scientific reports

Check for updates

OPEN

Construction of evolutionary stability and signal game model for privacy protection in the internet of things

Yu Li[1], Huamin Liu[2]✉ & Lei Lu[3]

The research focuses on privacy protection in the Internet of Things environment. A model based on evolutionary theory game and signal game mechanism is proposed to analyze and optimize privacy protection strategies. The study introduces evolutionary game theory and signal game mechanism to construct a game model between users, devices, network operators, and attackers. Detailed discussions are conducted on factors such as privacy protection needs, information asymmetry, and privacy leakage risks. The proposed Multi-stage Signal Game and Deep Learning Model for IoT Privacy Protection (IoT-PSGDL) performed the best on privacy protection effectiveness, at 98.25% on the CIC IoT dataset, with a policy update speed of 7.42 updates/second and a system response time of 35.12ms. Compared with other models, the proposed model performed well in multiple metrics, such as privacy protection persistence (97.56%), communication latency (54.12ms), and data storage security (96.75%). In addition, privacy protection strategies such as data encryption performed the best in the experiment, with a privacy protection success rate of 96.72% and the lowest privacy leakage probability of only 2.14%. The significance of the research lies in providing an efficient and dynamically optimized privacy protection strategy that can effectively respond to various privacy threats in complex Internet of Things environments.

Keywords Internet of things privacy protection, Evolutionary game model, Signal game mechanism, Deep learning algorithm, Privacy protection strategy

With the rapid development of Internet of Things (IoT) technology, smart devices make people's lives more convenient. However, this also brings a significant challenge to privacy protection[1]. IoT systems typically involve multiple stakeholders, such as users, devices, network operators, and attackers, among whom there are complex interactive relationships. Privacy protection has become a critical issue that urgently needs to be addressed[2]. IoT devices typically collect rich personal data and transmit it over the network. The data security and privacy protection during transmission are being addressed[3]. Once data is maliciously obtained or tampered with, user privacy and system security will face serious threats. Traditional research on privacy protection in the IoT mainly focuses on the single strategy, such as data encryption, anonymization, and access control[4]. These methods can improve privacy protection. However, due to complex and diverse IoT environments, they often cannot comprehensively solve the privacy leakage. Traditional research typically focuses on static privacy protection schemes, lacking dynamic adaptation and response mechanisms against attacker behavior. In addition, participants in IoT systems often have asymmetric information, and there are differences in data usage and privacy protection needs among users, devices, and network operators. This also makes it difficult for existing privacy protection models to achieve optimal results in practical applications[5]. Although existing research provides multiple privacy protection methods, optimizing privacy protection strategies based on constantly changing attacker behavior and user needs in dynamic environments remains an urgent problem[6,7].

In the field of IoT privacy protection, scholars have conducted in-depth research on data analysis, privacy protection framework construction, and technical solution design. Shahid J et al. analyzed the privacy challenges of healthcare IoT devices in sensitive information processing. They classified the components, analyzed device functionality and deployment, and explored the potential characteristics and causes of data breaches. A suitable regulatory framework to address compliance issues should be established. The research proposed suggestions

[1]Public Basics Department, Ganzhou Polytechnic, Ganzhou 341000, China. [2]Information Engineering College, Ganzhou Polytechnic, Ganzhou 341000, China. [3]Information Engineering College, Jiangxi College of Applied Technology, Ganzhou 341000, China. ✉email: liu13767715@163.com

to enhance security and privacy[8]. In terms of technical solutions, Zubaydi H D et al. integrated blockchain technology and the IoT. The basic principles, architecture, protocols, and consensus algorithms of blockchain technology and IoT were reviewed, and the challenges were summarized, including storage capacity, resource utilization, transaction speed, and legal issues. The application effects in privacy and security were explored[9]. Wang R et al. proposed a federated learning privacy protection scheme based on edge computing. Through lightweight privacy protection protocol and security algorithm design, it effectively solved the privacy disclosure and computing capacity limitation in the medical field of the IoT[10]. To securely transmit medical data, Yu F et al. proposed an encryption scheme based on the Memristive Hopfield Neural Network (MHNN). By constructing a new complex dynamic model and combining it with hardware implementation, it ensured the shared security of medical data[11]. Ali A et al. focused on the privacy protection of critical health data in IoT medical applications. A method that combined homomorphic encryption and blockchain technology was proposed. The homomorphic encryption was used to perform operations on encrypted data, and blockchain smart contracts were used to control access, set policies, and generate audit records. This method could protect data privacy while achieving efficient data processing and analysis[12].

Alzubi J A et al. focud on the privacy and security of medical and health data in industrial cloud computing and the IoT. The method took Convolutional Neural Network (CNN) to classify data sets and distinguished normal and abnormal users. The second was to combine blockchain and cryptography federated learning modules to process and remove abnormal user data while ensuring access rights to health records. Python simulation experiments showed that the model outperformed other existing technologies on classification performance and overall performance[13]. Alzubi O A et al. proposed a BAISMDT model that integrated blockchain and artificial intelligence to address the security of medical data transmission in the IoT environment. The model took signcryption technology to ensure the reliability and privacy of data transmission, and built a trusted transmission environment between data providers through blockchain. Experimental verification showed that the model achieved 97.54% and 98.13% accuracy on cardiac statistics logs and white blood cell datasets, respectively, significantly improving the security and diagnostic accuracy of medical data transmission in the IoT[14]. Alzubi J A et al. focused on the security and privacy of user data in the mobile edge computing environment. Aiming at its resource-constrained characteristics, a blockchain-driven security management framework was proposed. The framework introduced the characteristics of blockchain such as immutability, transparency and distributed ledger to build an access sharing mechanism driven by smart contracts. Theoretical analysis and simulation experiments verified that the framework reduced operating costs while ensuring high security, low latency, and high throughput. It is suitable for MEC devices with limited resources and effectively improves data security and access efficiency in MEC environments[15]. Thomas C K et al. focused on the application of Semantic Communication (SC) in privacy protection in the IoT. The study proposed an emerging SC framework that efficiently transmitted language through signal game design and combined neural symbolic artificial intelligence methods for causal inference. This framework utilized the Nash equilibrium strategy of signal game mechanism to optimize data transmission efficiency, while enhancing semantic reliability through generative stream networks[16]. Angelini F et al. further explored the privacy protection framework based on signal game mechanism. The Bayesian equilibrium problem in multi-stage dynamic games was analyzed, and an effective privacy protection model was proposed[17].

To sum up, many experts have explored different technologies and frameworks in the privacy protection, especially the data privacy of IoT devices, the integration of blockchain technology and IoT, and the application of edge computing and federated learning. However, there are still some shortcomings in current research, such as the lack of privacy protection mechanisms for large-scale IoT environments, the adaptability of various technological solutions, and how to balance the conflict between privacy protection and efficiency. Therefore, a more intelligent and dynamically optimized privacy protection model that combines evolutionary game theory and deep learning techniques is proposed to address efficiency, compatibility, and security in IoT privacy protection. The research innovatively integrates evolutionary game theory and signal game mechanism to address these challenges. Evolutionary game theory models the dynamic strategy evolution of multiple stakeholders - users, devices, operators, and attackers. The dynamic strategy evolution under information asymmetry captures how privacy protection policies adapt over time through mechanisms such as replication dynamics and Fermi update, in order to overcome the lack of dynamic adaptation in traditional static schemes. Meanwhile, the signal game mechanism focuses on real-time strategic interaction through signal transmission. Senders such as IoT devices convey privacy protection intentions through signals such as encryption levels or access control logs, while receivers like users or defenders adjust defenses based on these signals to counteract attackers' real-time strategy adjustments driven by Q-learning.

The two mechanisms are fused in a hierarchical framework, and evolutionary game theory shapes the macro-level strategy distribution through iterative interactions, determining equilibrium strategies such as device encryption adoption. Concurrently, the signal game mechanism drives micro-level adjustments through signal-reaction loops, such as attack interceptions based on encryption signals, and accelerates evolutionary optimization. The bidirectional Long Short-Term Memory (LSTM) combined with CNN (CNN-LSTM) updates the game payoff matrix by processing time privacy signals, combining data-driven insights with game theory to bridge the two layers. This allows for a balance between long-term evolutionary stability and real-time adversarial response.

The core contributions of this study are threefold: (1) A novel two-layer framework is proposed, which combines evolutionary game theory with signal game mechanisms to form strategy distributions through iterative interactions of evolutionary games at the macro level, ensuring long-term evolutionary stability; Real time strategy adjustment is achieved at the micro level by utilizing the signal response cycle of the signal game mechanism. (2) Introducing a bidirectional LSTM-CNN model to process temporal privacy signals, updating the game payoff matrix, and achieving effective connection of a dual layer mechanism, balancing long-term

stability and real-time response capability. (3) By combining Q-learning and deep learning methods, the real-time adjustment of attacker strategies is optimized through Q-learning. Deep learning algorithms such as LSTM and CNN are used to automatically extract privacy signal features and adaptively update privacy protection policies, thereby improving the efficiency and accuracy of policy optimization in dynamic environments.

