Proceeding of the 7th TICC International Conference 2023
Toward Sustainable Development Goals: Transformation and Beyond
February 4-5th, 2023, Chiang Mai, Thailand

Research on Triple Encryption Algorithm

Lin Wu1[1] and Ahmad Yahya Dawod[2]

International College of Digital Innovation, Chiang Mai University, Chiang Mai, 50200, Thailand[1]
E-mail: lin_wu@cmu.ac.th
International College of Digital Innovation, Chiang Mai University, Chiang Mai, 50200, Thailand[2]
E-mail: ahmadyahyadawod.a@icdi.cmu.ac.th

Abstract

This paper proposes an optimization model of information security. The algorithm is optimized based on the most common elliptic encryption algorithm. First, the data is encrypted by the elliptic curve digital signature algorithm. Then, the Tang poetry dictionary is divided into a hash table by the Tang poetry encryption algorithm, and the hash table is converted into bit characters according to the rhythm of the Tang poetry to generate the encrypted text. If the first and second layers are cracked and destroyed by malicious users, the system will enable the convolutional neural network and use the deep learning algorithm to form the convolutional countermeasures algorithm. On the premise of ensuring data security, a server cluster is built with multiple servers so that the load balancing service can process the input data, schedule the visited servers according to the load size, and allocate specific access servers to improve the processing performance.

After many tests, the information security model proposed in this paper can keep the protection rate of malicious attacks above 90% without affecting the performance of the server.

KEYWORDS: Encryption algorithm, elliptic encryption, performance optimization, load balancing

1 INTRODUCTION

In the 21st century, the tourism industry has become one of the important ways for countries to communicate with each other. Especially since the COVID-19 epidemic, the heavy damage to the tourism industry is also in urgent need of recovery with the opening-up of China. However, in tourism, especially transnational tourism, the problem of information leakage is also the research focus of major companies[1].

In 2011, the user database of CSDN website was leaked online by hackers, revealing about 6 million email passwords. In 2016, Yahoo user account information was hacked and at least 500 million user information was compromised. In view of the above, there are many applications of data encryption papers. For example, elliptic encryption algorithms are frequently used in many data encryption files.Some researchers propose to study the data encryption of electronic tags in RFID, the core technology of the Internet of Things, and optimize the underlying scalar multiplication of elliptic curve encryption system [2].Some researchers have proposed a data encryption scheme based on elliptic curve in the cloud computing environment to solve security problems such as easy leakage and illegal tamper of massive data in the cloud computing environment, as well as the shortcomings of general encryption algorithms such as RSA (Rivest Sharmir Adleman) with low security level and complex calculation [3].In addition, some researchers proposed

that in order to realize the secure and efficient sharing of cloud data, an attribute encryption scheme based on elliptic encryption algorithm (ECC) and supporting fine-grained revocation. [4]

However, most of the above studies adopt single-layer encryption, and the protection of data is relatively single[5].Once the public key of single-layer encryption is mastered, the user's data will be in an dangerous state[4].Therefore, a triple encryption algorithm is proposed in this paper for the first time.The first is to encrypt the data using an elliptic curve digital signature algorithm,In elliptic curve encryption (ECC), a special form of elliptic curve is used, that is, an elliptic curve defined over a finite field.$y^2 - x^3 + ax + b(\mod p)$, where p is a prime number, and a and b are two non-negative integers less than $p : 4a^3 + 27b^2(\mod p) \neq 0,\ x,\ y,\ a, b \in Fp,$ and then the points (x, y) satisfying equation (2) and an infinite point o form the elliptic curve E.

Let the above formula be $\sqrt{(2\&x^3 + 2x + b)},\ x \in [10, 100]$

And use the Tang encryption algorithm to encrypt the data for the second time, According to the existing research, there is already an encryption method based on Song Ci [6] (Song Dynasty is a dynasty in Chinese history, and Song Ci is a unique poetry theme of Song Dynasty, with unique rhythm[7]). so the encryption of Tang poetry proposed in this paper is based on the poetry of another dynasty, Tang Dynasty, as a blueprint for encryption .The Tang poems are decomposed into a hash table, converted into bits according to the rhythm of the Tang poems, and encrypted text is generated; If the first and second time are cracked and damaged by malicious users, Since convolutional neural network is one of the most popular algorithms for confrontation[8], this paper decides to improve it on the basis of previous algorithms[9], the system will enable convolutional neural network and use deep learning algorithm to form a convolutional countermeasures algorithm.And improve the reflection speed of various encryption algorithms by load balancing[10].

