Journal of Cyber Security
DOI:10.32604/jcs.2020.010548
Article

Tech Science Press

Data Security Defense and Algorithm for Edge Computing Based on Mean Field Game

Chengshan Qian[1,2], Xue Li[1,*], Ning Sun[2] and Yuqing Tian[1]

[1]School of Automation, Nanjing University of Information Science & Technology, Nanjing, 210044, China
[2]Binjiang College, Nanjing University of Information Science & Technology, Wuxi, 214105, China
[*]Corresponding Author: Xue Li. Email: xueli1009@qq.com

Received: 09 March 2020; Accepted: 28 June 2020

Abstract: With the development of the Internet of Things, the edge devices are increasing. Cyber security issues in edge computing have also emerged and caused great concern. We propose a defense strategy based on Mean field game to solve the security issues of edge user data during edge computing. Firstly, an individual cost function is formulated to build an edge user data security defense model. Secondly, we research the ε-Nash equilibrium of the individual cost function with finite players and prove the existence of the optimal defense strategy. Finally, by analyzing the stability of edge user data loss, it proves that the proposed defense strategy is effective.

Keywords: Edge computing; mean field game; cyber security

1 Introduction

With the rapid development of mobile smart terminals such as mobile internet and smart phones, edge users frequently use smart terminals for transactions, such as shared services, mobile payments, etc. [1]. In this transaction process, the attacker can steal the edge user's private information by attacking the terminal device or analyzing the data. For example, according to the face recognition or fingerprint recognition system of mobile payment, personal facial features and fingerprint information are inferred, which will bring serious consequences to users. In addition, the edge users unload part of the computing tasks to the terminal devices, which is also one of the major factors that the data of the edge users is easy to leak [2–4].

In addition, in the edge computing mode [5–6], edge users, edge network devices and edge data center can interact anytime and anywhere. Edge terminal devices usually store and share many personal data. In the process of data transmission and storage, its integrity and confidentiality may be damaged. Due to the limitation of terminal device resources, some traditional cryptography algorithms are no longer applicable to edge computing environment. Therefore, how to ensure the security of edge user data in the edge computing environment has become one of the issues of edge computing defense [7]. The following is an architecture for edge computing.

The traditional defense strategies are based on the cyber security algorithm, or some research work based on game theory mainly analyze the optimal defense strategy from the static point of view. Because the interaction between the edge users is random and dynamic, and the attacker's strategy is also random. Based on this, the innovation of this paper is as follows:

1) We proposed an edge user data security defense model based on Mean field game.

2) We proposed a dynamic and efficient data security defense algorithm.

The organization structure of this paper is as follows: the related issues are discussed in detail in the second section. In the third section introduces the data security defense model. In the fourth section analysis the optimality condition. The fifth section present the performance evaluation result to demonstrate the effectiveness of the proposed model and algorithm. Finally, conclusion and future work are presented in the sixth section.

2 Related Work

In the model of edge computing, the application of edge computing in different fields leads to the diversification and complexity of edge data. Edge users are more and more frequently using mobile applications to achieve mobile payment, shared services, etc. Due to the lack of centralized management of distributed devices, the edge user's information is easy to become the target of malicious attackers [8]. At present, most of the research on data security mechanism mainly depends on specific information security algorithm. For example, anonymity, access control and packet encryption [9–10].

In 2016, Bhardwaj et al. proposed a symmetric algorithm for cloud-based applications and services that require data and link encryption. For security reasons, they focus on symmetric and asymmetric algorithms, where symmetric algorithms are applied to cloud-based applications and services that require data and link encryption [11]. Then, in order to support the effective verification of dynamic data, Ge et al. [12] have designed a new type of cumulative authentication tag (AAT) based on symmetric keys. Verifiable and searchable symmetric encryption is an important cloud security technology that allows users to use keywords from the cloud retrieve encrypted data and verify the validity of the returned results.