Methods and materials

Evolutionary game model for privacy protection in the iot

In the evolutionary game model, information asymmetry is one of the core assumptions. Participants such as users, devices, network operators, and attackers may have different understandings of the system, which could lead to attackers exploiting privacy violations. The model models a dynamic IoT threat landscape where attackers exploit information asymmetry and system vulnerabilities to breach privacy protections. Attackers possess adaptive capabilities, using Q-learning to adjust strategies such as vulnerability exploitation or data interception in real time based on observed privacy signals from devices/users, as modeled in the signal game's receiver strategy. Although attackers are familiar with common privacy mechanisms (encryption, anonymization), their knowledge is partial, lacking full visibility into real-time defense updates and evolving with historical attack results (success/failure rewards in Q-learning), as reflected in metrics such as "privacy leakage probability". Their core objective is to maximize exploitation efficiency by minimizing attack costs while increasing leakage likelihood and disrupting defender resource balance, which is consistent with the model's focus on evolutionary stability and signal driven interaction. Meanwhile, there are differences in privacy protection needs among different users and devices[18]. Users choose strategies based on their own sensitivity, while the goals of devices and operators may conflict with those of users, requiring a balance between privacy protection and other interests in the game. Moreover, there is a dynamically changing risk of privacy leakage in the IoT environment, and attackers may exploit system vulnerabilities or information asymmetry for network intrusion or malicious attacks, further exacerbating the complexity of privacy protection[19,20]. The evolutionary game model for privacy protection in the IoT is shown in Fig. 1.

In Fig. 1, in the game model for privacy protection in the IoT, evolutionary game theory provides a framework for analyzing the stability of cooperative behavior, where complex networks are the organizational foundation and main venue of evolutionary games, and have decisive impacts on the outcome. The evolutionary game includes game models and strategy evolution rules. Game models such as prisoner's dilemma and snowball game provide a theoretical basis for evolutionary game theory and reflect individuals' strategy choices under different social dilemmas. The evolution rule is an important research point in evolutionary games, which characterizes the way individuals choose strategies in social environments, including neighbor selection rules and strategy update rules, such as replication dynamics, Fermi dynamics, and expected evolution rules for updating strategies.

In Fig. 2, the first step is to analyze the current situation and establish a network model, which is the basic step for clearly defining the research scope and object. Next, nodes in the network obtain game benefits based on the game model, and use this method to measure the gains and losses of different strategies. Then, the node selects learning nodes based on neighbor selection rules and draw on beneficial strategies from surrounding nodes. Finally, nodes update their own strategies based on policy update rules, continuously optimizing to better adapt to the complex environment of IoT privacy protection. In the model context, "policy update" refers to stakeholders and attackers dynamically adjusting privacy protection policies based on real-time environmental feedback, benefit evaluation, and learning algorithms. This process involves modifying strategies such as data encryption levels, access control rules, anonymization techniques, or attack tactics to optimize outcomes in response to changing risks and interactions. As a critical indicator, policy update speed directly reflects the model's adaptability to dynamic threats and its capability to maintain optimal privacy protection performance over time, with the key mechanisms including rules based on evolutionary game theory and adjustments based on reinforcement learning, where strategies are iteratively improved to maximize long-term returns. Q-learning,

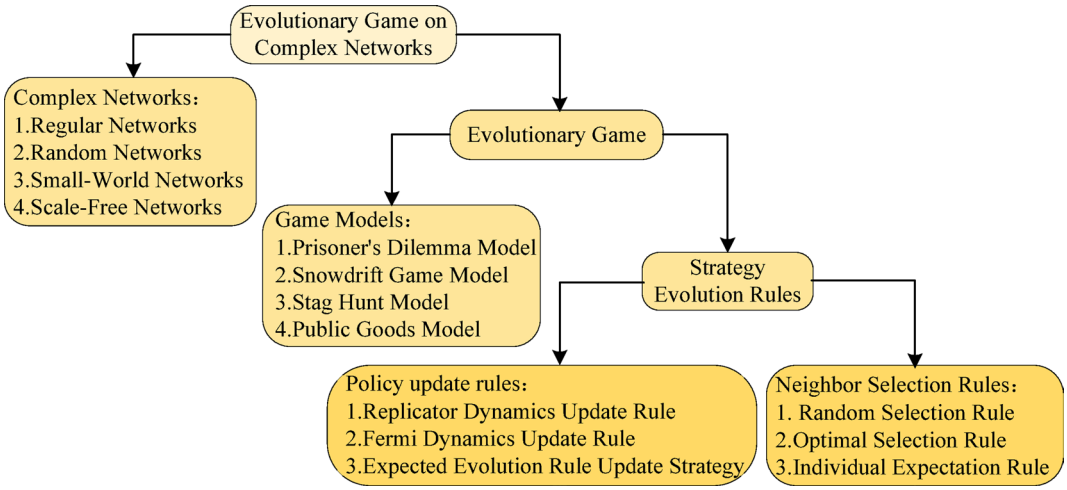


Fig. 1. Evolutionary game model for IoT privacy protection.

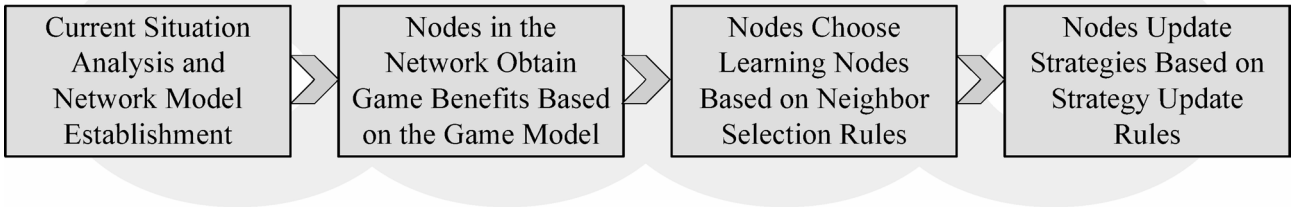


Fig. 2. Steps for updating privacy protection node strategies in the IoT based on game theory.

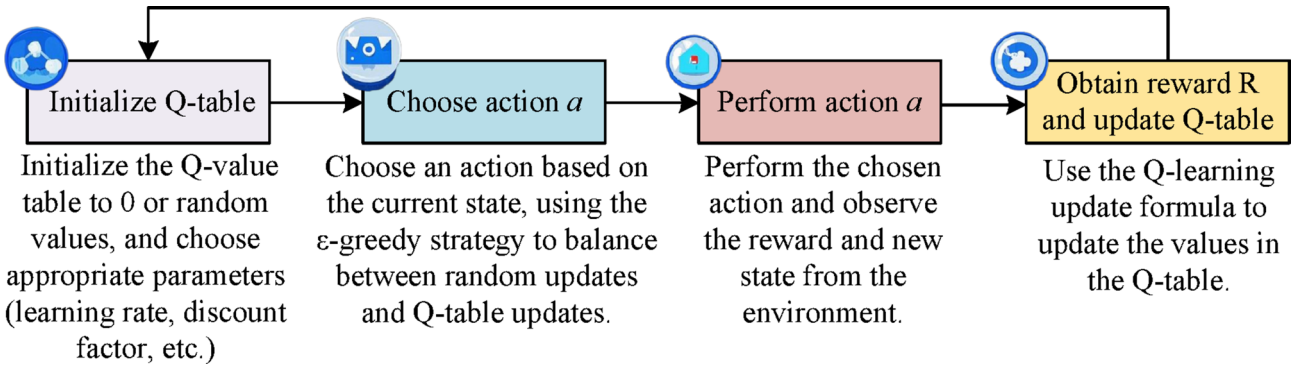


Fig. 3. Q-learning algorithm execution process in IoT privacy protection.

as a reinforcement learning method, can adjust strategies through feedback on the environment during the learning process, thereby achieving optimal strategies through various interactions. This method is particularly suitable for multi-stage game models, where participants (such as users, devices, network operators, and attackers) update their privacy protection strategies through continuous interaction. Q-learning integrates into the game-theoretic framework by modeling interactions among stakeholders (users, devices, attackers, and defenders) through a shared state-action space. Users/devices select privacy strategies (e.g., encryption, anonymization) based on real-time conditions (data sensitivity and resources), while attackers choose tactics from detected signals (e.g., encryption levels) and defenders adjust defenses using combined signals. The Q-value update rule (Eq. 1) balances immediate rewards (e.g., successful protection/attack interception) and future rewards through learning rate (α) and discount factor (γ), driving iterative strategy refinement to maximize long-term payoffs and embedding dynamic learning into static game structures.