2 METHOD AND MATERIALS

For elliptic curve encryption (ECC), a special form of an elliptic curve is used, that is, the elliptic curve defined on a finite field.$y^2 = x^3 + ax + b(\mod p)$, Here P is a prime number, and a and b are two nonnegative integers smaller than $P\ 4a^3 + 27b^2(\mod p) \neq 0$ among, $x,\ y,\ a,\ b \in Fp,$ Then the point $(x,\ y)$ satisfying equation (2) and an infinite point o comform to the elliptic curve E.

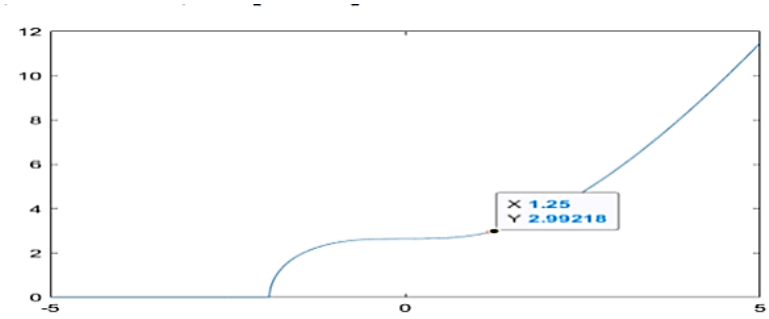

Figure 1: *elliptic encryption algorithm*

Input the training set X and the test set Y into the encrypted data set obtained by the algorithm respectively. By this step, it can ensure that the data is in the ciphertext form while using, and ensure the privacy and security of users.

The elliptic curve digital signature algorithm is used to encrypt the data at first, and the Tang poetry encryption algorithm is used to encrypt the data for more security. (PS: According to the existing research, there is already an encryption method based on Song Ci [6] (Song Dynasty is a dynasty in Chinese history, and Song Ci is a unique poetry theme of Song Dynasty, with unique rhythm[7]), so the encryption of Tang poetry proposed in this paper is based on the poetry of another dynasty, Tang Dynasty, as a blueprint for encryption)The Tang poetry is divided into a hash table, converted into bit representation according to the rhythm of Tang poetry, then the encrypted text is generated; If the first and second time is cracked and broken by malicious users, the system will enable a convolutional neural network and use a deep learning algorithm to triger a convolutional confrontation algorithm. The diagram is as follows:

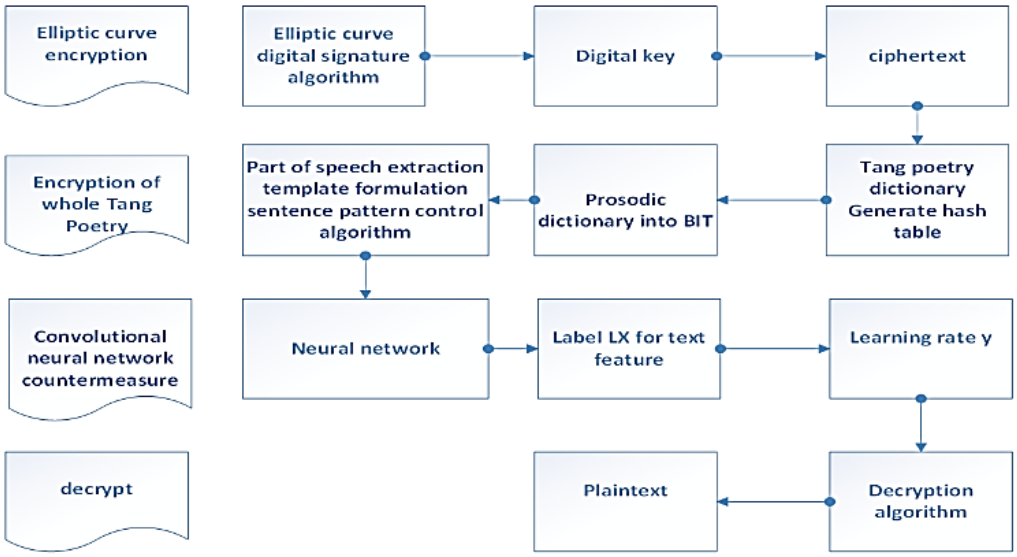

Figure 2: *encryption flow chart of Tang Poetry*

The convolution neural network algorithm based on Countermeasure Input: encrypted text, neural network F, text label LX, target label LT, learning rate y Output: deceptive text XF

1) for loop the following is the main steps for the algorithm 1000 iteration do
2) Get original eigenvalue score=f(x) Initialize target label Lt=Random()
3) Calculate target eigenvalue score = s[Lx, Lt]
4)Back propagation st.backwerd(),Calculated gradient r:=x-xf
5)Get increment dx
6)Generate deceptive text xf=x+d;
7)End for Until STOP
8)return xf