In addition, edge users bring risks to their personal sensitive data while using applications to realize online services. For example, attackers can obtain their location information according to the address they visit and online transactions. Alese [13] and others proposed a game theory to design a location privacy system, which aims to analyze the user's mobile behavior in the network, so that the user can maximize their location privacy while minimizing overhead.

Nevertheless, in the above paper mainly studies the data security of edge users from the perspective of traditional information security algorithm. Because the user's behavior also affects the establishment of its defense mode, Squicciarini et al. [14] collects common behavioral data among users and analyzes user's attitudes towards disclosure of sensitive information. They establish a static game model of users' real information sharing and false information disclosure. Through the derivation of ε -Nash equilibrium of the model, the attitude of users to their personal data publishing and hiding is studied. From this point of view, using game theory to study the data security of edge users can motivate users to protect their personal sensitive data.

3 Data Security Defense Model

3.1 Formulation Establishment

3.1.1 The Mean Field Game

Mean field game theory [15–17] is one of the most practical branches of game theory and has been used to research a class of complex problems with large number of players. Mean field game model is established by considering various assumptions, for example, players are homogeneous, and their behaviors are continuous in time, and the decision-making of each player depends on the mean field term. The homogeneity means that the subtle change among players can be negligible if the number of players is sufficiently large. The continuity leads to an approximation of the game model with many players, and the third assumption indicates that the process of decision-making of each player is affected by others through the mean field term.

3.1.2 Problem Description

In the edge computing mode, real-time processing of data is realized, but the privacy data of edge users is also easy to leak. In addition, for users, frequent use of third-party mobile applications for online payments increases the probability that their data will be attacked. For the security issues faced by edge user data. In this section, the edge user exposes a part of their personal data. Combined with the Mean field game theory, the edge user data loss problem and its defense strategy selection are modeled and analyzed.

3.1.3 Problem Formulation

Let N be the number of edge users in the edge computing environment. We use $p_i(t)$ to denote the data leakage probability of edge users. i at time t for $i=1,2,...,N$. We assume the data leakage probability $p_i(t)$ of edge users i at time t is independent of each other. Combined with the idea of information entropy, at game time t, the average loss of edge user personal data can be expressed by $x_i(p_i)=\left(p_i(0)\log p_i(0)+\sum_{i=1}^{T-1} p_i(t)\log p_i(t)\right)$, where $p_i(0)>0$.

This means that the more data leakage probability $p_i(t)$, the more average loss of personal data, the reverse is also true.

Considering that edge users take different degree of defense measures, we use $u_i(t)$ to denote the defensive strength of the defensive measures at t time, and $v(t)$ is regard as the attack frequency of attackers. For the individual edge users, the process of their personal data loss is related to their defense intensity and attack frequency of attackers.

Thus, the data loss process of edge users is expressed as

$$\begin{cases} \dfrac{dx_i(p_i)}{dt}=ax_i(p_i)+bu_i(t)+cv(t) \\ x_i(p_i(0))=x_{i0} \end{cases} \tag{1}$$

where x_{i0} is the data loss of edge user i at the beginning of game, a is the influence factor of the amount of data lost which is allowed disclosed by users, b is the probability of successful detection and blocking of attackers, and c is the probability of successful attack.

In the game process, it is assumed that edge users can disclose part of their personal data. When the probability of data leakage $p_i(t)$ is close to zero, let $F_{i1}(x_i)$ be the number of user's cost function of data loss. When user i is under the attack of eavesdropping, the cost function of data loss is expressed as $F_{i2}(x_i)$. Thus, the change rate of user cost function $F_i^{'}(x_i)$ is a monotone function about the amount of data loss and subject to $F_{i1}^{'}(x_i)\neq F_{i2}^{'}(x_i)$. This shows that the change rate of user cost function $F_i^{'}(x_i)$ is not a constant C_0, that is $F_i^{'}(x_i)\neq C_0$. So, let's assume that the cost function of edge users caused by their data loss is

$$F_i(x_i)=\alpha_i x_i^q \tag{2}$$

where $q>1$,and α_i is the unit cost of i user.