Q-learning optimizes privacy strategies through the ε-greedy policy, balancing exploration (randomly testing new strategies, e.g., novel encryption) and exploitation (relying on high-Q proven tactics, e.g., established anonymization). This prevents suboptimal convergence, especially against evolving attacks. Users/devices might temporarily switch to untested defenses when ε triggers exploration, while attackers refine tactics and defenders adjust responses based on Q-value updates. According to this cycle, Q-learning continuously enhances its strategy adaptability to users/devices and defense effectiveness against dynamic threats. The Q-learning algorithm execution process in IoT privacy protection is shown in Fig. 3.

When building a game model for privacy protection in the IoT, Q-learning first initializes the Q-value table, which can be set to 0 or a random value, and selects appropriate parameters such as learning rate, discount factor, etc., laying the foundation for subsequent learning. Next, based on the current state, an action is selected using the ε-greedy strategy to balance random exploration with utilization based on the Q-value table. The selected action is executed, the rewards obtained from the environment and the new state entered are observed. Finally, based on the Q-learning update equation, the Q-value table is updated, and this process is continuously iterated to continuously optimize its strategy in the game scenario of IoT privacy protection[21]–[22]. In the game model, Q-learning can help participants respond to attackers' different strategies by continuously learning and adjusting their strategies, thereby optimizing the privacy protection effect. The process is shown in Eq. (1).

$$Q(s_t, a_t) \leftarrow Q(s_t, a_t) + \alpha \left(r_t + \gamma \max_{a'} Q(s_{t+1}, a') - Q(s_t, a_t)\right) \tag{1}$$

In Eq. (1), $Q(s_t, a_t)$ signifies the Q-value for taking action a_t in state s_t. α signifies the learning rate. r_t signifies the reward obtained after taking action a_t in state s_t. γ signifies the discount factor, indicating the attenuation of future rewards. $\max_{a'} Q(s_{t+1}, a')$ signifies the maximum Q-value of all possible actions in the next state s_{t+1}. Users may choose different privacy protection measures based on their privacy protection needs and device resource limitations, such as enabling encryption, data anonymization, or limiting data sharing. Devices can also

choose corresponding privacy protection strategies based on current environmental changes such as bandwidth, battery level, etc[23]. In Q-learning, the strategy selection of users and devices can be optimized through the following Q-value update equation, as shown in Eq. (2).

$$\begin{cases} Q_u(s_t, a_t) \leftarrow Q_u(s_t, a_t) + \alpha_u \left(r_t + \gamma_u \max_{a'} Q_u(s_{t+1}, a') - Q_u(s_t, a_t)\right) \\ Q_d(s_t, a_t) \leftarrow Q_d(s_t, a_t) + \alpha_d \left(r_t + \gamma_d \max_{a'} Q_d(s_{t+1}, a') - Q_d(s_t, a_t)\right) \end{cases} \tag{2}$$

In Eq. (2), γ_u and γ_d are discount factors used for the attenuation of rewards for users and devices, respectively. r_t is a privacy protection reward that can be evaluated based on the privacy protection. The attacker is to identify potential vulnerabilities and carry out attacks by recognizing privacy protection signals of users and devices. The attacker's strategy selection can be optimized through Q-learning algorithm, as shown in Eq. (3).

$$Q_a(s_t, a_t) \leftarrow Q_a(s_t, a_t) + \alpha_a \left(r_t + \gamma_a \max_{a'} Q_a(s_{t+1}, a') - Q_a(s_t, a_t)\right) \tag{3}$$

In Eq. (3), α_a is the learning rate of the attacker. γ_a is the discount factor of the attacker. Defenders (such as network operators, platforms, etc.) need to identify the behavior of attackers through signal mechanisms and adjust defense strategies based on user and device privacy protection signals. The updated Q-value of the defense side is shown in Eq. (4).

$$Q_d(s_t, a_t) \leftarrow Q_d(s_t, a_t) + \alpha_d \left(r_t + \gamma_d \max_{a'} Q_d(s_{t+1}, a') - Q_d(s_t, a_t)\right) \tag{4}$$

In Eq. (4), the defense party adjusts the protection measures based on the attacker's strategy and the privacy protection needs of the device, optimizes its defense effectiveness, and reduces privacy leakage.

Signal game model for privacy protection in the iot

After exploring the evolutionary game model of IoT privacy protection, the signal game model of IoT privacy protection is discussed. This model is different from that of evolutionary game models, as it focuses on analyzing how participants convey privacy protection intentions and behaviors through sending and receiving signals, and formulates strategies. In the signal game model of privacy protection in the IoT, the signal mechanism is the core part. Based on signal mechanisms, participants can convey privacy protection intentions and behaviors, while attackers and defenders adopt corresponding strategies based on the signals. Signal transmission can not only assist all parties in making decisions, but also effectively influence strategy choices and equilibrium points in the game process[24,25]. The strategies of the sender and receiver in the signal game model are shown in Fig. 4.

In Fig. 4 (a), the sender sends signal (m_1, m_2) based on its type (t_1, t_2). Regardless of the sender type, the strategy of sending signal m_1 can be considered as a default privacy protection measure, while selecting to send m_1 or m_2 based on type represents a dynamic privacy protection strategy based on risk assessment. These strategies can be likened to IoT devices choosing different privacy protection measures under different levels of privacy threats. In Fig. 4 (b), the receiver selects its response strategy based on the received signal (a_1, a_2) and the type of sender (t_1, t_2). The strategy selection of the receiver reflects how IoT users or systems adjust their privacy settings based on the received privacy protection signals (such as encryption levels, access control signals, etc.) and the trustworthiness of the sender (such as devices, service providers). In the context of privacy protection in the IoT, the selection of sending and receiving strategies is similar to the decision-making process of devices or users in terms of privacy protection. The sending strategy can be a fixed privacy protection measure (mixed strategy), a conditional privacy protection measure (separation strategy), or a probability based privacy protection measure (mixed strategy). The receiving strategy is how the user or system responds to these privacy protection signals to achieve the optimal privacy protection effect.

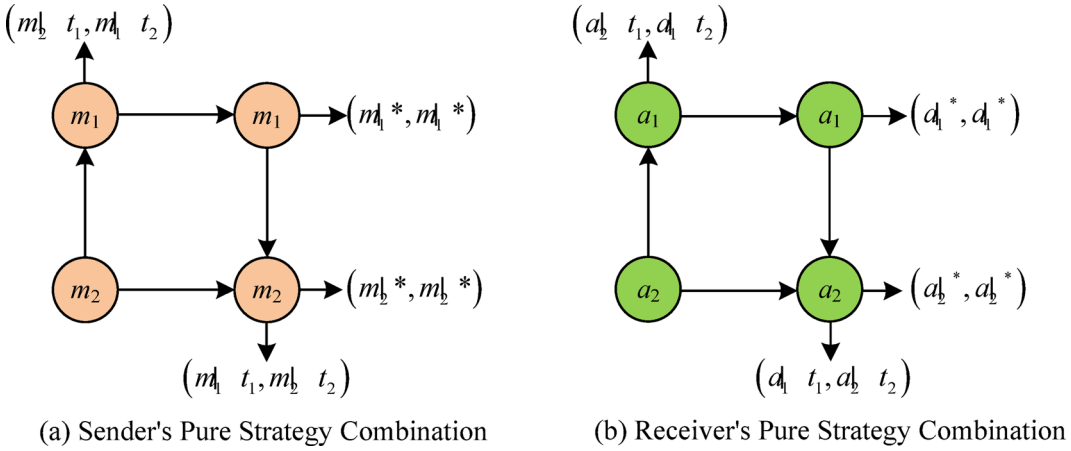
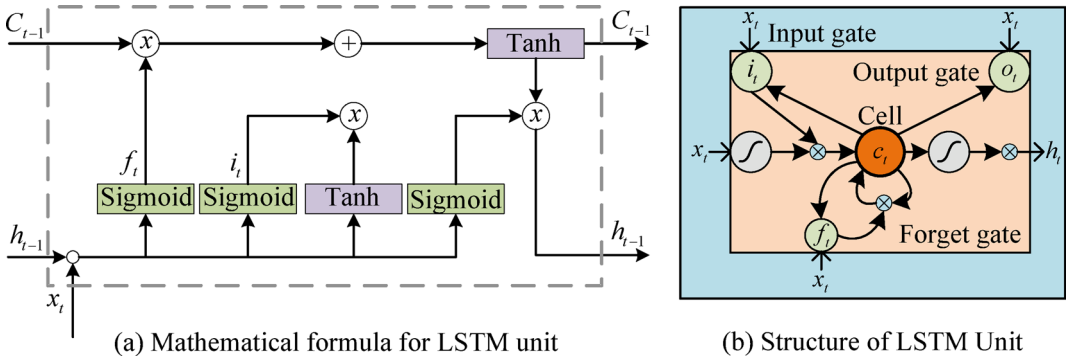


Fig. 4. Strategies of sender and receiver in the signal game model.



(a) Mathematical formula for LSTM unit (b) Structure of LSTM Unit

Fig. 5. LSTM unit structure and process.