3 PERFORMANCE IMPROVEMENT

In order to improve the data access efficiency, a server cluster is built by multiple servers. The external data access first enters the load balancing service, which is responsible for scheduling the servers according to the load and allocation. The diagram of the server cluster is shown in figure 5 load balancing server:

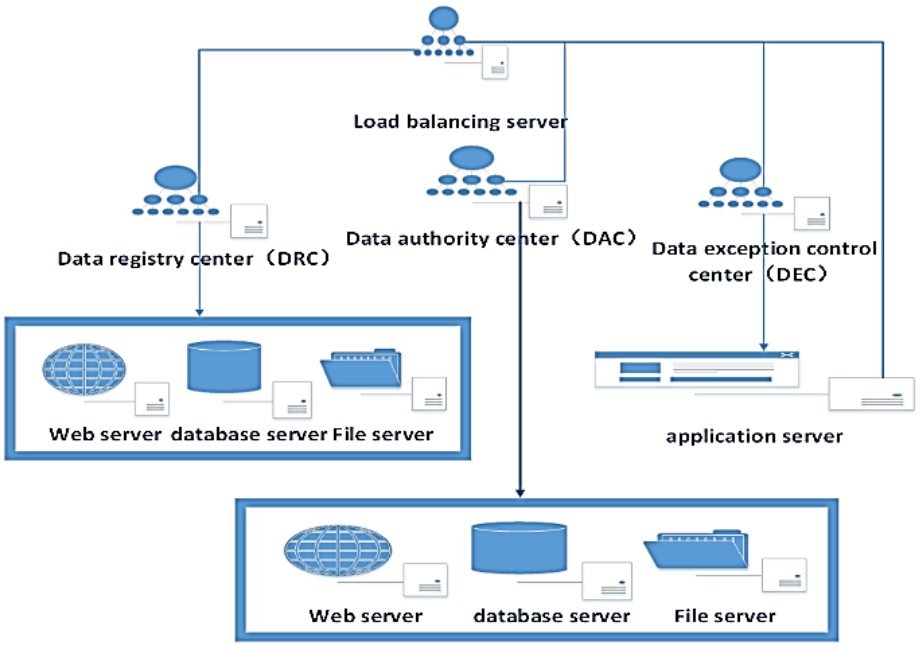

Figure 3: *load balancing server*

Due to large access and heavy load, the data registration center and data authority center can set up multiple web servers, database servers, and file servers. To handle exceptions, the data exception control center and application servers are temporarily set up with one server as shown in the figure5.

Each server will contaion the information table such as hard disk utilization, CPU consumption, and memory utilization. Each server can be regarded as a data domain. A tree is formed between the data domain. The spatial search tree algorithm can be used to sort the performance usage of building a service cluster. Servers with less load will be called first when accessing. The node attribute division in the spatial search tree is determined by information entropy. If the proportion of class k samples in the current sample set D is Pk $(k = 1, 2, 3, - - --, |y|)$, the information entropy of D can be,

$$\mathrm{Ent}(D) = -\sum_{k=1}^{|y|} P_K \log_2 P_K \tag{1}$$

The smaller the value of Ent (D), the higher the purity of D.

The information gain of the attribute can be calculated according to the sample data and weight of utilization, CPU consumption, memory, and network bandwidth. It can be defined

as follows.

$$\text{Gain}(D,a) = \text{Ent}(D) - \sum_{v=1}^{V} \frac{|D^v|}{D} \text{Ent}\,(D^v) \tag{2}$$

Where $d \wedge V$ is the sample number of branch nodes and $(|d \wedge V|)\,/D$ is the weight of branch nodes. The greater the information gain, the greater the purity improvement obtained by using attribute A. therefore, the information gain can be used to distinguish the primary and secondary attributes of the spatial search tree to determine the parent node and child node in the tree.

4 EXPERIMENTAL RESULTS

4.1 Performance test

Set the server cluster using load balancing. The server configuration is as follows:

I. TEST SERVER CONFIGURATION DATA

Server list		
operating system	Memory size	CPU
linux	16	i5
windows 2003 service	16	i7
windows 10	16	i5
windows 11	16	i5
linux	16	i7
windows 2003 service	16	i7
windows 7	16	i7
windows 8	16	i5

The following is the CPU ratio of the server that simulates the transmission of 100000 passenger data in the system, compared with the server that starts the convolutional neural network to form the confrontation algorithm after using elliptic encryption and Tang poetry encryption.

