IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received July 13, 2019, accepted August 5, 2019, date of publication August 16, 2019, date of current version August 30, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2935759

Cooperative Fraud Detection Model With Privacy-Preserving in Real CDR Datasets

NA RUAN[1], ZHIKUN WEI[1], AND JIENAN LIU[2]
[1]MoE Key Lab of Artificial Intelligence, Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai 200240, China
[2]Department of Computer Science, University of Georgia, Athens, GA 30602, USA

Corresponding author: Jienan Liu (jienan@cs.uga.edu)

This work was supported by the Chinese National Research Fund (NSFC) under Grant 61702330.

ABSTRACT The researchers have shown broad concern about detection and recognition of fraudsters since telecommunication operators and the individual user are both suffering significant losses from fraud activities. Researchers have proposed various solutions to counter fraudulent activity. However, those methods may lose effectiveness in fraud detection because fraudsters always tend to cover their tracks by roaming among different telecommunication operators. What is more, due to the lack of real data, researchers have to do simulations in a virtual scenario, which makes their models and results less persuasive. In our previous paper, we proposed a novel strategy with high accuracy and security through cooperation among mobile telecommunication operators. In this manuscript, we will validate it in a real-world scenario using real Call Detail Records(CDR) data. We apply the Latent Dirichlet Allocation (LDA) model to profile users. Then we use a method based on Maximum Mean Discrepancy (MMD) to compare the distribution of samples to match roaming fraudsters. Cooperation between telecommunication operators may boost the accuracy of detection while the potential risk of privacy leakage exists. A strategy based on Differential Privacy(DP) is used to address this problem. We demonstrate that it can detect the fraudsters without revealing private data. Our model was validated using simulated dataset and showed its effectiveness. In this manuscript, experiments are performed on real CDRs data, and the result shows that our method has impressive performance in the real-world scenario as well.

INDEX TERMS Data privacy, data mining, security, real-world scenario, spam detection.

I. INTRODUCTION

Telecommunication operators and the individual user are suffering significant losses from fraud activities with the increasing scale of the mobile phone user. In order to detect the fraud activity, different strategies are proposed, which apply methods such as machine learning and statistical model. Bolton *et al.* [1] demonstrated how a statistical model could be used to detect fraudsters. Weatherford [2] adopted neural networks to make use of historical records to generate the patterns of legitimate users for the long-term. Works [3], [4] showed that evidence of fraud and fraudulent activities hides in a vast amount of data, and it is possible to apply statistical techniques and artificial intelligence to uncover those hidden fraudsters. Recently deep learning was used to process data from physical world [5], [6], which brought new ideas to the detecting fraudsters from CDR data. Diffusion networks and secure transmission are discussed in a broader view of the scurrility issue [7]–[9]. The industry developed software to detect fraud. One early example was that the FICO Falcon fraud assessment system in the banking industry. The company TransNexus developed a system called NexOSS to detect fraudsters who use VoIP network.

Notably, researchers have shown deep concern about the detection and recognition of fraudsters. Researchers proposed various solutions to counter fraudulent activity. Becker *et al.* [10] differentiated legitimate and fraud accounts by a threshold which was found by utilizing historical data. However, there are too many types of user behavior in a real-world scenario. Thus this threshold method is inclined to misclassify normal users as fraudsters. They also introduced a signature-based approach which profiles the behavior of users, but it needs a more efficient profiling method. For the profile method, Yusoff et al [11] used a statistical model like Gaussian Mixed Model to profile users.

The associate editor coordinating the review of this article and approving it for publication was Guan Gui.

 This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see http://creativecommons.org/licenses/by/4.0/

However, there are still many challenges in this area. In a real-world scenario, fraudsters always tend to cover their tracks by roaming among different telecommunication operators while solutions are intendedly built for only one telecommunication operator. For example, Olszewski [12] introduced a model using Latent Dirichlet Allocation (LDA) to profile users, where an automatic threshold is built to detect fraudsters in one telecommunication operator. The lack of data also brings difficulties to researchers. Models hardly learn the behaviors of fraudsters from data with a limited amount of feature, and there is usually only a small number of fraudulent call samples. Henecka *et al.* [13] proposed a method to detect fraud across multiple databases, while only one feature (destination) is used to profile users. Ajmal *et al.* [14] proposed a framework to achieve privacy-preserving collaboration across multiple service providers to combat telecoms spam. Azad and Morla [15], [16] introduced a method to filter smart spammers in a decentralized schema with privacy-aware. Their model needs improvement on matching strategy for they only focus on the distance of two signatures. What is more, without real data source from the telecommunication operator, researchers have to do simulations to validate their model in a virtual scenario using simulated data, which makes their models and results less persuasive. Finally, for the real-world scenario, telecommunication operators need to exchange data if they want to cooperate in detecting roaming fraudsters. Data exchange may cause privacy violation problem. Thus privacy preserving policy is in urgent need to protect the privacy of legitimate users.

Our previous work(the conference version) [17], in which we proposed a novel strategy with high accuracy and security through the cooperation among mobile telecommunication operators. We validated it with simulated data and showed its effectiveness. In this manuscript, we upgrade the model concerning the time complexity reducing in matching module and measurement of the safety of privacy. More importantly, we construct a new scenario with real-world CDRs dataset to evaluate our model, and it proves to be useful in the evaluation.

Our contributions can be summarized as the following:

1) We propose a Cooperative Fraud Detection model to uncover the sophisticated fraudsters who take advantage of transmitting phone calls among multiple operators to conceal their malicious behaviors.
2) We propose an efficient and accurate profiling method to profile the behavior of mobile phone users, a comprehensive and accurate matching method to detect fraudsters. Meantime, We prevent privacy leakage in the cooperation model efficiently.
3) We construct a real-world scenario using a set of real CDRs data provided by a leading telephony provider in China to validate the practicability of our model. The result shows that our model still has an impressive performance in a real-world scenario.

A set of experiments are conducted using real-world dataset, and we compare them with previous work to evaluate the accuracy and efficiency of our detection model. The Receiver Operating Characteristic (ROC) curves and the value Area Under Receiver Operating Characteristic (AUROC) are used to evaluate the accuracy of our model. Moreover, The scale of data is taken into consideration, and different parameters are set to show the influence of features of the datasets. The result shows that our detection model also has high accuracy, efficiency, and can prevent privacy disclosure efficiently in a real-world scenario.

The remainder of this work is organized as follows. Section II briefly introduces the relevant background knowledge including Latent Dirichlet Allocation(LDA), Maximum Mean Discrepancy(MMD) and Differential Privacy(DP). Section III describes our Cooperative Fraud Detection model and its application scenarios. Section IV to VI completely introduce our methods. Section VII show the evaluation of our work in a real-world scenario. A conclusion are drawn in Section VIII.

II. PRELIMINARIES

This section will introduce the basics of Latent Dirichlet Allocation(LDA) model, Maximum Mean Discrepancy(MMD) and Differential Privacy(DP).

A. LATENT DIRICHLET ALLOCATION (LDA)

Blei *et al.* [18] firstly introduced Latent Dirichlet Allocation(LDA), which is a generative probabilistic model for document collection or corpus. LDA is a three-level Bayes model, where a hidden set of topics can model each document as a finite mixture, and distribution over words models each topic. LDA can be applied in our scenario because each account can be regarded as a document, and each feature is the words. Thus the hidden identities of an account are the latent topics.