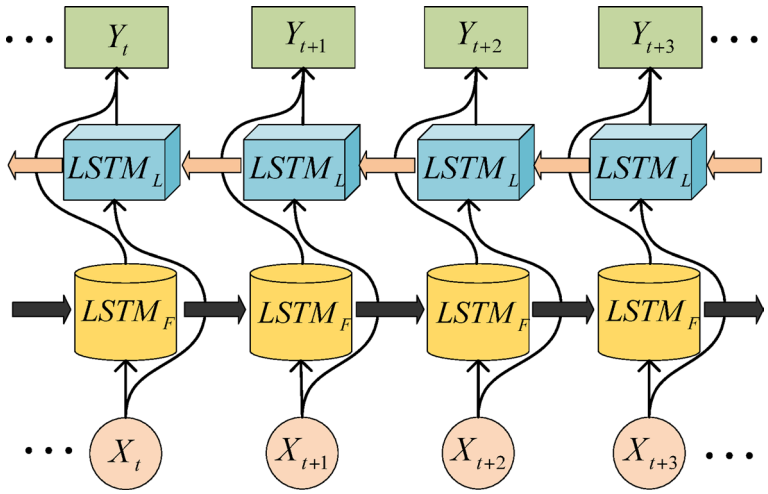


Fig. 6. Schematic diagram of bidirectional LSTM architecture.

In the current research on improving signal game models for privacy protection in the IoT, deep learning algorithms have provided improved solutions. Its main advantage lies in its ability to learn from large-scale datasets and express high-dimensional features[26]. Deep learning technology can automatically learn feature representations suitable for tasks. Therefore, there is no need to manually select features and design algorithms, thereby reducing the subjectivity of manual intervention[27]. In addition, deep learning technology also has better robustness and generalization ability, which can better cope with the diversity of privacy protection signals in the IoT environment. The study introduces the LSTM. The LSTM processes time-series privacy signals generated by IoT devices, including encryption levels, access control logs, and data transmission patterns, which are critical for capturing temporal dependencies in privacy protection behaviors. Specifically, it receives continuous data from device nodes as input and outputs privacy risk predictions, quantifying the likelihood of privacy breaches under different signal patterns. These predictions are fed into the signal game model to enhance strategy selection. Senders (devices) take LSTM outputs to dynamically adjust transmitted signals, while receivers (users/systems) leverage them to optimize the response strategy. By integrating the deep learning framework (Fig. 5) with the game model, LSTM collaborates with CNN layers to extract layered features from mixed spatiotemporal data. The combined CNN-LSTM architecture first processes raw signals into high-dimensional feature representations, which are then fed into a fully connected layer for strategy classification, predicting the optimal privacy measure consistent with the Bayesian equilibrium of the signal game. This integration allows the model to handle the diversity of IoT privacy signals by utilizing the sequential modeling capability of LSTM, ensuring that policy updates in signal games are data-driven and adaptable to dynamic threat environments. The LSTM unit structure and process are shown in Fig. 6.

As shown in Fig. 6, the input sequence in this unit is $x = (x_1, \cdots x_T)$, the hidden vector sequence is $h = (h_1, \cdots h_T)$, and the time is set to $t = (1, \cdots, T)$. The conventional RNN is iterated, as shown in Eq. (5).

$$h_t = H\left(W_{xh}x_t + W_{hh}h_{t-1} + b_h\right) \tag{5}$$

In Eq. (5), W signifies the weight matrix. b signifies the bias. H signifies the hidden layer function. Assuming that the output vector sequence is $y = (y_1, \cdots y_T)$, it is shown in Eq. (6).

$$y_t = W_{hy} h_t + b_y \tag{6}$$

Furthermore, the input gate and forget gate in LSTM can be represented, as shown in Eq. (7).

$$\begin{cases} i_t = \sigma\left(W_{xi} x_t + W_{hi} h_{t-1} + W_{ci} c_{t-1} + b_i\right) \\ f_t = \sigma\left(W_{xf} x_t + W_{hf} h_{t-1} + W_{cf} c_{t-1} + b_f\right) \end{cases} \tag{7}$$

The unit activation vector, output gate, and hidden vector can be represented, as shown in Eq. (8).

$$\begin{cases} c_t = f_t c_{t-1} + i_t \tanh\left(W_{xc} x_t + W_{hc} h_{t-1} + b_c\right) \\ o_t = \sigma\left(W_{xo} x_t + W_{ho} h_{t-1} + W_{co} c_{t-1} + b_o\right) \\ h_t = o_t \tanh\left(c_t\right) \end{cases} \tag{8}$$

In Eqs. (7) and (8), σ represents the activation function. i_i signifies the input gate. f_t signifies the forget gate. c_t signifies the unit activation vector. o_t signifies the output gate. h_t signifies the hidden vector. x_i can determine whether to obtain input. h_i can determine whether to forget the storage of the previous state. c_{i-1} is used to generate the current state c_i. For lip language recognition technology, the associative function of contextual semantics is very important, but the unidirectional LSTM structure may lack contextual information[28]. Therefore, a reverse bidirectional LSTM structure is adopted, mainly using connections between hidden layers to extract semantic features, as shown in Fig. 7[29].

In the reverse bidirectional LSTM structure proposed in the study, the forward transfer parameter $\vec{h}_i$ and backward transfer parameter $\overleftarrow{h}_i$ are mainly used, and the output h_i of the *i*-th group image is utilized, as shown in Eq. (9).

$$h_i = \vec{h}_i + \overleftarrow{h}_i \tag{9}$$

In the field of privacy protection in the IoT, the pre-operation data preparation work of the signal game model is completed. The next task of the entire composite neural network is to extract and classify privacy protection features, as shown in Fig. 5.

In Fig. 5, the model first receives location information from various node groups of IoT devices as input, and then conducts privacy risk assessment on the information through the privacy risk evaluation module. The evaluation results are sent to the strategy filtering module, which consists of multiple LSTM and CNN layers, to extract privacy protection related features and perform strategy filtering[30]. After feature extraction and strategy screening, the data is further reduced in dimensionality through a pooling layer and processed through a fully connected layer. The classifier analyzes the processed features to identify and classify different privacy protection strategies. Finally, the model outputs the integrated results of privacy protection effects. The proposed model is named the Multi-stage Signal Game and Deep Learning Model for IoT Privacy Protection (IoT-PSGDL).

Results

Performance evaluation and strategy analysis of iot privacy protection model

To compare the performance of different models in IoT privacy protection tasks, experiments are conducted on CIC IoT Dataset 2023 and TPCx-IoT Benchmark Dataset. The CIC IoT (https://www.kaggle.com/datasets/dhoogla/ciciotdataset2022) is a publicly available dataset developed by the Canadian Institute for Cybersecurity (CIC) for IoT security research. It contains network traffic data of real devices that are operating normally and under attack. The data covers various protocols and device types, which is suitable for training intrusion detection models, analyzing device behavior, and testing vulnerabilities. The UNSW-NB15 dataset, developed

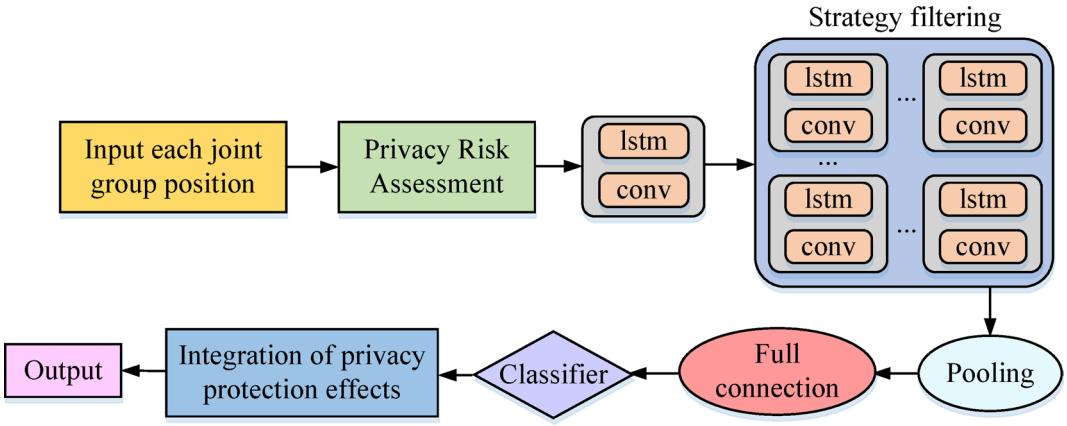


Fig. 7. Deep learning framework for IoT privacy protection signal game model.

by the Australian Center for Cyber Security (ACCS), provides labeled IoT network traffic data encompassing normal and attack scenarios, including DDoS, brute force, and reconnaissance attacks. It supports intrusion detection system evaluation and behavior analysis in IoT environments. The TPCx-IoT dataset is the first industry standard benchmark for evaluating IoT gateway systems, designed by the Transaction Processing Performance Council (TPC). It simulates large-scale sensor scenarios and generates time series data to test the gateway's data ingestion rate, real-time analysis capabilities, and cost efficiency. The measurement indicators include Operations per Second (IoTPS) and price/performance ($/kIoTPS), supporting industrial-grade system performance comparisons. All results are reported as the average of 30 independent runs (standard deviation $\leq 3\%$) to ensure statistical robustness, with performance metrics such as privacy protection effectiveness and strategy update speed validated for consistency. To mitigate overfitting, the dataset is divided into training-validation-test segments according to 70%-20%-10% using stratified sampling to handle class imbalance in attack datasets. Training is halted via early stopping after 15 consecutive epochs without validation loss improvement. Regularization techniques include adding dropout layers (rate = 0.2) to LSTM and CNN components and applying L2 regularization ($\lambda = 0.001$) to network weights. Minor temporal perturbations ($\pm 5\%$ noise in timestamps) are applied to time-series signal data during training for data augmentation. These datasets contain multiple types of attacks and are suitable for evaluating the performance of privacy protection models. Several representative models are selected for comparison in the study, including traditional Recurrent Neural Networks (RNN), LSTM combined with CNN (CNN-LSTM), and the proposed IoT-PSGDL model. The experiment records the error rate of each model during training and testing to evaluate their learning efficiency and generalization ability. The model error for different IoT datasets is shown in Fig. 8.