It can be seen from the above figure that after the triple encryption is applied, the performance occupation of the server is not serious. Even if the convolutional neural network is started again on the basis of elliptic encryption and Tang poetry encryption, the CPU occupation ratio of the server can still be maintained at about 30%. So it has little impact on the performance of the server. Convolution neural network is adopted

According to the account number, password, input time, password length, input times, and other information obtained in time when logging in the system, words are obtained by the convolution neural network

Here ,E (w_i)is the left-right bidirectional representation C is obtained by textrcnn_ L (w_i) and C_ R (w_i) will indicate that x is obtained by splicing_ I = [c_l (w_i); E (w_i); c_r (w_i)], and then y is obtained by transformation_ i=tanh f_0([Wx]_i+b); For multiple y_ I to perform Max pooling to obtain the sentence representation y, forming the final classification.

4.2 Safety test

The DPA (Differential Power Analysis) script was used to simulate the attack on the system and obtain data, which was divided into four groups of experiments. The first group uses 3000

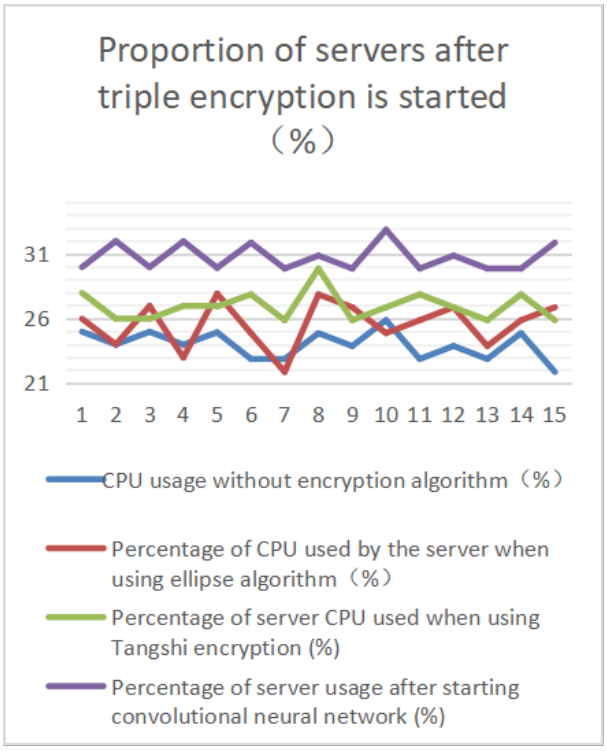

Figure 4: *encryption performance test*

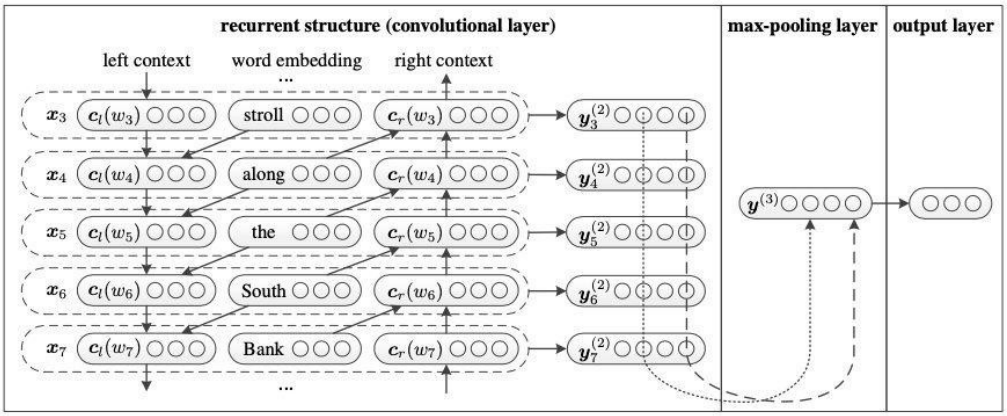

Figure 5: *convolutional neural network*

simulation scripts to attack unencrypted systems.On the premise of relying solely on the server firewall, 2987 times were successfully decoded. Relying solely on the server's own firewall, only 13 times of 3000 simulated attacks were successfully detected, and the proportion of data theft was as high as 99.57%

Group 2

In the same 3000 simulated script attacks, the elliptic encryption algorithm was simply used this time. 1756 were successfully decoded and 1244 failed, The proportion of data theft fell sharply, from 99.57 to 58.53%, but there are still 1244 failures The third group of experiments

On the basis of elliptic encryption, the data was encrypted for the second time in the whole Tang Dynasty, and 3000 script attacks were used again. 987 were successfully decoded and failed 2013 times. After the second encryption, the proportion of data theft fell again, but the data was still successfully obtained by 987 malicious users The fourth group of experiments