The process of LDA to generate a document is defined as follows:

Definition 1: For each document w in a corpus D: (1)Choose $N \sim Poisson(\xi)$. (2)Choose $\theta \sim Dir(\alpha)$. (3)For each of the N word w_n: Choose a topic $z_n \sim Multinomial(\theta)$. Choose a word w_n from $p(w_n|z_n, \beta)$.

Where the w denotes a document, w_n denotes the n-th word in the document sequence, N denotes the number of words in a document, z denotes the topic.

B. MAXIMUM MEAN DISCREPANCY (MMD)

Gretton *et al.* [19], proposed a framework for analyzing and comparing distributions, using statistical tests to determine if two samples are drawn from different distributions. Firstly, the problem is defined as follows:

Problem 1: Let p_x and p_y be Borel probability measures defined on domain $\mathcal{X}$. Given observations $X := \{x_1, \cdots, x_m\}$ and $Y := \{y_1, \cdots, y_n\}$, drawn independently and identically distributed (i.i.d.) from p_x and p_y, respectively, can it decides whether $p_x \neq p_y$?

To solve this problem, there is the Lemma.1:

Lemma 1: Let $(\mathcal{X}, d)$ be a metric space, and let p_x, p_y be two Borel probability measures defined on $\mathcal{X}$. Then $p_x = p_y$ if and only if $E_{x\sim p_x}(f(x)) = E_{y\sim p_x}(f(y))$ for all $f \in C(\mathcal{X})$, where $C(\mathcal{X})$ is the space of bounded continuous functions on $\mathcal{X}$.

Therefore a rich and general function classes $\mathcal{F}$ will be used to define MMD which can measure the disparity between two samples, the definition is:

Definition 2: Let $\mathcal{F}$ be a class of functions $f : X \to \mathbb{R}$ and let p_x, p_y, X, Y be defined as above. The maximum mean discrepancy (MMD) is defined as:

$$MMD[\mathcal{F}, p_x, p_y] := sup_{f\in\mathcal{F}}(E_{x\sim p_x}[f(x)] - E_{y\sim p_y}[f(y)]) \quad (1)$$

C. DIFFERENTIAL PRIVACY (DP)

Security of a statistical database must be ensured. Dalenius [20] described a desideratum that none individual information should be learned without access to the database. However, Dword [21] proved it is impossible later, but he proposed a new model, which was called Differential Privacy(DP), to ensure that, any given disclosure will be, within a small multiplicative factor, just as likely whether or not the individual participant in the database, i.e., the presence of an individual data would not be the cause of information disclosure. The rigorous definition of DP is showed in Definition 3:

Definition 3: A randomized function M gives ϵ-differential privacy if for all data sets D_1 and D_2 differencing on at most one element, and all $S \subseteq Range(M)$:

$$Pr(M(D_1) \in S) \leq exp(\varepsilon) \times Pr(M(D_2) \in S) \quad (2)$$

By applying DP, users are allowed to interact with the database only by statistical queries. Other privacy methods such as homomorphic encryption usually publish a variant version of the original database, which provides less efficiency than DP. What is more, DP can prevent risk caused by leakage of encryption keys. Moreover, it can handle complex and various real data better and block more kinds of attack.

Random noise whose magnitude is chosen as a function of L_1-sensitivity is added to each query result to achieve DP when the result is numeric. L_1-sensitivity, which is showed in Definition 4 is the largest change a single participant could have on the output to query function.

Definition 4: For $f : D \to R_d$, the L_1-sensitivity of f is:

$$\triangle f = max_{D_1,D_2}||f(D_1) - f(D_2)|| \quad (3)$$

for all D_1, D_2 differing in at most one element.

III. COOPERATIVE FRAUD DETECTION MODEL AND ATTACK MODEL

This section presents the application scenarios for our work. We propose our cooperative fraud detection model, as well as the attack model, including the fraud forms and possible privacy attacks.

A. APPLICATION SCENARIOS

To detect the fraudsters accurately and efficiently, we propose a model based on the cooperation of multiple telecommunication operators. Our application scenario is shown in Figure.1. All of the operators have a database of their user data, but only one of them possess a fraud accounts list, so the other operators can apply our model to find out those fraudsters in its database even hidden ones.

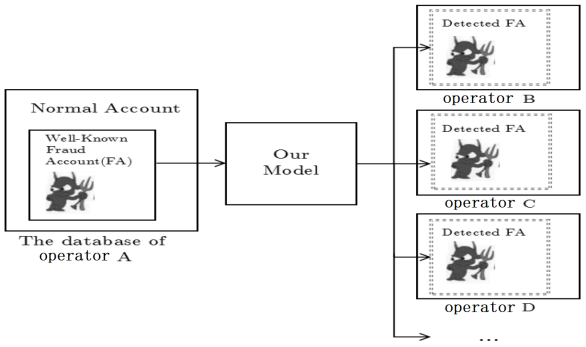


FIGURE 1. Application scenarios.

In this manuscript, to validate our model's practicability, we construct a real-world scenario using a set of call data records(CDRs) data, which will be discussed in Section VII in detail.

B. OUR COOPERATIVE FRAUD DETECTION MODEL

The traditional methods detect fraudsters in one telecommunication operator. They use various profiling methods to profile the characteristic of individual accounts through features such as duration, destination. Classification algorithm can be used to detect the fraudsters due to the observation that fraud accounts always behave differently from legitimate users.

However, experienced and sophisticated fraudsters also have some countermeasures. They roam among multiple telecommunication operators to hide their tracks. It is hard for traditional methods to deal with those fraudsters. However, for the fraudster always wants to save cost, it can be assumed that a fraudster would have the same behaviors in two operators, so the characteristics of two accounts would be alike. According to this assumption, a cooperative fraud detection model between two telecommunication operators is built as follows:

1) Get the CDRs from operator A.
2) Profile the behavior of fraud accounts in operator A using our profile module based on LDA.
3) Use our match module based on MMD to determine the similarity between accounts in operator A and another operator B.
4) Find out fraudsters in operator B by setting a threshold.

Illustration of our model is shown in Fig.2.

C. ATTACK MODEL

In this manuscript, the following attack models are considered:

- Conventional scam: In this kind of attack, fraudsters make phone calls to a large number of legitimate users to fool them into paying extra fees or other fraud

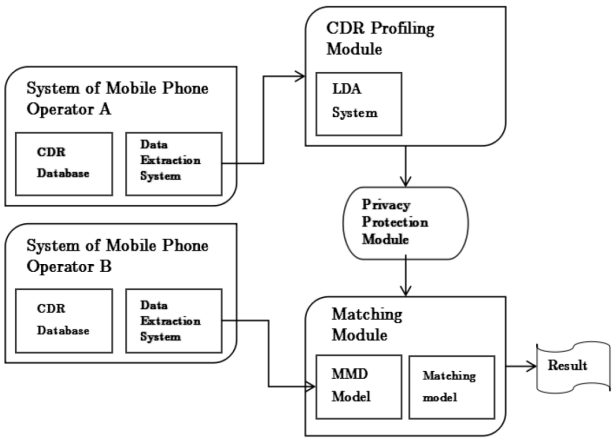


FIGURE 2. Cooperative fraud detection model.

activities. This kind of attack has unique behavior pattern and features. For example, they must make calls very frequently, and their target's locations should be distributed throughout a vast range of place. As a result, the fraudsters will be detected accurately using the profiling method. However, similar to other fraud detection problem, there are only a few fraudulent call samples for us to study the behavior pattern of fraudsters. We deal with this problem by proposing our cooperation model among multiple telecommunication operators.