In Fig. 8 (a), the error rate of IoT-PSGDL rapidly decreased and remained at the lowest level during the iteration process, indicating that it had higher learning efficiency and better generalization ability in handling privacy protection tasks on CIC IoT dataset. In contrast, other models such as RNN, LSTM, and CNN-LSTM also reduced error rates with increasing iteration times, but the decrease was slower and the final error was higher. On the TPCx-IoT benchmark dataset, the IoT-PSGDL model also performed well. As shown in Fig. 8 (b), the error rate of IoT-PSGDL remained the lowest throughout the entire training process, and the downward trend was more stable. This indicates that the model can not only learn quickly, but also effectively maintain a low error rate when dealing with the complex TPCx-IoT dataset. Although other models have also shown some learning ability, there is still a significant gap in their performance compared with IoT-PSGDL. The correlation analysis between IoT privacy protection strategies and measures is shown in Fig. 9.

Figure 9 (a) shows the strategies related to privacy protection in the IoT environment, including data encryption, access control, anonymization, privacy strategy, user consent, and data minimization. The colors in the heatmap represent the strength of the correlation among these strategies, with colors closer to red indicating stronger correlation and colors closer to blue indicating weaker correlation. From the graph, there was a strong correlation between data encryption, access control, anonymization, and other strategies. In IoT environments, these strategies often need to work together to provide effective privacy protection. Figure 9 (b) displays specific measures related to privacy protection in the IoT environment, including encryption protocols, blockchain, privacy design, monitoring and detection, compliance checks, and privacy impact assessments. There is a strong correlation between privacy design and monitoring and detection, as privacy design needs to consider the needs of monitoring and detection to ensure that the privacy protection measures designed can effectively prevent privacy leakage. The MSE and MAE of the four algorithms are shown in Fig. 10.

In Fig. 10 (a), the MSE of the IoT-PSGDL model decreased the fastest and reached the lowest value in fewer iterations, demonstrating its high efficiency and superior performance during the training process. In contrast, the MSE of CNN-LSTM and LSTM models decreased slower, while the MSE of RNN model remained relatively high throughout the entire training process. Figure 10 (b) illustrates the MAE changes of different models

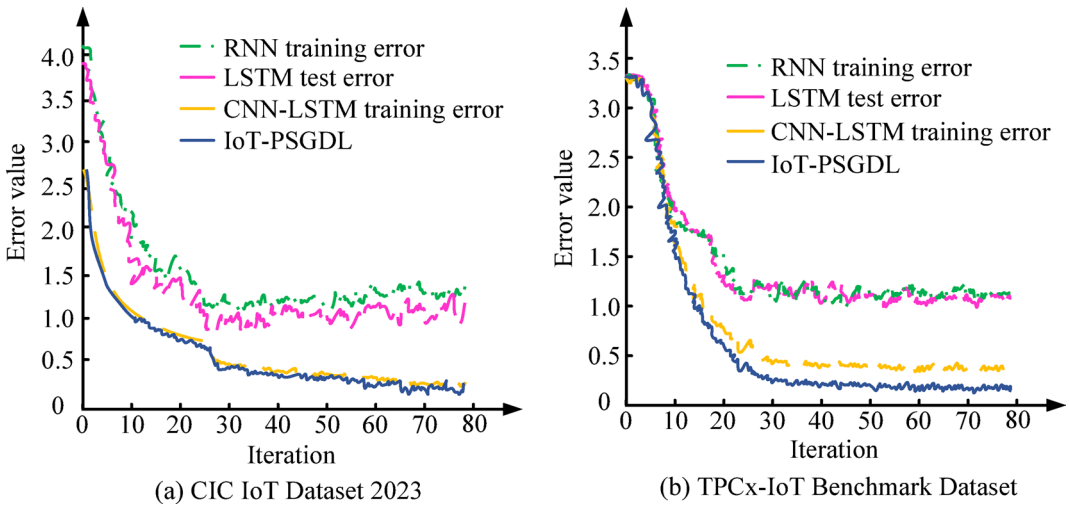
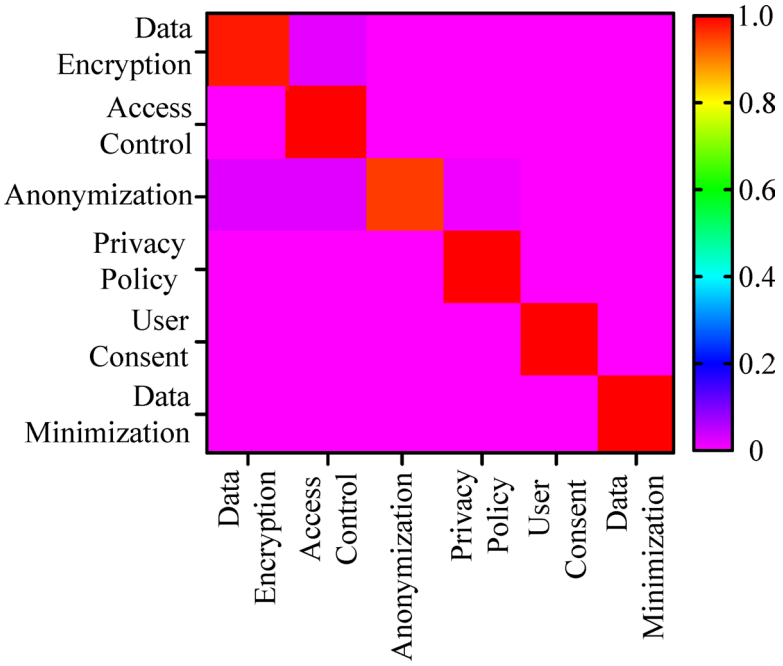
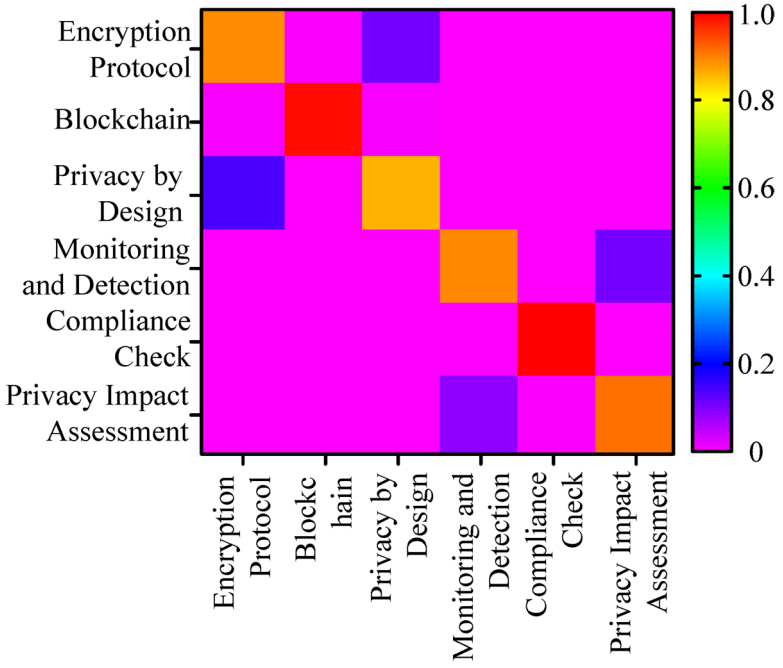


Fig. 8. The comparison of model errors for different IoT datasets.



(a) Strategies related to privacy protection in the Internet of Things



(b) Specific measures related to privacy protection in the Internet of Things

Fig. 9. Correlation analysis of privacy protection strategies and measures in the IoT.

during the training process. The IoT-PSGDL model also showed the fastest decline rate and reached the lowest value in fewer iterations, further demonstrating its advantage in prediction accuracy. The MAE of CNN-LSTM and LSTM models decreased slowly, while the MAE of RNN was higher. The F1 values and recall of the four algorithms are shown in Fig. 11.