For edge users, the cost of computing resources consumed by responding to defense measures can be expressed by a function of defense intensity $F_i(u_i(t))$. Inspired by the relationship between network node resource consumption and security patches in [2], it is written as $F_i(u_i(t))=\beta_i u_i(t)(1-u_i(t))$, where β_i is the unit cost of calculating resources consumption.

For attackers, it aims to get more user data by maximizing their attack frequency. Due to the limited computing resources of terminal device, the increase of attack frequency will easily lead to edge network congestion, which will affect the normal communication of edge users. Thus, we define $F(v(t))=\sigma v(t)(1-v(t))$ as the cost function of attacker caused by attack frequency, where σ is the influence factor of attack frequency on normal communication of edge users.

According to the Mean field game [11], we assume $f_N(t,x)=\frac{1}{N}\sum_{i=1}^{N}x_i$ is the Mean field terms in order to describe the overall data loss changes of edge users. Because edge users usually share and store many interactive data packets in the process of information interaction, when encountering attacks, one user doesn't deploy defense measures, which may lead to the leakage of other users' data or affect the choice of other users' defense strategies. Based on this, the penalty function for edge users who do not respond to defense measures is written as

$$F(G(f_N(t,x),v(t)))=\chi_i G(f_N(t,x),v(t)) \tag{3}$$

where $G(f_N(t,x),v(t))=G(f_N(t,x))u_i(t)=\frac{f_N(t,x)}{b}\left(\frac{df_N(t,x)}{dt}-af_N(t,x)-cv(t)\right)$ and χ_{i} the unit penalty cost to users.

Above all, for an individual edge user, based on the attack frequency of the attacker, the total cost function of the edge user in time $[0,T]$ is expressed as

$$\begin{aligned}&J_i(x_i,u_i(t),v(t))\\&=\int_0^T\alpha_i x_i^q+\beta_i u_i(t)(1-u_i(t))+\chi G(f_N(t,x),v)+\sigma v(t)(1-v(t))+h(x_i(p(T)))\end{aligned} \tag{4}$$

where $h(x_i(p(T)))$ is the cost of data loss of marginal users at the end of game.

3.2 A Solution to ε -Nash Equilibrium

3.2.1 Problem Description

For marginal users, when deploying defensive measures, they must consider their limited energy, computing and storage resources, and need to consider allowing some personal sensitive data to be publicly braked for convenient services. In view of the analysis of the edge user data security problem in the previous section, this section will use the first order Mean field game to analyze the equilibrium solution of the above problem.

3.2.2 ε -Nash Equilibrium

In addition, based on the analysis in the previous section, when edge user data tends to infinity, that is, $N\to+\infty$, individual differences between terminal devices are ignored. This means that different users choose their state-dependent defense strategy, meanwhile, there exists $\alpha_i\to\alpha,\beta_i\to\beta,\chi_i\to\chi$. Thus, if $N\to+\infty$, we define $f_{1t}=\int_{R^+}xf_N(t,x)dx$, then the edge user's state change Eq. (1) is transformed into

$$\frac{df_{1t}}{dt}=af_{1t}+bu^*(t)+cv^*(t) \tag{5}$$

where $u^*(t)$ is the user's optimal defense strategy and $v^*(t)$ is the attacker's optimal attack strength.

Firstly, the relevant assumptions and equilibrium definitions are given. Combined with the Mean field game theory, the equilibrium solutions of the first order mean field game theory are analyzed.

Besides, if $N\to+\infty$, the initial value of edge user data loss $f_0(x)$ is an absolute continuous function, that is, for $\forall\varepsilon_0>0$, there is a $\delta>0$ such that holds $x_i-x_j<\delta(i\neq j)$, and we have $\left|f_0(x_i)-f_0(x_j)\right|<\varepsilon_0$, where the final value function $h(x(T))\in C^\infty$ is bounded and satisfies the Lipschitz continuous.