- Subscription scam: In this kind of attack, fraudsters avoid paying fees by changing their device and service, for example, fraudsters sign up a new account in a new operator to continue his fraud activity. Traditional methods which focus on only one mobile operator cannot handle this kind of fraudsters efficiently and accurately. Our cooperation model contains an accurate matching method based on MMD, and it can detect this type of fraudsters without extra cost.
- Privacy attack: This attack is nothing about fraud; it is an accessory problem coming with our cooperation model. In our model, all operators can make queries to all other operator's database, resulting in a risk of personal privacy leakage. For example, attackers would get call duration of 101st call record if they make queries for the sum of the call duration of first 100 and first 101 call records. Even when the database only answers queries for sum statistics, the attackers can make such queries repeatedly to get the privacy information through the difference of answers. Sharing access to each others database is the fundamental of our fraud detection cooperation model, so it is impossible to prohibit making queries or stopping giving answers. To address this problem, we propose a method based on DP to block this kind of attacks.

IV. PROFILING MODULE

This section describes the profiling module based on Latent Dirichlet Allocation(LDA) to profile the behavior of accounts.

A. NOTATIONS OF VARIABLES

K : Number of latent class

ξ : The parameter of Poisson distribution

α : It is the parameter of prior Dirichlet distribution over the latent class

V : The number of features

β : It is $K \times V$ matrix, whose rows denote the parameters of the Multinomial distributions

a : Denote the feature vector.

N : Denote the number of iterations.

Γ : Denote the Gamma Function.

z : Denote the class

z_i : Denote the ith class

B. USING LDA MODEL TO PROFILE USER

Mobile operators usually use Signature Based Fraud Detection to detect fraudsters, but it requires an accurate and efficient signature generating method. The kernel problem to profile user behavior is how to take advantage of historical data to find the user's behavior pattern, as well as to classify different types of user accurately.

LDA model was used to find the topic probabilities which provide an explicit representation of a document. LDA model is used to profile users in mobile operators. Data of an account can be viewed as a document, and the features or statics of an account are the words in the document. So the topics are referred to the unknown types, and these types may be legitimate user, fraud type A or fraud type B.

It is a three-level hierarchical Bayesian model. In our model, accounts are represented as a finite mixture over latent class, and distribution over multinomial represents the classes. In our method, there are seven features which are *duration*, *ringtime*, *callfrequency*, *clock*, *source*, *destination* and *callresult* as multinomial. Thus, an account is represented by probabilities vector of the K lass, and probabilities of the seven features represent a class.

An account can be generated from the LDA model using the following procedure in Algorithm 1. The hidden variables θ and z are estimated using variational approximation. A k-dimensional Dirichlet random variable θ can take values in the $(k-1)$-simplex. A k-vector θ lies in the $(k-1)$-simplex if:

$$\theta_i \geq 0, \quad \sum_{i=1}^{k} \theta_i = 1 \tag{4}$$

And has following probability density on this simplex:

$$p(\theta|\alpha) = \frac{\Gamma(\sum_{i=1}^{k} \alpha_i)}{\prod_{i=1}^{k} \Gamma(\alpha_i)} \theta_1^{\alpha_1 - 1} \cdots \theta_k^{\alpha_k - 1} \tag{5}$$

And the parameters α and β of this model can be estimated by using the EM algorithm(α and β maximize the (marginal) log likelihood of the data).

Given the parameters α and β, the joint distribution of a latent class mixture θ, and z. The vector of V features a is

Algorithm 1 generating Accounts Data Using LDA

Require: ξ, α, β

Ensure: a

1: randomly draw the number of iterations $N \sim Poisson(\xi)$;
2: randomly draw the parameter for generating account from the class distribution $\theta \sim Dirichlet(\alpha)$;
3: **for** each of the N multinomials a_i **do**
4: draw the class z_i, $z \sim Multinomial(\theta)$;
5: draw the feature a_i from $p(a|z_i, \beta)$ which is a multinomal probability distribution vector of features a in the class z_i, which is in the row of the matrix-parameter β
6: **end for**
7: **return** a;

given by:

$$p(\theta, z, a|\alpha, \beta) = p(\theta|\alpha)\prod_{i=1}^{K} p(z|\theta)p(a|z_i, \beta) \tag{6}$$

The marginal distribution of an account in the mobile phone operator is defined as:

$$p(a|\alpha, \beta) = \int p(\theta|\alpha)(\prod_{i=1}^{N}\sum_{i=1}^{N} p(z_i|\theta)p(a_i|z_i, \beta)) \tag{7}$$

For each account, refer to the work of Girolami and Kabán [22], the distribution is calculated as:

$$\begin{aligned} p(a_{LDA}) &= \int_{\triangle} p(a|\theta)p(\theta|c_n)\mathrm{d}\theta \\ &= \sum_{k=1}^{K} p(a_{LDA}|k)E_{p(\theta|c_n)}\{\theta_k\} \\ &\approx \sum_{k=1}^{K} p(a_{LDA}|k)E_{D(\theta|c_n)}\{\theta_k\} \\ &= \sum_{k=1}^{K} p(a_{LDA}|k)\frac{\gamma_{kn}}{\sum_{i=1}^{K}\gamma_{in}} \end{aligned} \tag{8}$$

where a_{LDA} represents an account, c_n denotes the phone calls of this account, γ_{in} denotes the variational free parameter. $E_{D(\theta|c_n)}\{\theta_k\}$ denotes expectation of discrete random variable θ_k with respect to $D(\theta|c_n)$. $E_p\{\theta_k\}$ denotes expectation of discrete random variable θ_k with respect to p.

V. MATCHING MODULE

We propose a matching method for two profiles of mobile phone users based on MMD. Any difference between the two profiles could be the key to distinguish normal and fraud users, and MMD can give the similarity of two distribution efficiently. Our model defines that if two samples generated by our profiling module from two mobile accounts are derived from the same distribution, they are the same type of user.

A. NOTIONS OF VARIABLES

P_i : the profile of the ith account in mobile phone operators.

p_i : the distribution of P_i.

x_i : the ith features of the profile P_x.

y_i : the ith features of the profile P_y.

$\mathscr{F}$: the function class of f.

$\mathscr{H}$: Reproducing Kernel Hilbert Space.

$\mathscr{X}$: Compact Metric Space.

k : the Gaussian Kernel Function.

x_c : tbe center of the kernel function.

σ : the width of kernel function which can control the influence range of kernel function.

x^* : the normalized features of the profile P_x.

$Fraud_A$: the fraud list of operator$A$.

$Fraud_B$: the fraud list of operator$B$.

threshold : the parameter of our model which control the tolerability of our model.

B. OUR MATCHING METHOD

In our model, the generated profile is denoted as P_i for every account i. Essentially, each P_i is derived from distribution p_i, i.e. $P_i \sim p_i$. Assume that there is already a profile of fraud account, say, P_i, and it is derived from a hidden distribution p_i. This fraud profile is used to compare with other account's profile to decide other accounts are fraudsters or not. Generally speaking, two profiles $P_i \sim p_i$ and $P_j \sim p_j$ need to be compared to decide whether $p_i = p_j$, i.e. they are the same type of users.