Figure 11 (a) shows the F1 value change of different models. The F1 value of the IoT-PSGDL rapidly increased and reached its highest value in fewer iterations, demonstrating its high efficiency and superior performance during the training process. In contrast, the F1 values of CNN-LSTM and LSTM models increased slowly, while

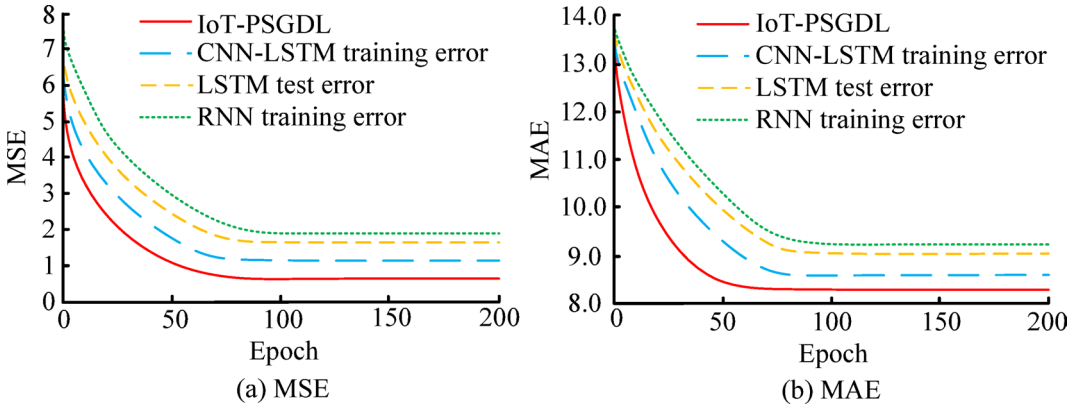


Fig. 10. MSE and MAE of four algorithms.

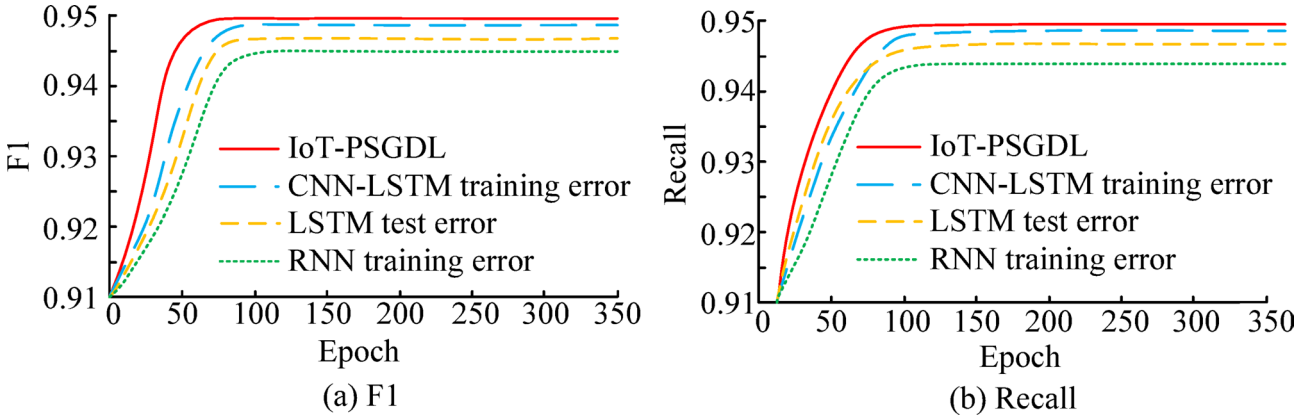


Fig. 11. F1 values and recall of four algorithms.

the F1 value of RNN model remained at a lower level throughout the entire training process. Figure 11 (b) shows the recall changes of different models during the training process. The IoT-PSGDL model also showed the fastest upward speed and reached the highest value in fewer iterations, further demonstrating its advantage in prediction accuracy. The recall of CNN-LSTM and LSTM models increased slowly, while the recall of RNN model remained at a low level throughout the entire training process.

Dynamic evolution and stability analysis of models

To evaluate the performance of privacy protection models, experiments are conducted on two datasets: CIC IoT Dataset 2023 and TPCx-IoT Benchmark Dataset. The experiment records the error rate of each model during training and testing to evaluate the learning efficiency and generalization ability. The experiment is evaluated through multiple indicators, including privacy protection effectiveness, strategy update speed, system response time, resource consumption, data transmission efficiency, and data protection rate. The specific results are shown in Table 1.

Table 1 displays the experimental results, including IoT-PSGDL, CNN-LSTM, LSTM, and RNN, on the CIC IoT and TPCx-IoT. The IoT-PSGDL model achieved a privacy protection effectiveness of 98.25% on the CIC IoT dataset, with a strategy update speed of 7.42 updates/second and a system response time of 35.12ms. The privacy protection effectiveness on the TPCx-IoT dataset was 97.84%, the strategy update speed was 6.98 updates/second, and the system response time was 39.57ms. In contrast, CNN-LSTM, LSTM, and RNN models all performed poorly in various indicators, especially the RNN, whose privacy protection effectiveness was 85.93% and 84.56% on the two datasets, respectively, significantly lower than the IoT-PSGDL model. The IoT-PSGDL model has better performance in IoT privacy protection tasks. The performance evaluation indicators of the IoT privacy protection model are presented in Table 2.

Table 2 provides performance evaluation metrics for IoT privacy protection models on different datasets, including privacy protection continuity, communication delay, strategy flexibility, data storage security, energy efficiency, and system throughput. After 150 iterations on the CIC IoT dataset, the IoT-PSGDL model achieved privacy protection continuity of 97.56%, communication delay of 54.12ms, strategy flexibility of 93.48%, data storage security of 96.75%, energy efficiency of 4.23 joules/GB, and system throughput of 3.65GB/s. On the TPCx-IoT dataset, the IoT-PSGDL model underwent 200 iterations, with a privacy protection continuity of

Model Type	Dataset	Iterations	Privacy Protection Effectiveness (%)	Strategy Update Speed (updates/second)	System Response Time (ms)	Resource Consumption (W)	Data Transmission Efficiency (Mbps)	Data Protection Rate (%)
IoT-PSGDL	CIC IoT	150	98.25	7.42	35.12	0.85	45.76	99.68
IoT-PSGDL	TPCx-IoT	200	97.84	6.98	39.57	0.92	44.62	99.52
CNN-LSTM	CIC IoT	180	94.61	5.62	42.31	0.78	42.93	98.27
CNN-LSTM	TPCx-IoT	210	93.14	5.29	45.03	0.83	41.85	97.95
LSTM	CIC IoT	170	92.38	4.80	48.74	0.75	41.02	97.14
LSTM	TPCx-IoT	180	90.27	4.60	51.36	0.80	40.50	96.38
RNN	CIC IoT	220	85.93	3.21	56.17	0.71	39.64	94.72
RNN	TPCx-IoT	240	84.56	3.08	59.24	0.74	38.72	94.11

Table 1. Experimental results of IoT privacy protection model.

Model Type	Dataset	Iterations	Privacy Protection Continuity (%)	Communication Delay (ms)	Strategy Flexibility (%)	Data Storage Security (%)	Energy Efficiency (J/GB)	System Throughput (GB/s)
IoT-PSGDL	CIC IoT	150	97.56	54.12	93.48	96.75	4.23	3.65
IoT-PSGDL	TPCx-IoT	200	96.88	59.34	92.61	95.42	4.08	3.52
CNN-LSTM	CIC IoT	180	94.76	62.21	88.59	93.12	3.92	3.44
CNN-LSTM	TPCx-IoT	210	93.12	67.45	86.75	91.36	4.01	3.30
LSTM	CIC IoT	170	92.46	70.32	85.14	90.98	4.09	3.12
LSTM	TPCx-IoT	180	91.12	74.08	84.23	89.67	4.15	3.07
RNN	CIC IoT	220	88.67	79.33	82.41	86.29	4.25	2.98
RNN	TPCx-IoT	240	87.54	83.67	80.57	84.12	4.30	2.90

Table 2. Performance evaluation indicators for IoT privacy protection model.

Indicator	Data Encryption	Data Anonymization	Access Control	Data Minimization	Privacy Policy	User Consent
Privacy Protection Success Rate (%)	96.72	94.56	93.84	91.67	92.18	90.32
System Processing Capacity (Requests/second)	850	900	820	750	870	780
Privacy Leakage Probability (%)	2.14	3.25	4.07	5.21	4.89	6.03
Attack and Defense Effectiveness (%)	92.68	89.71	90.55	85.32	87.97	84.12
System Load (%)	45.12	48.53	42.79	50.18	46.64	52.45
Data Storage Security (%)	97.34	95.63	96.21	94.78	96.54	93.85
Strategy Update Time (second)	3.45	3.87	4.15	4.58	3.95	5.02

Table 3. Experimental results of IoT privacy protection strategies.