After the third group of experiments, the convolutional neural network is used for the third encryption. After malicious users break through the first two layers of encryption, machine learning is used to form a confrontation algorithm In this experiment, of the 3000 script attacks, only 281 were successfully obtained and 2719 failed. Under triple encryption, the proportion of data theft has decreased to less than 10%

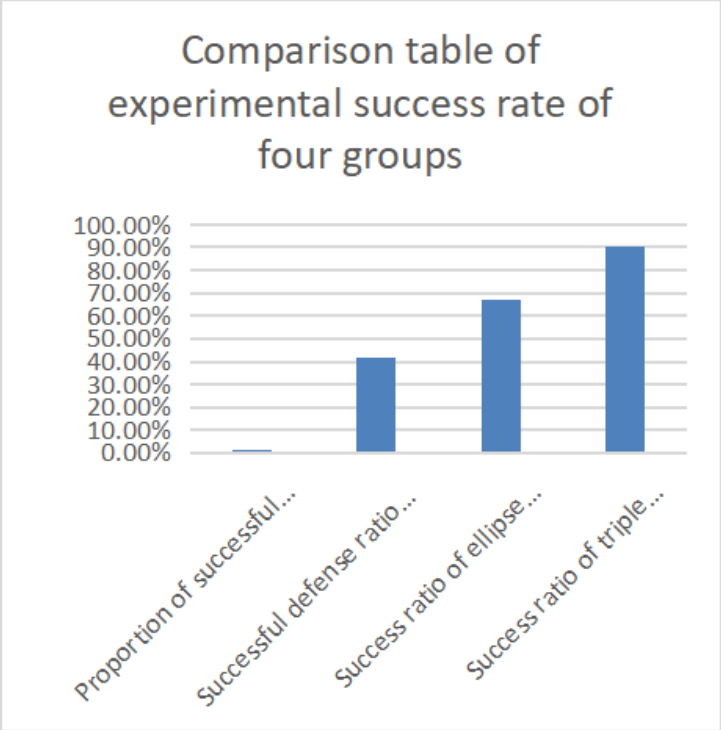

Figure 6: *Result comparison diagram*

5 SUMMARY

In the information security more and more attention now, this paper on the basis of the predecessors, put forward a new encryption method, and will be applied to the tourist information security in the tourism industry, improve the passenger data security, both for the tourists and tourism resources providers, have a huge practical value.

After using the encryption algorithm proposed in this paper, passengers do not need to worry about their information leakage. In the future, we hope to further improve the encryption algorithm, improve the security of passenger information, and can be used in more fields.

REFERENCES

[1] Miao F., Yang W., Xie Y., Fan W. and Wang J. (2018). The study of ownership-based data security application. In Proceedings of the 7th International Conference on Advanced Technologies (ICAT'18), 2018, 393-399. E-ISBN: 978-605-68537-1-5. Antalya, Turkey.

[2] Jianying L., Hongtao L and Bo W. (2021). Research on data encryption mechanism based on elliptic curve in cloud environment. Journal of Shanxi Normal University (NATURAL SCIENCE EDITION), 35 (02): 6-12 DOI:10.16207/j.cnki. 1009-4490.2021. 02.002.

[3] Wei X. and Rong W. (2021). Internet of things authentication scheme based on message queue telemetry transmission and elliptic curve encryption. Journal of Xiamen University (NATURAL SCIENCE EDITION),60 (06): 1024-1031

[4] Yiyu Z., Haijun Z., Chunlin H and Yihong C. (2021). Research on RFID electronic tag encryption algorithm based on elliptic curve [J] Journal of Yunnan University (NATURAL SCIENCE EDITION),43 (01): 60-67

[5] 刘彦辰,王箭,屈琪锋.混合加密的宋词载体文本信息隐藏技术[J].计算机技术与发展, 2018,28(01):138–143.

[6] 刘彦辰.(2017).宋词载体的文本信息隐藏技术[D].南京航空航天大学.

[7] 王升超.(2022).基于卷积神经网络的MCMC反演研究[D].吉. DOI:10.27162/d.cnki.gjlin.2022.007636.

[8] 徐俊辉.基于卷积神经网络的issue分类研究[D].(2022).南京邮电大学, 2022.DOI:10.27251/d.cnki.gnjdc.2022.001614.

[9] 孟萍. 软件定义网络中的负载均衡路由算法研究[D].(2022).南京邮电大学,2022.DOI:10.27251/d.cnki.gnjdc.2022.001266.