Two arbitrarily profile samples in the database, P_x and P_y:

$$\begin{aligned} P_x &:= [x_1, x_2, \ldots x_m] \\ P_y &:= [y_1, y_2, \ldots y_n] \end{aligned} \tag{9}$$

There is a unspecified function class $\mathscr{F}$, and the functions in { can help us to measure the disparity between p_i and p_j. According to the Definition.2, the Maximum Mean Discrepancy of these samples as 1.0. And a biased empirical estimate of the MMD as:

$$MMD_b[\mathcal{F}, p_x, p_y] := sup_{f\in\mathcal{F}}(\frac{1}{m}\sum_{i=1}^{m} f(x_i) - \frac{1}{n}\sum_{i=1}^{n} f(y_i)]) \tag{10}$$

To estimate the MMD, an appropriate function class which is rich enough to identify whether $p_x = p_y$ is needed generally, and it needs to be restrictive enough to provide useful finite sample estimates. If the class $\mathscr{F}$ is the unit ball in a Reproducing Kernel Hilbert Space(RKHS) $\mathscr{H}$, the empirical MMD can be computed efficiently. Therefore there is the Theorem.1:

Theorem 1: Let $\mathscr{F}$ be a unit ball in a universal RKHS $\mathscr{H}$, defined on the compact metric space $\mathscr{X}$, with associated kernel $k(.,.)$. Then $MMD[\mathcal{F}, p_x, p_y] = 0$ IF and only if $p_x = p_y$.

A witness function f is used to exhibit the maximum discrepancy between two distributions. In our model, $f(x)$ and

its empirical estimate $\hat{f}(x)$ are:

$$\hat{f}(x) \propto \langle \phi(x), \mu[p_x], \mu[p_y] \rangle = E_{x' \sim p_x}[k(x, x')] - E_{y' \sim p_y}[k(x, y')] \quad (11)$$

$$\hat{f}(x) \propto \langle \phi(x), \mu[P_x], \mu[P_y] \rangle = \frac{1}{m}\sum_{i=1}^{m} k(x_i, x) - \frac{1}{n}\sum_{i=1}^{n} k(y_i, x) \quad (12)$$

where the $k(x_i, x)$ is a kernel function. In our model, the Gaussian Radial Basis Function(RBF) Kernel is used to formulate the accurate MMD between p_x and p_y, which is defined as follows:

$$k(x, x_c) = Exp(\frac{-(||x - x_c||)^2}{(2\sigma)^2}) \quad (13)$$

In our model, an appropriate kernel width σ should be set carefully to assure the accuracy of MMD however, if $\sigma = 0$ or $\sigma \to \infty$, the empirical MMD is zero for any two distribution samples. Without losing generality, we set the σ to be the median distance between a point in the sets of all points in the P to avoid the extreme situation.

Finally, the equations (10), (12), (13) conclude the Maximum Mean Discrepancy of any two profiles generated by our profiling module.

The Algorithm 2 describes the pseudo code to predict the fraud account.

Algorithm 2 Predict the Fraud Account

Require: profile P_i for every accounts, $Fraud_B$, *threshold*
Ensure: $Fraud_A$.

```
for each account i in operatorA do
    set the minimum = ∞
    for each account j in Fraud_B do
        determine the MMD(P_i, P_j) between two accounts i and j
        if the MMD(P_i, P_j) is lower than the minimum of i then
            update the minimum
        end if
    end for
    if the minimum is lower than threshold then
        add account i into Fraud_A
    end if
end for
return Fraud_A;
```

In order to save time cost in this step, fraud accounts can be clustered into a smaller set under the condition that They are representative enough to replace all fraud account profiles. We use the k-means method to cluster fraud accounts as $Fraud_{cluster}$. In the above algorithm, replace $Fraud_B$ with $Fraud_{cluster}$ to get a faster algorithm.

VI. DIFFERENTIAL PRIVACY

This section introduces a privacy preserving method based on DP. It is used when the operators exchange information or make database queries.

A. NOTIONS

$G_k(S)$: the sum of k powers of all elements in set S, e.g. $G_2(a, b, c) = a^2 + b^2 + c^2$

$X_{i,j}$: the jth feature of the ith sample X_i

$Y_{i,j}$: the jth feature of the ith sample Y_i

B. THE METHOD BASED ON DP

To calculate the similarity between two accounts in different operators, say, operator A and B. They have to give out information about the involved account, as the witness function of MMD requires. However, the operator must protect their users' privacy. In other words, operator B will not give the operator A the exactly statistics feature of an account profile.

This problem can be solved by showing that the estimate of the witness function of MMD can be expressed as an expression of statistics on an account profile. Operator A computes the estimate of the witness function value on an account profile by making queries for statistics on that account in operator B. And operator A provides B with statistics which B needs to compute the estimate of witness function value on that account profile in operator B, so the MMD value is calculated without directly showing accounts profile to each other. Then noise to the query results to ensure that privacy attackers cannot get the attributes of an accounts specific call record, based on the DP.

The estimate of the witness function of MMD can be approximately expressed as expression of statistics on the accounts profile such as $G_k(x_i)$ and $G_k(y_i)$. Then function(12) can be estimated without the knowledge of accurate value of y_i. Let $Y_k = \frac{y_k}{2\sigma}$, $X_j = \frac{x_j}{2\sigma}$, and according to kernel function(13), there should be:

$$f(\hat{x}_j) = \frac{1}{m}\sum_{i=1}^{m} Exp((||X_i - X_j||)^2) - \frac{1}{n}\sum_{k=1}^{n} Exp((||Y_k - X_j||)^2) \quad (14)$$

As mentioned above, σ is set to be the median distance among all point pairs. Because A doesn't know the exact value of y_k, A regards all x_i as P. If the account in operator A is the same kind of fraudster as the fraud account in B that is compared with the account in A, the distance between y_i and x_j is in the range of distance between all other x_i and x_j with very high probability. Therefore, in this case, for all Y_k:

$$||Y_k - X_j|| \leq 1 \quad (15)$$

Consider series expansion:

$$Exp(t) = \sum_{i=0}^{\inf} \frac{t^i}{i!} \quad (16)$$

Construct a function $r(t)$:

$$r(t) = \frac{Exp(t) - (1 + t + \frac{t^2}{2} + \frac{t^3}{6})}{Exp(t)} \tag{17}$$

It is easy to derive that $r'(t) = Exp(-t)\frac{t^3}{6} > 0$ when $t > 0$. Thus when $0 < t \leq 1$, $r(t) \leq r(1)$ with error less than 2%. We use $1 + t + \frac{t^2}{2} + \frac{t^3}{6}$ as an approximate estimate of $Exp(t)$ to compute $\hat{f}(x_j)$. As shown above, the error of computing is less than 2% of the largest $k(y_k, x_j)$ with very high probability. The error is negligible when detecting the same type of fraudsters, for the MMD difference between two different kinds of accounts is large.