Definition 1. For $\forall t\in[0,T]$, if $N\to+\infty$, the attack frequency is bounded with v^*, there exists $\varepsilon\geq 0$ such that the following inequality holds

$$J(x,u^*,v^*)-\varepsilon \le J(x,u,v^*) \tag{6}$$

where $u^*(t)$ is the user's optimal defense strategy.

The inequality in Eq. (5) holds for a finite number of participants, the ε-Nash equilibrium of the Mean filed game will degenerate into the general ε-Nash equilibrium as the number of player tends to infinity and ε tends to zero. Each player in our model is assumed to be rational, and the process of decision-making of each node depends on the Mean field term.

3.2.3 The First Order Mean Field Game

Lemma 1. For $\forall t \in [0,T]$, if $N \to +\infty$, there exists a continuously differentiable function $\varphi_t(x)$, where first order differential bounded. Such that the following equation set holds

$$\begin{cases} \partial_t \varphi_t(x) + \dfrac{c^2\beta+\sigma b^2}{4\beta\sigma}(\partial_x \varphi_t)^2 + \left(ax + \dfrac{\beta(b+c)+b\chi f_{1t}}{2\beta} \right) \partial_x \varphi_t + \alpha x^q + \dfrac{1}{4}\left[\dfrac{1}{\beta}(\beta+\chi f_{1t})^2 + \sigma \right] = 0 \\ \partial_t f_{1t}(x) + \partial_x \left[f_{1t} \left(\alpha x + b\dfrac{\beta+\partial_x \varphi_t(x) b + \chi f_{1t}}{2\beta} + c\dfrac{\partial_x \varphi_t(x) c + \sigma}{2\sigma} \right) \right] = 0 \\ \varphi_T(x) = h(x(T)), f_1(x,0) = f_0(x) \in R \end{cases} \tag{7}$$

where the user's optimal defense strategy $u^*(x,t) = \dfrac{\beta+\partial_x \varphi_t(x) b + \chi f_{1t}}{2\beta}$.

Proof. For $\forall t \in [0,T]$, according to the Mean filed game, if there is a continuously differentiable function $\varphi(t,x)$ such that

$$\varphi(t,x) = \inf_{u(t)} \sup_{v(t)} J(x,u(t),v(t)) \tag{8}$$

and the following first-order *HJB* backward equation and *FPK* forward equation

$$\begin{cases} \partial_t \varphi_t(x) + H\left(x, \partial_x \varphi_t(x), f_{1t}\right) = 0 & (HJB) \\ \varphi_T(x) = h\left(x(T)\right) \\ \partial_t f_{1t}(x) + \partial_x \left(f_{1t} \partial_\lambda H_t \left(x, \partial_x \varphi_t(x), f_{1t}\right)\right) = 0 & (FPK) \\ f_1(x,0) = f_0(x) \in R \end{cases} \tag{9}$$

where $H\left(x, \partial_x \varphi_t(x), f_{1t}\right)$ is Hamiltonian function, λ is accompanying variable. Thus, $\varphi_t(x)$ is the minimum cost of the user when the attack reaches the optimal attack frequency.