96.88%, communication delay of 59.34ms, strategy flexibility of 92.61%, data storage security of 95.42%, energy efficiency of 4.08 joules/GB, and system throughput of 3.52GB/s. In contrast, CNN-LSTM, LSTM, and RNN are lower than the IoT-PSGDL model in various performance indicators, with the RNN performing the worst on privacy protection continuity and system throughput. The experimental results of IoT privacy protection strategies are displayed in Table 3.

In Table 3, among all strategies, data encryption performed the best, with a privacy protection success rate of 96.72% and a privacy leakage probability of only 2.14%. Meanwhile, the attack and defense effectiveness was also high, reaching 92.68%. The privacy protection success rate of data anonymization strategy was 94.56%, while the privacy leakage probability was 3.25%. Although the system has strong processing capabilities, the privacy leakage probability of data anonymization strategy is slightly higher than that of data encryption. The privacy protection success rate of the access control policy was 93.84%, the system processing capacity was 820 requests/second, and the privacy leakage probability was 4.07%. Although its privacy protection effect is slightly inferior, it still demonstrates good security and defense effectiveness. The dynamic evolution and stability analysis results of the IoT privacy protection model are displayed in Table 4.

Table 4 presents the analysis results of the IoT privacy protection model on dynamic evolution and stability. The fitness of the data encryption strategy increased from 0.37 to 0.92 after 100 iterations, with the highest stability of 0.85 and final evolutionary stability of 97.56%. The system resource consumption was 4.65 W. The data anonymization and privacy policy strategies also showed high fitness improvement and stability, reaching fitness of 0.9 and 0.91, respectively, with stability indices of 0.82 and 0.83, respectively. The fitness improvement

Strategy Type	Initial Fitness	Fitness After 100 Iterations	Stability	Evolution Time (sec)	Convergence Speed (Fitness Increase/sec)	Final Evolutionary Stability (%)	System Resource Consumption (W)
Data Encryption	0.37	0.92	0.85	120	0.0043	97.56	4.65
Data Anonymization	0.42	0.89	0.82	110	0.0051	96.84	4.35
Access Control	0.35	0.88	0.78	130	0.0049	95.23	4.25
Data Minimization	0.30	0.85	0.74	140	0.0037	93.67	4.10
Privacy Policy	0.40	0.91	0.83	115	0.0054	96.57	4.55
User Consent	0.33	0.87	0.75	125	0.0045	94.12	4.20

Table 4. Dynamic evolution and stability analysis results of IoT privacy protection model.

of access control and data minimization strategies was slightly lower, at 0.88 and 0.85 respectively, and the stability index and final evolutionary stability were also relatively low. The fitness of the user consent policy improved to 0.87, and the stability and final evolutionary stability were both 0.75 and 94.12%, respectively. The system resource consumption was the lowest, at 4.20 W.

Discussion

The proposed IoT-PSGDL model demonstrates notable advancements in addressing IoT privacy challenges by integrating evolutionary game theory, signal game mechanism, and deep learning, achieving superior performance metrics such as a 98.25% privacy protection effectiveness on the CIC IoT dataset and 7.42 updates/second efficient strategy updates. Evolutionary dynamics achieves adaptive strategy refinement through replication and Fermi update, and real-time interaction driven by signal games is achieved through privacy signals processed by LSTM. The synergistic effect between these two enhances the ability to balance long-term stability and immediate threat response. Experimental results also highlight the efficacy of data encryption as a cornerstone strategy, achieving a 96.72% protection success rate and minimal leakage (2.14%). There is a trade-off in system load (45.12%) compared to lighter strategies such as data minimization.

However, the robustness and generalizability of the model depend on several assumptions and structural features that require critical reflection. A key limitation lies in the assumption of rational behavior among stakeholders. Users, devices, network operators, and attackers are modeled as consistently optimizing for maximal payoffs, which may not align with real-world scenarios where users might prioritize convenience over privacy or attackers employ non-optimal stochastic strategies This idealized rationality can undermine the model's prediction accuracy in environments with noisy or unpredictable stakeholder behaviors. Additionally, the centralized architecture underpinning the policy decision-making module (e.g., the strategy filtering and deep learning framework in Fig. 5) introduces a vulnerability to single-point failures. Targeted attacks on this component may disrupt the policy updates of the entire network, thereby compromising overall privacy protection. Although the model exhibits stable convergence in homogeneous datasets, its performance in heterogeneous IoT ecosystems faces challenges. These ecosystems are characterized by different device capabilities (such as low-power sensors in smart homes, high-throughput industrial controllers in industrial IoT), network latency, and resource limitations. For instance, resource-constrained edge devices in real-world deployments (such as smart home sensors or industrial IoT gateways) may struggle with the computational overhead of LSTM-based signal processing, which requires significant CPU/GPU resources and energy, and may delay policy adaptation and convergence, as hinted by the slower evolutionary stability metrics observed in less efficient strategies such as user consent (final stability: 94.12%). Furthermore, the signal game framework assumes that attackers operate within a defined strategy space, but emerging adversarial techniques such as generating misleading encryption signals to evade detection may exploit unmodeled signal patterns, highlighting the need for enhanced robustness against evasion attacks.

These limitations underscore opportunities for future research, such as incorporating behavioral economics to model bounded rationality, designing decentralized architectures to mitigate single-point risks, and developing lightweight neural models or hierarchical edge-cloud frameworks to improve convergence in heterogeneous environments. Despite these challenges, the fundamental framework that combines game theory with data-driven learning provides a solid foundation for addressing dynamic privacy threats. The empirical results have validated its effectiveness in multiple IoT datasets and scenarios. Table 5 shows a comparison with previous research in this field.

Conclusion

With the continuous development of IoT technology, privacy protection issues have become increasingly important. A privacy protection model for the IoT based on evolutionary game theory and signal game mechanism was proposed, and the privacy protection strategy was optimized by combining Q-learning algorithm and deep learning technology. The method simulates the behavior evolution of multiple participants by introducing evolutionary game theory, utilizes signal game mechanism to deal with information asymmetry, and optimizes privacy protection effect through deep learning methods. The proposed IoT-PSGDL performed well on the CIC IoT dataset, with a privacy protection effectiveness of 98.25%, a policy update speed of 7.42 times/second, and a system response time of 35.12ms. In addition, the performance on the TPCx-IoT dataset was also excellent, with a privacy protection effectiveness of 97.84%, a policy update speed of 6.98 times/second, and a system response

Method	Core Technology	Application Scenario	Privacy Protection Effectiveness	Processing Efficiency	Reference
Regulatory framework analysis	Component classification and compliance design	Healthcare IoT data processing	N/A (qualitative)	N/A	Shahid J et al.[8]
Systematic review & blockchain integration	Blockchain technology and consensus algorithms	General IoT security/privacy	N/A (review-based)	N/A	Zubaydi H D et al.[9]
Edge computing with federated learning	Lightweight privacy protocols	Medical IoT data sharing	N/A (focus on privacy disclosure)	Low-latency edge processing	Wang R et al.[10]
Memristive neural network encryption	MHNN-based hardware encryption	Secure medical data transmission	High (hardware-level security)	High-speed encryption (hardware-accelerated)	Yu F et al.[11]
Homomorphic encryption + blockchain technology	Homomorphic operations and blockchain smart contracts	Healthcare IoT critical data protection	High (encrypted data processing)	Moderate (blockchain transaction latency)	Ali A et al.[12]
CNN + blockchain federated learning	CNN and blockchain	Industrial cloud IoT health records	97.54-98.13% (classification accuracy)	High (data filtering efficiency)	Alzubi J A et al.[13]
Blockchain + signcryption	Signcryption technology and blockchain trust layer	Medical data transmission in IoT	High (secure transmission)	Low-latency signaling (signcryption)	Alzubi O A et al.[14]
Blockchain-driven security management framework	Blockchain, smart contracts, and distributed ledger	Mobile edge computing (MEC) environment, user data security/privacy	High (security assurance)	Low latency and high throughput	Alzubi J A et al.[15]
Semantic communication + signal game	Signal game mechanism and neural-symbolic AI	General IoT data transmission	N/A (efficiency-focused)	High (semantic compression)	Thomas C K et al.[16]
Signal game mechanism framework	Bayesian equilibrium analysis	Multi-stage dynamic privacy games	N/A (theoretical model)	N/A	Angelini F et al.[17]
Evolutionary game + signal game + deep learning	LSTM-CNN, Q-learning, and replication dynamics	General IoT ecosystems (CIC IoT, TPCx-IoT)	98.25% (CIC IoT dataset)	7.42 updates/second (strategy update speed)	Proposed model

Table 5. Comparison with previous research in this field.

time of 39.57ms. This indicates that the IoT-PSGDL can efficiently optimize privacy protection strategies on different datasets, with low response time and high learning efficiency. Among various privacy protection strategies, data encryption strategy performed the best, with a privacy protection success rate of 96.72% and a privacy leakage probability of 2.14%. The privacy protection success rate of data anonymization strategy was 94.56%, and the probability of privacy leakage was 3.25%. These results indicate that data encryption not only has the most outstanding privacy protection effect, but also has a lower risk of leakage. Although the model demonstrates good adaptability, the scalability of large-scale IoT ecosystems faces a bottleneck that combines evolutionary game dynamics and deep learning complexity, making edge devices with limited resources, CPU/GPU, and energy budgets overwhelmed. Computation time, particularly for iterative strategy updates in deep learning modules, further prolongs convergence delays and hinders real-time adaptation in heterogeneous networks. Different delays can delay the optimal strategy adaptation during the iterative update process. Mitigation includes: (1) model lightweighting through parameter quantization and neural architecture search to reduce edge computational load for faster signal processing; (2) Hierarchical collaborative architecture: While processing real-time signal encoding/decoding on edge devices, dense evolutionary simulations are offloaded to the cloud, using federated learning to aggregate decentralized updates without centralized data exposure. These measures balance the scalability and privacy efficiency for distributed IoT environments.