There are K features of account in the mobile telecommunication operators. The kernel function can be transformed as follows:

$$\begin{aligned}
&Exp((||Y_k - X_j||)^2) \\
&\quad \approx 1 + (||Y_k - X_j||)^2 + \frac{(||Y_k - X_j||)^4}{2} + \frac{(||Y_k - X_j||)^6}{3} \\
&\quad = 1 + \sum_{s=1}^{K}(Y_{k,s}^2 - 2Y_{k,s}X_{j,s} + X_{j,s}^2) + \sum_{s=1}^{K}\sum_{t=1}^{K}(Y_{k,s}^2 Y_{k,t}^2 \\
&\qquad + X_{j,s}^2 X_{j,t}^2 - 4Y_{k,s}^2 Y_{k,t} X_{j,t} - 4X_{j,s}^2 X_{j,t} Y_{k,t} + 2X_{j,s}^2 Y_{k,t}^2) \\
&\qquad + \sum_{s=1}^{K}\sum_{t=1}^{K}\sum_{r=1}^{K}(Y_{k,s}^2 Y_{k,t}^2 Y_{k,r}^2 - 2Y_{k,s}^2 Y_{k,t}^{@} Y_{k,r} X_{j,r} + \cdots \\
&\qquad + 2Y_{k,s}^2 X_{j,t}^2 X_{j,r}^2)
\end{aligned} \tag{18}$$

Therefore, $\hat{f}(x_j)$ can be computed given the values of $G_k(Y_{i,s})$ and other statistics on Y_i without using the exact value of $Y_{k,s}$ by querying for $\sum_{l=1}^{k-1} Y_{l,s}$ and $\sum_{l=1}^{k} Y_{l,s}$. At least noise has to be added to the results of these queries. As for other statistics such as $\sum_{k=1}^{n} Y_{k,s}^2\, Y_{k,t}^2\, Y_{k,r}^2$, attackers can't get the value directly in the same way. Combining the results of different queries and solving the equation group to get the information is out of our privacy attack model, and the computation complexity is high when n is large. Thus, only the results of queries of $\sum_{l=1}^{k} Y_{l,s}$ are added with noise, which also improves the availability of estimation result of MMD in this way.

Lets consider the details of adding noises.

Theorem 2: For a query f: $D \leq R^d$, the mechanism K_f that adds independently generated noise L with distribution

$$Lap(0, \sigma) : Pr(L = x) = \frac{1}{2\sigma} Exp(-\frac{||x||}{2\sigma}) \tag{19}$$

it gives $\frac{\Delta f}{\sigma}$-differential privacy.

Note that $\sum_{l=1}^{k} Y_{l,s}^q$ where $(q > 1)$ can be calculated with the values of $\sum_{l=1}^{k} Y_{l,s}$ and some symmetric polynomials of $Y_{l,s}$. We consider adding noise to the result of query for $\sum_{l=1}^{k} Y_{l,s}^2$ and computing the result of $\sum_{l=1}^{k} Y_{l,s}$ and the real value of $\sum_{1 \leq l \leq m \leq k} Y_{l,s} Y_{m,s}$. Attackers can't get the value of $Y_{i,s}$ directly from the results of quests for $\sum_{1 \leq l \leq m \leq k} Y_{l,s} Y_{m,s}$ and $\sum_{1 \leq l \leq m \leq k-1} Y_{l,s} Y_{m,s}$. However:

$$Y_{k,s} = \frac{\sum_{1 \leq l \leq m \leq k} Y_{l,s} Y_{m,s} - \sum_{1 \leq l \leq m \leq k-1} Y_{l,s} Y_{m,s}}{\sum_{l=1}^{k-1} Y_{l,s}} \tag{20}$$

the numerator can be calculated out accurately, and though attackers can only get the perturbed value of denominator, it cannot be too far from the real value, or would result in large error in estimation of MMD. Thus $Y_{k,s}$ calculated in this way is close to the real value of it.

Theorem 3: Let M_i each provides ϵ-differential privacy. $M(M_1(D), M_2(D), \ldots, M_n(D))$ provides $\sum_{i=1}^{n} \epsilon$-differential privacy

Therefore, noise can be added as follows. For the result of query for $\sum_{l=1}^{k} Y_l^q$ from operator A, operator B answers $\sum_{l=1}^{k} Y_l^q + noise$.

The confidence level of data which contains noise is also defined. By the definition of our privacy attack, the difference between the two queries can be used to infer our data, so the confidence level will define how close the attacker to real record data. When the noise is more significant than 0.5, two records would be impossible to distinguish for their statistical number is between 0 and 1. Thus

$$confidence\ level = \int_{-0.5}^{0.5} \frac{1}{2\sigma} Exp(-\frac{||x||}{2\sigma}) dx \tag{21}$$

Since B will also make queries to A for statistics, double noise would be involved in the final estimate result of MMD function. They can contribute partial noise to each side as long as the aggregated noise can promise differential privacy.

Lemma 2: Laplace distribution random variable $L \sim Lap(0, \sigma)$ can be simulated by the sum of 2n random variables as follows:

$$L = \sum_{i=1}^{n} (G_i + H_i) \tag{22}$$

where G_i and H_i are independent Gamma distributed random variables with densities following the formula:

$$Pr(G_i = x) = Pr(H_i = x) = \frac{(\frac{1}{\alpha})^{\frac{1}{n}} x^{\frac{1}{n-1}} e^{-\frac{x}{\alpha}}}{\Gamma(\frac{1}{n})} \tag{23}$$

where Γ is the Gamma Function

According to Lemma 2, operator A and operator B can add Gamma noise to their results of queries, such that the aggregated noise in the estimate of MMD is Laplace noise.

VII. EVALUATION

In this section, to evaluate the performance of our Cooperative Fraud Detection Model and the Privacy Protection Module in the real-world scenario, we conduct a set of experiments with different datasets and simulations using PYTHON. In the following, there are details of evaluations and results. We also compare the results with our previous evaluations and extend more experiments over the influence of different conditions on accuracy.

A. REAL-WORLD SCENARIO

We used generated data to evaluate the model and got relatively satisfactory results. It showed that our model has better performance than previous models. However, the generated data cannot be used to validate the practicability of our model. Thus a real-world scenario is needed to evaluate our model.

A real-world scenario is constructed using a set of CDRs data provided by a leading telephony provider in China. This data set consists of more than one million CDRs and involves about half a million users. It contains CDRs from 0:00 to 23:59, date at 15th March 2016, located at several cities in China. There is also a well known fraud account list with high reliability which comes from our another work [23].

With this dataset, the scenario can be constructed as follows. Without loss of generality, suppose there are only two telecommunication operators, A, and B. It is accessible to extend our model into multiple telecommunication operators scenario. The dataset is divided into two parts by city to represent two mobile telecommunication operators, i.e., operator A and B respectively. Suppose operator A possesses a well known fraud account list while operator B does not, and operator B wants to find out which users in his database are fraudsters with the help of operator A.

In this scenario, users from both telecommunication operators should be profiled in the first place. Thus the Profile module IV can be testified. Then operator B can use our Matching module V to seek fraudsters in his database. In the meantime, our Privacy module VI serve to protect the privacy of users from operator A.

B. EVALUATION SETTINGS

Since there is a real-world dataset which has more than seven features and more than one million CDRs, our model can be evaluated in the constructed real-world scenario using the following settings.

1) COOPERATIVE FRAUD DETECTION

To evaluate our cooperative fraud detection module, we conduct groups of basic experiments over different conditions.

In the real-world scenario, the scale of the dataset and the number of accounts must be taken into consideration. Operator A and B may have a large number of CDRs, or they may be willing to contribute a small set of it, so to study the influence of different scales is essential.

The details of number of accounts are in Table 1, where N denotes the sequence number of experiments, n_a denotes the number of accounts, n_c denotes the average number of CDRs for each account, n_f denotes number of fraud accounts, n_t denotes number of types of accounts, n_{fea} denotes number of features. In order to testify our methods on real-world records, our previous experiments shall be conducted again over settings of experiment #1 to #6.

Experiment #1 is most similar to our previous experiment settings, which has four features (duration, type, time, cost). In this dataset, there are only two feature match them, duration and time(i.e., clock). Cost should be linearly related to duration so that this feature can be omitted, and type does not matter if the target is to detect whether it is a fraud account instead of what type of fraud it is. Experiment #2 to #6 use five features (duration, ring time, call frequency, clock, destination). The other conditions remain same.