Hence, to calculate Eq. (8), we assume $\lambda = \partial_x \varphi_t(x)$ and construct the following Hamiltonian function, it can be written as

$$\begin{aligned} & H\left(x, \partial_x \varphi_t(x), f_{1t}\right) \\ & = \inf_{u(t)} \sup_{v(t)} \left\{ \alpha x^q + \beta u(t)\left(1-u(t)\right) + \chi f_{1t} u(t) \right. \\ & \left. + \sigma v(t)\left(1-v(t)\right) + \partial_x \varphi_t(x)\left(\alpha x(t) + b u(t) + c v(t)\right) \right\} \end{aligned} \tag{10}$$

Next, for Eq. (10), find the first derivative of $u(t)$ and $v(t)$, and calculate the optimal defense strategy and the optimal attack strength, such that

$$u^*(x,t)=\frac{\beta+\partial_x\varphi_t(x)b+\chi f_{1t}}{2\beta} \tag{11}$$

$$v^*(x,t)=\frac{\partial_x\varphi_t(x)c+\sigma}{2\sigma} \tag{12}$$

based on the Eqs. (11) and (12), Eq. (10) indicates that

$$\begin{aligned} &H\left(x,\partial_x\varphi_t(x),f_{1t}\right)\\ &=\alpha x^q+\beta u^*(1-u^*)+\chi f_{1t}u^*+\sigma v^*(1-v^*)+\partial_x\varphi_t(ax+bu^*+cv^*)\\ &=\frac{c^2\beta+\sigma b^2}{4\beta\sigma}(\partial_x\varphi_t)^2+\left(ax+\frac{\beta(b+c)+b\chi f_{1t}}{2\beta}\right)\partial_x\varphi_t+\alpha x^q+\frac{1}{4}\left[\frac{1}{\beta}(\beta+\chi f_{1t})^2+\sigma\right] \end{aligned} \tag{13}$$

In addition, from Eqs. (13) and (9), we derive the HJB backward equation in formula (7). Combining the $u^*(x,t)$, $v^*(x,t)$ and the Eq. (9), we form the FPK forward equation. For the above first-order Mean field game model, the equations set (9) is formed by the coupling of HJB backward equation FPK forward equation, the equilibrium solution of the equation depends on the initial state of the user $f_{i0}(x)$ and the cost function $h\left(x\left(p(T)\right)\right)$ at time T.

According to the above analysis, when Hamiltonian function $H\in C^\infty$, and $\left|\frac{\partial H}{\partial x}\right|$ bounded, the equilibrium solution of the Mean field game system (9) exists. That is, if $N\to+\infty$, for $\forall t\in[0,T]$, there exists $\varepsilon>0$, the best defense strategy $u^*(x,t)=\frac{\beta+\partial_x\varphi_t(x)b+\chi f_{1t}}{2\beta}$ and the optimal attack frequency $v^*(x,t)=\frac{\partial_x\varphi_t(x)c+\sigma}{2\sigma}$ hold the inequality $J\left(x,u^*(t),v^*(t)\right)-\varepsilon\le J\left(x,u(t),v^*(t)\right)$. In fact, since the data loss x of edge users is considered to be bounded, and the $\partial_x\varphi_t$ is bounded. Thus, there exists constant $C_1>0$ such that the following inequality holds $\left|\frac{\partial H}{\partial x}\right|=2\alpha x+a\partial_x\varphi_t\le C_1(1+|\lambda|)$.

End of proof.

The N_t waypoints are evenly distributed to N_s task. Then we allocate s-th task to the k-th UAV. Before the UAV flyting form the i-th waypoint to j-th waypoint, we sort the waypoints to find the best order to find the best path to reduce the flying distance, then the UAV take off and flying by the waypoint sequence, finally arrive and land at the N_0.

4 The Optimality Conditions

In the edge computing environment, the edge users minimize their data loss through response defense mechanism. For the analysis of the equilibrium solution based on the Mean field game model in the previous section, this section takes the first order Mean field game model as an example to analyze how to minimize the data loss of the edge users.

In addition, in the Mean field game model, each edge user affects other users' decision-making choices through the Mean field term in the game process. In this process, the state variables of individual edge users are gradually approximate to the state variables of the whole edge users. On the contrary, when the data loss of the whole edge users is minimized, the data loss of individual edge users is also approximate to the optimal. The following Tab. 1 shows the edge user data security defense Algorithm based on the Mean field game in the edge computing environment.

