive features in the data set, and conducted experimental verification on the UNSW-NB15 data set, CICIDS2018 data set and the corresponding differential privacy data set. The experimental prove that the hybrid IDS proposed in this paper can effectively detect intrusive traffic while greatly protecting privacy. As privacy and security issues become increasingly prominent, the application of differential privacy and IDS is of vital importance for ensuring network security.

ACKNOWLEDGMENT

This paper is funded by the International Exchange Program of Harbin Engineering University for Innovation-oriented Talents Cultivation.

REFERENCES

[1] Voigt, Paul, and Axel Von dem Bussche. "The eu general data protection regulation (gdpr),"A Practical Guide, 1st Ed., Cham: Springer International Publishing ,2017.

[2] N. Gao, L. Gao, Q. Gao and H. Wang, "An Intrusion Detection Model Based on Deep Belief Networks," 2014 Second International Conference on Advanced Cloud and Big Data, 2014, pp. 247-252, doi: 10.1109/CBD.2014.41.

[3] R. Vinayakumar, K. P. Soman and P. Poornachandran, "Applying convolutional neural network for network intrusion detection," 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Udupi, 2017, pp. 1222-1228, doi: 10.1109/ICACCI.2017.8126009.

[4] Y. Yan, L. Qi, J. Wang, Y. Lin and L. Chen, "A Network Intrusion Detection Method Based on Stacked Autoencoder and LSTM," ICC 2020 - 2020 IEEE International Conference on Communications (ICC), 2020, pp. 1-6, doi: 10.1109/ICC40277.2020.9149384.

[5] Dwork, Cynthia, et al. "Calibrating noise to sensitivity in private data analysis," Theory of cryptography conference. Springer, Berlin, Heidelberg, 2006.

[6] Q. Wang, Y. Zhang, X. Lu, Z. Wang, Z. Qin and K. Ren, "Real-Time and Spatio-Temporal Crowd-Sourced Social Network Data Publishing with Differential Privacy," in IEEE Transactions on Dependable and Secure Computing, vol. 15, no. 4, pp. 591-606, 1 July-Aug. 2018, doi: 10.1109/TDSC.2016.2599873.

[7] T. Zhang and Q. Zhu,"Dynamic Differential Privacy for ADMM-Based Distributed Classification Learning" in IEEE Transactions on Information Forensics and Security, vol. 12, no. 1, pp. 172-187, Jan. 2017, doi: 10.1109/TIFS.2016.2607691.

[8] Bindschaedler, Vincent, Reza Shokri, and Carl A. Gunter, "Plausible deniability for privacy-preserving data synthesis,", arXiv preprint arXiv:1708.07975

[9] Z. Huang, R. Hu, Y. Guo, E. Chan-Tin and Y. Gong, "DP-ADMM: ADMM-Based Distributed Learning With Differential Privacy," in IEEE Transactions on Information Forensics and Security, vol. 15, pp. 1002-1012, 2020, doi: 10.1109/TIFS.2019.2931068.

[10] N. Wang et al., "Collecting and Analyzing Multidimensional Data with Local Differential Privacy," 2019 IEEE 35th International Conference on Data Engineering (ICDE), 2019, pp. 638-649, doi: 10.1109/ICDE.2019.00063.