TABLE 1. The data scale setting.

N	n_a	n_f	n_c	n_t	n_{fea}
#1	1000	15	8	5	2
#2	1000	15	8	5	5
#3	5000	15	8	5	5
#4	5000	75	8	5	5
#5	5000	200	8	5	5
#6	5000	200	8	1	5

TABLE 2. Features setting.

N	n_{fea}	f_{dur}	f_{ring}	f_{fre}	f_{clk}	f_{src}	f_{des}	f_{res}
#1	2	✓	×	×	✓	×	×	×
#2-#6	5	✓	✓	✓	✓	×	✓	×
#7	1	✓	×	×	×	×	×	×
#8	1	×	×	×	×	×	✓	×
#9	3	✓	✓	✓	×	×	×	×
#10	1	×	×	×	✓	×	×	×
#11	3	×	×	×	×	✓	✓	✓
#12	7	✓	✓	✓	✓	✓	✓	✓

In the real-world scenario, two telecommunication operators may have different CDR data storage system. The features may not be the same as each other. Thus the number of features of an account should be taken into consideration. Different features are set in our experiments. The features information are in Table 2, where N denotes the sequence number of experiments, n_{fea} denotes the group number of features. f_{dur} denotes which is the length it last, the CDRs of fraudster should have similar call duration for the fact that the called person would end this call once the fraudsters show a similar sign. f_{ring} denotes ringing time, according to the observation of the real CDR data, most calls end with no answering, so the fraudsters should stop calling after a fixed ringing period. f_{fre} denotes the call frequency. A fraudster should have made a similar number of calls in a day. f_{clk} denotes clock, which is when this call begins. A fraudster should make his fraud call densely around some time points. f_{src} denotes calling source region which is where the call from, fraudsters usually do not travel around. f_{des} denotes called destination region, which is where the call went. The fraudsters usually have a list of the phone number which should be located nearby. f_{res} denotes call result, which is how this call processed by the operator if it is not ended usually, it has a high probability to be a fraud account. ✓ denotes this group contains this feature, × denotes that this group does not contain this feature. The feature settings of experiment #1 to #6 are shown in the first two lines of Table 2. Experiment #7 to #12 is under dataset scale settings of experiment #5.

Each numerical feature has a different parameter for its kernel function, which is in Table 3. These parameters are derived by analyzing data in training set. Some nonnumerical

TABLE 3. Parameters of kernel function in MMD.

parameters	f_{dur}	f_{ring}	f_{fre}
μ	59.74	5.79	3.4
σ	60.72	9.23	4.55

TABLE 4. Parameters of matching module.

N	k	n_c	n_f	n_t	n_{fea}
#13	10	5000	200	1	5
#14	100	5000	200	1	5
#15	1000	5000	200	1	5
#16	10000	5000	200	1	5

TABLE 5. Parameters of Laplace distribution $Lap(\mu, \sigma)$.

N	μ	σ	n_f
#17	0	0.001	4
#18	0	0.01	4
#19	0	0.5	4
#20	0	1	4
#21	0	10	4

features are not calculated using the kernel function, so they are not listed here.

Data scale may grow explosively in real-world scenario, so time complexity improvement is evaluated in Matching Module. The performance will be evaluated under different k which denotes the number of cluster centers of fraud accounts' CDRs. Detail of this experiment setting is shown in Table 4. Five features are the same with Experiment #6.

2) DIFFERENTIAL PRIVACY

Privacy protection is always necessary. In the constructed real-world scenario, operator A is willing to help operator B to find fraudsters, but A does not want his user data to be disclosed. DP is applied to the MMD result to protect privacy. Data of experiment #3 is used to set the stimulation to evaluate the influence of noise on the MMD result. It needs to find a suitable level of noise where both our data privacy and satisfactory detection accuracy can be ensured. The experiment parameters setting are showed in Table 5. In our application of privacy protection, the scale parameter of Laplace distribution, i.e., σ, is needed to confirm. We choose four feature which is *duration*, *ringtime*, *frequency* and *clock*, because the Laplace distribution can only be applied to numerical features.

Accordingly, it needs to evaluate how secure our data is. There would be an evil attacker, and he tries to steal private data. The confidence level of those stolen data is evaluated to evaluate our privacy protection methods.

C. EVALUATION RESULTS

Receiver Operating Characteristic(ROC) curve and Area Under Receiver Operating Characteristic(AUORC) are the common methods used to evaluate the accuracy of fraud detection model. In this manuscript, they are used to evaluate our model. A useful tool scikit-learn [24] is used to draw a ROC curve and calculate the AUROC value from our results.

TABLE 6. AUROC values.

N	#1	#2	#3	#4	#5	#6	#7
$AUROC$	0.637	0.768	0.747	0.765	0.781	0.808	0.537
N	#8	#9	#10	#11	#12	#13	#14
$AUROC$	0.299	0.720	0.522	0.460	0.772	0.462	0.485
N	#15	#16	#17	#18	#19	#20	#21
$AUROC$	0.621	0.732	0.810	0.801	0.791	0.452	0.348

In this section, the AUROC of our evaluation of real-world dataset is presented, and it shows that our model works well in the real-world scenario. Secondly, we will compare our work with previous ones. Thirdly, there is a discussion about influence over different parameters. Next, we will validate our improvement in MMD module. Finally, we will analyze the influence of DP on our model.

1) COOPERATIVE FRAUD DETECTION

Firstly we present the AUROC value of all the experiments to show the accuracy of our model. They are shown in Table 6. Our best result is $AUROC = 0.808$ in Experiment #6. It makes full use of all the available feature. Experiment #2 to #6 have similar performance, and they are all the better than Experiment #1. The high accuracy shows that operator B can find out fraudsters in his database with the help of our model, which implies that our method works well in the real-world scenario. Other experiments show the capability of our model in a real-world scenario. Some single feature does not work in our model like Experiment #7 and #8 while some feature combination works well together like Experiment #11. In a real-world scenario, more features do not guarantee higher accuracy, as is shown that Experiment #6 ($AUROC = 0.808$) with five features outperforms Experiment #12 ($AUROC = 0.772$) with seven features. Experiment #17-#21 show that our privacy module will decrease accuracy, but it is affordable. To protect privacy in a real-world scenario is necessary, and experiments show that our model can make a good compromise between accuracy and privacy.

Next, there is the ROC curves comparison between Experiment #1 and #2 in Figure 3. Experiment #1 represents our previous and Experiment #2 represents our current setting. When there is the same number of fraud accounts, our current setting has a lower false rate and has higher AUROC value. It shows that our method works better on the real-world records using the current setting.

Thirdly, it comes to the discussion of influence over different parameters. In a real-world scenario, suitable parameters need to be set according to the specific environment.

a) Data scale is concerned in Experiment #2 to #5. When the fraud account number is fixed to 15, two data scale 1000 CDRs(experiment #2) and 5000 CDRs(experiment #3) are compared in Fig.4, which implies that fraud accounts are easier to be detected in a smaller dataset. It is because the smaller

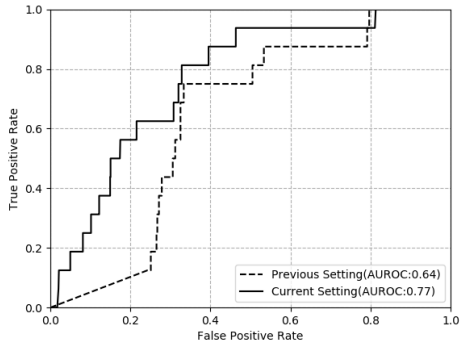


FIGURE 3. Comparison between previous and current settings.