Table 1: The edge user data security defense Algorithm

```
Data security of edge users based on the Mean field game
Input: Total number of edge users $N$ initial state $x_{10}, x_{20}, \cdots\cdots, x_{N0}$;
Output: Optimal strategy $u^*$ and $v^*$;
1. Setting parameters $\beta, \alpha, \sigma, \chi, a, b, c, s$;
2. For $t = 1$ to T:
3. According to formula $f_N(t,x) = \frac{1}{N}\sum_{i=1}^{N} x_i$ ,calculate $f_N$;
4. Based on formula (8), calculate $\varphi(t,x)$;
5. Combing (11) and (12), calculate the optimal strategy $u^*$ and $v^*$;
6. End for;
7. Return the optimal defense strategy and optimal state trajectory.
```

5 Performance Evaluation

5.1 Related Parameters

In this section, the edge user data security defense model and algorithm based on Mean field game are simulated and verified. Firstly, from the overall point of view of the edge users, by analyzing the optimal attack frequency $v^*(t)$, the change process of edge users' defense level $u^*(t)$, and then get the amount of data loss to edge users. The purpose of f_{1t} simulation is to reveal the process of data loss of edge users under the worst case attack intensity and the best defense strategy of edge users.

According to the above analysis, for large-scale edge users, the state variables of individual edge users are gradually approximate to the state variables of the whole edge users, thus, it can be replaced by $\varphi_i(x)$ approximation, we assume the function $\varphi_i(x) = sx^2$, where s is nonnegative real number. From (11) and (12), we drive the optimal defense strategy of edge users $u^*(t) = \frac{\beta + 2xsb + \chi f_{1t}(x)}{2\beta}$, the worst attack strength of the attacker $v^*(t) = \frac{2xsc + \sigma}{2\sigma}$, where $z = 2a - \sqrt{a^2 - \alpha \frac{b^2\sigma - c^2\beta}{\beta\sigma}} < 0$. Considering the number of marginal users participating in the game $N = 500$, Initial time of game $t_0 = 0$, end time $T = 100s$, Tab. 2 shows the simulation parameters.

Table 2: Setting of relevant parameters

α	β	χ	σ	a	b	c	s
0.96	0.5	0.11	0.38	0.46	0.7	0.88	0.5

5.2 The Trend of Attack Frequency

For the attacker, the target is to increase the attack intensity by increasing the attack frequency in unit time under the condition of fixed attack success rate, to steal more user data. However, the higher the attack intensity is, the greater the probability that the attacker will be detected. At the same time, with the change of time and the response of the edge user defense mechanism, the attack success rate will gradually decrease. Thus, attackers will choose to maximize their attack frequency in the initial stage of game time, the trend of attack frequency $v^*(t)$ with time is analyzed in Fig. 1 below. The attacker's attack frequency $v^*(t)$ decreases with time and maintains irregular changes near zero. This is because edge users can disclose part of their personal data, and without detection, attackers will still launch attacks of different frequencies.

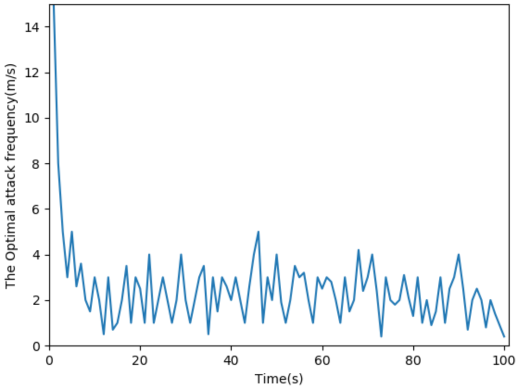

Figure 1: The trend of attack frequency $v^*(t)$

5.3 The Trend of The Optimal Defense Strategy

In case of malicious attack, the edge users prevent the attack through the response defense mechanism. Fig. 2 analyzes the trend of the defense strategy of edge users with respect to time. From the figure, we can see that in the first 10 seconds of the game time, the defense level of edge users is increasing. The higher the attack intensity is, the greater the probability of detection is. With the increase of attack frequency, the defense intensity increases. Then with the change of time, the defense intensity decreases gradually, and finally stabilizes near a non-negative value. This is because in the edge computing environment, edge users can disclose some sensitive personal data in order to obtain convenient services such as online payment. Therefore, even when no malicious attack is detected, edge users still take defensive measures against their data. For example, permission setting and so on, which also shows that edge users improve their awareness of personal data security protection.