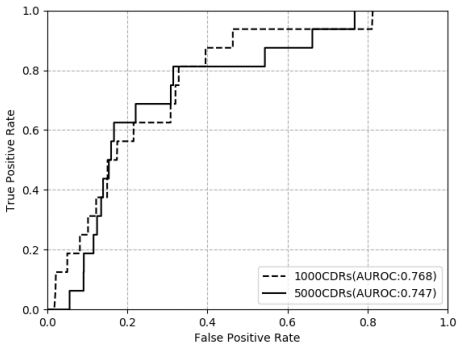


FIGURE 4. Data scale's influences-same fraud number 15.

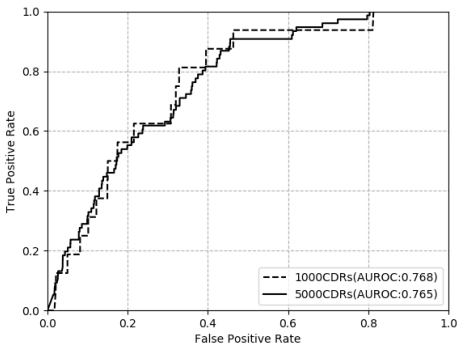


FIGURE 5. Data scale's influences-same fraud ratio 1.5%.

the dataset is, our MMD module can distinguish distance between accounts more effectively.

When the fraud ratio is fixed to 1.5%, two data scale 1000 CDRs(experiment #2) and 5000 CDRs (experiment #4) are compared in Fig.5. There is no much difference. When the CDR number is 5000, fraud ratio is set to 0.3%(experiment #3), 1.5%(experiment #4) and 4%(experiment #5) in Fig.6. Higher fraud ratio dataset has higher AUROC value, but the ROC curve of experiment #3 is steeper, and it even outperforms experiment #5 at some points. This is because when the fraud ratio is low, the account profiles generated by LDA module can be accidentally concentrated.

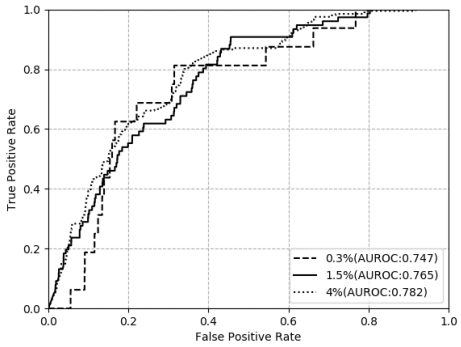


FIGURE 6. Data scale's influences-influence of fraud ratio.

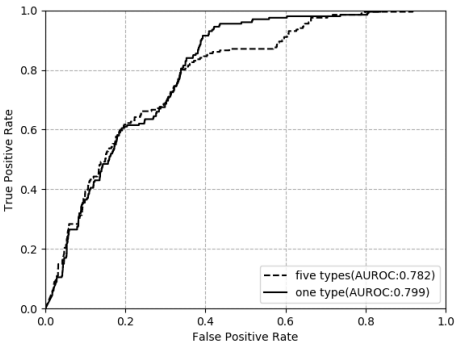


FIGURE 7. Influence of number of fraud types.

Moreover, this can be confirmed by the non-smoothness of the ROC curves.

b) Number of account types also have influence; it is validated in experiment #5 and #6. Our dataset provides five types of accounts, including fraud, telemarketing, advertising, etc. There is only a fraud type in experiment #6; as a contrast, there are five different types of abnormal accounts in Experiment #5. See Fig.7. It shows the detection method performs better on the dataset with only one type fraud account: the AUROC value(0.799) is higher, and experiment #6 has higher True Positive Rate(TPR) when they have same False Positive Rate(FPR). The reason is obvious: when there are fewer types of abnormal accounts, interference is also reduced so that the MMD module can detect fraud account more easily.

c) Different features' impact is observed and studied in experiment #7 to #12. From the AUROC values in Fig.8, some of them are even lower than 0.5. Only Experiment #9 and #12 have relatively satisfactory results. Experiment #9 use these features:*duration*, *ring_time*, *call_frequency*, which are all numerical features, while Experiment #10 and #11 use all non-numerical features: *clock*, *source*, *destination* and *call_result*. In general, numerical features have a stronger impact on the detection performance, and non-numerical features can only make a limited contribution. The result of Experiment #12(AUROC = 0.772)

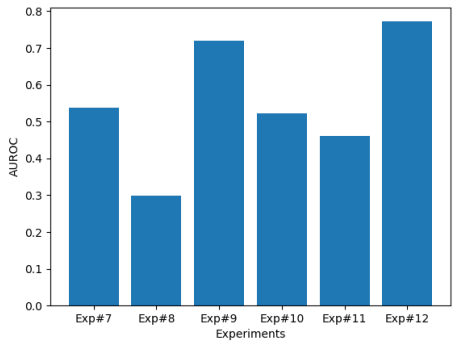


FIGURE 8. Influence of features.

TABLE 7. AUROC values and time cost.

N	k	AUROC	Time/s
13	10	0.462	26
14	100	0.485	80
15	1000	0.621	901
16	10000	0.732	8564
6	none	0.808	84779

shows that the MMD module has better performance when the features are jointly used. The reason is that when more features are combined, the MMD has more dimensions to classify accounts.

We have made some optimization in MMD module's algorithm complexity, and Experiment #13 to #16 are set to validate our improvement. Experiment #6 does not use this clustering method, and its CDRs number is about 100000. The AUROC value and time cost are in Table7. From the table, it shows that our method takes much less time to finish the MMD module while keeping relatively high AUROC value. When the number of cluster points is less than 1% of total CDRs number in Experiment #13 and #14, the MMD matching module loses its detection function(AUROC value are under 0.5). If the number of cluster points is set higher than 1% of total CDRs number in Experiment #15, the MMD module can predict through the AUROC value is just 0.621. The compromised choice would be set cluster number to 10% of total CDRs number in Experiment #16. We can keep a relatively high prediction ability(AUROC $=$ 0.732) while it saves time cost up to 90%.

2) DIFFERENTIAL PRIVACY

To validate the practicability of our model, we experiment in a real-world scenario, and results are shown in this subsection. In our model, Laplace noise is added to avoid attackers to get private CDR data. However, the noise also can influence the exact result of MMD. Thus, simulations are done to evaluate the influence of noise on the result of MMD. We draw the *noise* from Laplace distribution. Experiment #17 to #21 are designed to study the influence of different levels of noise on MMD results. In the meantime, we would evaluate the data confidence level from the privacy attacker's perspective, because data with high-level noise can be meaningless to the attackers. The results are in Table8. In the table, once the noise level is higher than 1 (Experiment #20), our model fails to detect the fraud accounts(AUROC $=$ 0.452, which is under 0.5). Moreover, when the noise level is lower than 0.1 (Experiment #17 and #18), the privacy attacker can get our data with confidence level very close to 1, which would threaten our data privacy. So a compromised option would be Experiment #19, our model can keep a relatively high AUROC value(0.719) while the privacy attacker can only get data with confidence level 0.63 which means that our private data is safe from differential attack.

TABLE 8. AUROC values and time cost.