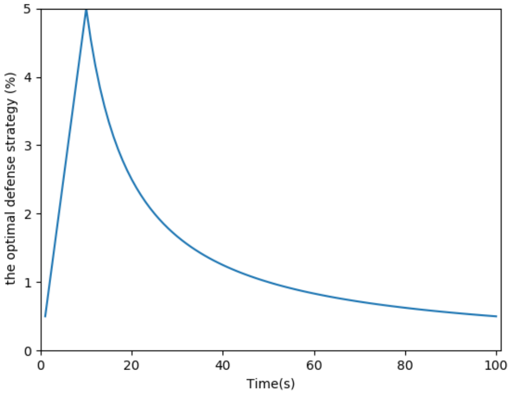

Figure 2: The trend of the optimal defense strategy $u^*(t)$

5.4 The Trend of Data Loss of Edge Users

In face of malicious attacks, edge users reduce their data loss through response defense mechanism. Because each edge user is coupled by the Mean field term, that is, each node affects the other node's policy choice by the Mean field term. At the same time, when the total amount of data loss of edge users is minimized, the individual edge users achieve the best amount of data loss based on their optimal defense strategy. Fig. 3 shows the trend of edge users' data loss. The data loss in the edge computing environment decreases monotonously with time, when time $t \geq 80s$, user data loss is stable at zero. This shows that in the initial stage of game time, under attack, the average loss of data of edge users increases gradually. With the response of nodes to their defense mechanism, although they may still be attacked, their data will not be leaked.

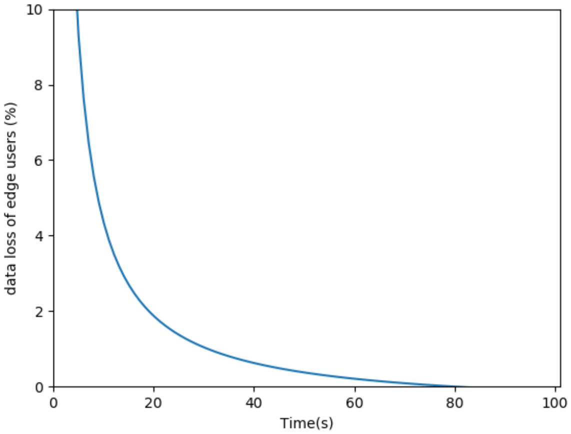

Figure 3: the trend of data loss of edge users f_{1t}

6 Conclusion and Future Work

This paper studies the data security defense of edge users and establishes a data security defense model for edge users based on the Mean field game. By analyzing the average loss of the edge user data, the existence of the equilibrium solution of the Mean field model is verified, and the optimal strategy is obtained. Simulation results show that when both the edge user and the attacker adopt the optimal strategy, the edge user can reduce data loss and minimize the consumption of computing resources.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] B. Chen, J. Wan, A. Celesti, D. Li, H. Abbas and Q. Zhang, "Edge computing in IoT-based manufacturing," *IEEE Communications Magazine*, vol. 56, no. 6, pp. 10–109, 2018.

[2] P. Hu, S. Dhelim, H. Ning and T. Qiu, "Survey on fog computing: architecture, key technologies, applications and open issues," *Journal of Network and Computer Applications*, vol. 98, pp. 27–42, 2017.