N	Noise Level	AUROC	Confidence Level
6	0	0.808	1.0
17	0.005	0.810	$1-10^{-200}$
18	0.05	0.801	$1-10^{-20}$
19	0.5	0.791	0.632
20	1	0.452	0.40
21	10	0.348	0.05

VIII. CONCLUSION

In this manuscript, we succeed in validating the cooperative fraud detection model over a real-world scenario. By a set of comprehensive experiments, our methods, including LDA to profile accounts and MMD to match fraud accounts, are adaptive to the real-world dataset. We also validate the protection to private data of users during the cooperation of multiple telecommunication operators.

Our enhanced and comprehensive evaluations show that the improved detection model is capable of detecting fraud accounts with high accuracy in real-world situations where the data scale is larger, and the model is also suitable for real-world features. Meantime applying privacy protection does not affect the accuracy of detection with well-chosen level Laplace noise.

ACKNOWLEDGMENT

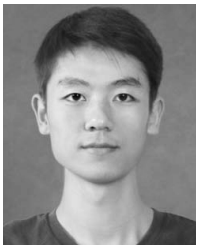
(Na Ruan and Zhikun Wei contributed equally to this work.)

REFERENCES

[1] R. J. Bolton and D. J. Hand, "Statistical fraud detection: A review," *Stat. Sci.*, vol. 17, no. 3, pp. 235–249, 2002.
[2] M. Weatherford, "Mining for fraud," *IEEE Intell. Syst.*, vol. 17, no. 4, pp. 4–6, Jul. 2002.
[3] H. Tu, A. Doupé, Z. Zhao, and G.-J. Ahn, "SoK: Everyone hates robocalls: A survey of techniques against telephone spam," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2016, pp. 320–338.
[4] N. Miramirkhani, O. Starov, and N. Nikiforakis, "Dial one for scam: A large-scale analysis of technical support scams," 2016, *arXiv:1607.06891*. [Online]. Available: https://arxiv.org/abs/1607.06891
[5] Y. Wang, M. Liu, J. Yang, and G. Gui, "Data-driven deep learning for automatic modulation recognition in cognitive radios," *IEEE Trans. Veh. Technol.*, vol. 68, no. 4, pp. 4074–4077, Apr. 2019.
[6] G. Gui, H. Huang, Y. Song, and H. Sari, "Deep learning for an effective nonorthogonal multiple access scheme," *IEEE Trans. Veh. Technol.*, vol. 67, no. 9, pp. 8440–8450, Sep. 2018.
[7] J. Wang, F. Dai, J. Yang, and G. Gui, "Efficient combination policies for diffusion adaptive networks," *Peer-Peer Netw. Appl.*, vol. 12, pp. 1–14, Feb. 2019.

[8] F. Cheng, G. Gui, N. Zhao, Y. Chen, J. Tang, and H. Sari, "UAV-relaying-assisted secure transmission with caching," *IEEE Trans. Commun.*, vol. 67, no. 5, pp. 3140–3153, May 2019.
[9] N. Zhao, Q. Cao, G. Gui, Y. Cao, S. Zhang, Y. Chen, and H. Sari, "Secure transmission for interference networks: User selection and transceiver design," *IEEE Syst. J.*, to be published.
[10] R. A. Becker, C. Volinsky, and A. R. Wilks, "Fraud detection in telecommunications: History and lessons learned," *Technometrics*, vol. 52, no. 1, pp. 20–33, 2010.
[11] M. I. M. Yusoff, I. Mohamed, and M. R. A. Bakar, "Fraud detection in telecommunication industry using Gaussian mixed model," in *Proc. IEEE Int. Conf. Res. Innov. Inf. Syst. (ICRIIS)*, Nov. 2013, pp. 27–32.
[12] D. Olszewski, "A probabilistic approach to fraud detection in telecommunications," *Knowl.-Based Syst.*, vol. 26, pp. 246–258, Feb. 2012.
[13] W. Henecka and M. Roughan, "Privacy-preserving fraud detection across multiple phone record databases," *IEEE Trans. Dependable Secure Comput.*, vol. 12, no. 6, pp. 640–651, Dec. 2015.
[14] M. Ajmal, S. Bag, S. Tabassum, and F. Hao, "privy: Privacy preserving collaboration across multiple service providers to combat telecoms spam," *IEEE Trans. Emerg. Topics Comput.*, to be published.
[15] M. A. Azad and S. Bag, "Decentralized privacy-aware collaborative filtering of smart spammers in a telecommunication network," in *Proc. ACM Symp. Appl. Comput.*, 2017, pp. 1711–1717.
[16] M. A. Azad and R. Morla, "Rapid detection of spammers through collaborative information sharing across multiple service providers," *Future Gener. Comput. Syst.*, vol. 95, pp. 841–854, Jun. 2019.
[17] W. Yao, N. Ruan, F. Yu, W. Jia, and H. Zhu, "Privacy-preserving fraud detection via cooperative mobile carriers with improved accuracy," in *Proc. IEEE 14th Annu. Int. Conf. Sens., Commun., Netw. (SECON)*, Jun. 2017, pp. 1–9.
[18] D. M. Blei, A. Y. Ng, and M. I. Jordan, "Latent Dirichlet allocation," *J. Mach. Learn. Res.*, vol. 3, pp. 993–1022, Mar. 2003.
[19] A. Gretton, K. M. Borgwardt, M. J. Rasch, B. Schölkopf, and A. Smola, "A kernel two-sample test," *J. Mach. Learn. Res.*, vol. 13, pp. 723–773, Mar. 2012.
[20] T. Dalenius, "Towards a methodology for statistical disclosure control," *Statistik Tidskrift*, vol. 15, nos. 429–444, pp. 1–2, 1977.
[21] C. Dwork, "Differential privacy: A survey of results," in *Proc. Int. Conf. Theory Appl. Models Comput.* Xi'an, China: Springer, 2008, pp. 1–19.
[22] M. Girolami and A. Kabán, "Sequential activity profiling: Latent Dirichlet allocation of Markov chains," *Data Mining Knowl. Discovery*, vol. 10, no. 3, pp. 175–196, 2005.
[23] J. Liu, B. Rahbarinia, R. Perdisci, H. Du, and L. Su, "Augmenting telephone spam blacklists by mining large CDR datasets," in *Proc. ACM Asia Conf. Comput. Commun. Secur.*, 2018, pp. 273–284.
[24] F. Pedregosa, G. Varoquaux, A. Gramfort, V. Michel, B. Thirion, O. Grisel, M. Blondel, P. Prettenhofer, R. Weiss, V. Dubourg, J. Vanderplas, A. Passos, D. Cournapeau, M. Brucher, M. Perrot, and É. Duchesnay, "Scikit-learn: Machine learning in Python," *J. Mach. Learn. Res.*, vol. 12, pp. 2825–2830, Oct. 2011.

NA RUAN received the Ph.D. degree in computer science from Kyushu University, Japan, in 2012. She is currently an Assistant Professor with the Department of Computer Science and Engineering, Shanghai Jiao Tong University, China. Her research interests include big data, security and privacy, networks, and block chain.



ZHIKUN WEI is currently pursuing the master's degree with the Department of Computer Science and Engineering, Shanghai Jiao Tong University, China. His research interests include security, privacy, and machine learning.

JIENAN LIU is currently pursuing the Ph.D. degree with the Department of Computer Science, University of Georgia, Athens, GA, USA. His research interests include machine learning and data mining.