[3] J. Zhang, B. Chen, Y. Zhao, X. Cheng and F. Hu, "Data security and privacy-preserving in edge computing paradigm: Survey and open issues," *IEEE Access*, vol. 6, pp. 18209–18237, 2018.

[4] H. Zhang, H. Han, X. Lai, D. Lin, J. Ma and J. Li, "Survey on cyberspace security," *Science China Information Sciences*, vol. 58, no. 11, pp. 1–43, 2015.

[5] W. Shi, J. Cao, Q. Zhang, Y. Li and L. Xu, "Edge computing: vision and challenges," *IEEE Internet of Things Journal*, vol. 3, no. 5, pp. 637–646, 2016.

[6] B. Varghese, N. Wang, S. Barbhuiya, P. Kilpatrick and D. S. Nikolopoulos, "Challenges and opportunities in edge computing," *IEEE International Conference on Smart Cloud*, pp. 20–26, 2016.

[7] D. Chen and H Zhao, "Data security and privacy protection issues in cloud computing," *International Conference on Computer Science and Electronics Engineering*, vol. 1, pp. 647–651, 2012.

[8] R. Roman, J. Lopez and M. Mambo, “Mobile edge computing, fog et al.: a survey and analysis of security threats and challenges,” *Future Generation Computer Systems*, vol. 78, pp. 680–698, 2018.

[9] H. Cui, X. Yi and S. Nepal, “Achieving scalable access control over encrypted data for edge computing networks,” *IEEE Access*, vol. 6, pp. 30049–30059, 2018.

[10] M. Du, K. Wang, Y. Chen, X. Wang and Y. Sun, “Big data privacy preserving in multi-access edge computing for heterogeneous Internet of Things,” *IEEE Communications Magazine,* vol. 56, no. 8, pp. 62–67, 2018.

[11] A. Bhardwaj, G. V. B. Subrahmanyam, V. Avasthi and H. Sastry, “Security algorithms for cloud computing,” *Procedia Computer Science*, vol. 85, pp. 535–542, 2016.

[12] X. Ge, J. Yu, H. Zhang, C. Hu, Z. Li, Z. Qin *et al.*, “Towards achieving keyword search over dynamic encrypted cloud data with symmetric-key based verification,” *IEEE Transactions on Dependable and Secure Computing*, pp. 1, 2019.

[13] B. K. Alese, A. F. Thompson and P. Y. Oni, “A location privacy system in mobile network using game theory,” in *International Conference on Cyber Situational Awareness, Data Analytics and Assessment*, pp. 1–5, 2017.

[14] A. C. Squicciarini and C. Griffin, “An informed model of personal information release in social networking sites,” *International Conference on Social Computing*, pp. 636–645, 2012.

[15] Y. Wang, F. R. Yu, H. Tang and M. Huang, “A mean field game theoretic approach for security enhancements in mobile ad hoc networks,” *IEEE Transactions on Wireless Communications*, vol. 13, no. 3, pp. 1616–1627, 2014.

[16] M. Nourian and P. E. Caines, “ε -Nash mean field game theory for nonlinear stochastic dynamical systems with major and minor agents,” *SIAM Journal on Control and Optimization*, vol. 51, no. 4, pp. 3302–3331, 2012.

[17] R. Carmona and F. Delarue, “Probabilistic analysis of mean-field games,” *SIAM Journal on Control and Optimization*, vol. 51, no. 4, pp. 2705–2734, 2013.

[18] J. Barreiro-Gomez, T. E. Duncan and H. Tembine, “Linear-quadratic mean-field-type games with multiple input constraints,” *IEEE Control Systems Letters*, vol. 3, no. 3, pp. 511-516, 2019.

[19] M. H. R. Khouzani, S. Sarkar and E. Altman, “Optimal dissemination of security patches in mobile wireless networks,” *IEEE Transactions on Information Theory,* vol. 58, no. 7, pp. 4714–4732, 2012.