Data availability

The datasets used and/or analysed during the current study available from the corresponding author on reasonable request.

Received: 1 April 2025; Accepted: 24 June 2025
Published online: 01 July 2025

References

1. Paraschos, P. D. & Koulouriotis, D. E. Game difficulty adaptation and experience personalization: A literature review. *Int. J. Human-Comput Interact.* **39** (1), 1–22. https://doi.org/10.1080/10447318.2021.2020008 (Jan. 2023).
2. Singh, B. & Kaunert, C. Integration of cutting-edge technologies such as internet of things (IoT) and 5G in health monitoring systems: a comprehensive legal analysis and futuristic outcomes. *GLS Law J.* **6** (1), 13–20. https://doi.org/10.69974/glslawjournal.v6i1.123 (Jan. 2024).
3. Mohammad, N. et al. Ensuring security and privacy in the internet of things: challenges and solutions. *J. Comput. Commun.* **12** (8), 257–277. https://doi.org/10.4236/jcc.2024.128016 (Aug. 2024).
4. Ullah, A. et al. Smart cities: the role of internet of things and machine learning in realizing a data-centric smart environment. *Complex. Intell. Syst.* **10** (1), 1607–1637. https://doi.org/10.1007/s40747-023-01175-4 (Feb. 2024).
5. Dornelas, R. S. & Lima, D. A. Correlation filters in machine learning algorithms to select demographic and individual features for autism spectrum disorder diagnosis. *J. Data Sci. Intell. Syst.* **1** (2), 105–127. https://doi.org/10.47852/bonviewJDSIS32021027 (Jun. 2023).
6. Tudoran, A. A. Rethinking privacy in the Internet of Things: a comprehensive review of consumer studies and theories, Internet Res., vol. 35, no. 2, pp. 514–545, Mar. (2025). https://doi.org/10.1108/INTR-01-2023-0029
7. Sarker, I. H., Khan, A. I., Abushark, Y. B. & Alsolami, F. Internet of things (IoT) security intelligence: a comprehensive overview, machine learning solutions and research directions. *Mob. Netw. Appl.* **28** (1), 296–312. https://doi.org/10.1007/s11036-022-01937-3 (Feb. 2023).

8. Shahid, J. et al. Data protection and privacy of the internet of healthcare things (IoHTs). *Appl. Sci.* **12** (4), 1927–1949. https://doi.org/10.3390/app12041927 (Feb. 2022).
9. Zubaydi, H. D., Varga, P. & Molnár, S. Leveraging blockchain technology for ensuring security and privacy aspects in internet of things: A systematic literature review, Sensors, vol. 23, no. 2, pp. 788–831, Jan. (2023). https://doi.org/10.3390/s23020788
10. Wang, R. et al. Privacy-preserving federated learning for internet of medical things under edge computing. *IEEE J. Biomed. Health Inf.* **27** (2), 854–865. https://doi.org/10.1109/JBHI.2022.3157725 (Feb. 2022).
11. Yu, F. et al. Privacy protection of medical data based on multi-scroll memristive Hopfield neural network, *IEEE Trans. Netw. Sci. Eng.*, **10**, 2, 845–858, https://doi.org/10.1109/TNSE.2022.3223930.Apr. (2022).
12. Ali, A., Al-Rimy, B. A. S., Alsubaei, F. S., Almazroi, A. A. & Almazroi, A. A. Healthlock: Blockchain-based privacy preservation using homomorphic encryption in internet of things healthcare applications, Sensors, vol. 23, no. 15, pp. 6762–6791, Jul. (2023). https://doi.org/10.3390/s23156762
13. Alzubi, J. A., Alzubi, O. A., Singh, A. & Ramachandran, M. Cloud-IIoT-based electronic health record privacy-preserving by CNN and blockchain-enabled federated learning. *IEEE Trans. Ind. Informat.* **19** (1), 1080–1087. https://doi.org/10.1109/TII.2022.3189170 (Jan. 2022).
14. Alzubi, O. A., Alzubi, J. A., Shankar, K. & Gupta, D. Blockchain and artificial intelligence enabled privacy-preserving medical data transmission in internet of things. *Trans. Emerg. Telecommun Technol.* **32** (12), e4360. https://doi.org/10.1002/ett.4360 (Sept. 2021).
15. Alzubi, J. A., Alzubi, O. A., Singh, A. & Mahmod Alzubi, T. A blockchain-enabled security management framework for mobile edge computing. *Int. J. Netw. Manage.* **33** (5), e2240. https://doi.org/10.1002/nem.2240 (May. 2023).
16. Thomas, C. K. & Saad, W. Neuro-symbolic causal reasoning Meets signaling game for emergent semantic communications. *IEEE Trans. Wirel. Commun.* **23** (5), 4546–4563. https://doi.org/10.1109/TWC.2023.3319981 (May. 2023).
17. Angelini, F. & Castellani, M. Price and information disclosure in the private Art market: a signalling game. *Res. Econ.* **76** (1), 14–20. https://doi.org/10.1016/j.rie.2022.01.002 (Mar. 2022).
18. Al-Shaarani, F. & Gutub, A. Increasing participants using counting-based secret sharing via involving matrices and practical steganography. *Arab. J. Sci. Eng.* **47** (2), 2455–2477. https://doi.org/10.1007/s13369-021-06165-7 (Feb. 2022).
19. Rahmani, A. M., Bayramov, S. & Kiani Kalejahi, B. Internet of things applications: opportunities and threats. *Wirel. Pers. Commun.* **122** (1), 451–476. https://doi.org/10.1007/s11277-021-08907-0 (Jan. 2022).
20. Zhou, Y. et al. Game theoretic physical layer authentication for spoofing detection in UAV communications. *IEEE Trans. Veh. Technol.* **71** (6), 6750–6755. https://doi.org/10.1109/TVT.2022.3161006 (Jun. 2022).
21. Swessi, D. & Idoudi, H. A survey on internet-of-things security: threats and emerging countermeasures. *Wirel. Pers. Commun.* **124** (2), 1557–1592. https://doi.org/10.1007/s11277-021-09420-0 (May. 2022).
22. Ghaemi Asl, M., Ghasemoghli, A. & Khalfaoui, R. Nash equilibrium in emerging partnership-based Islamic banking industry with a bayesian game-theoretic approach. *Int. J. Emerg. Mark.* **19** (11), 3709–3728. https://doi.org/10.1108/IJOEM-08-2022-1274 (Nov. 2024).
23. Chi, H. R., Wu, C. K., Huang, N. F., Tsang, K. F. & Radwan, A. A survey of network automation for industrial internet-of-things toward industry 5.0. *IEEE Trans. Ind. Inf.* **19** (2), 2065–2077. https://doi.org/10.1109/TII.2022.3215231 (Oct. 2022).
24. Niu, R. et al. Plant-mimetic vertical-channel hydrogels for synergistic water purification and interfacial water evaporation. *ACS Appl. Mater. Interface.* **14** (40), 45533–45544. https://doi.org/10.1021/acsami.2c14773 (Oct. 2022).
25. Saheed, Y. K., Abiodun, A. I., Misra, S., Holone, M. K. & Colomo-Palacios, R. A machine learning-based intrusion detection for detecting internet of things network attacks. *Alexandria Eng. J.* **61** (12), 9395–9409. https://doi.org/10.1016/j.aej.2022.02.063 (Dec. 2022).
26. Niazi, P., Alimyar, O., Azizi, A., Monib, A. W. & Ozturk, H. People-plant interaction: plant impact on humans and environment. *J. Environ. Agr Stud.* **4** (2), 1–7. https://doi.org/10.32996/jeas.2023.4.2.1 (May. 2023).
27. Ghimire, B. & Rawat, D. B. Recent advances on federated learning for cybersecurity and cybersecurity for federated learning for internet of things. *IEEE Internet Things J.* **9** (11), 8229–8249. https://doi.org/10.1109/JIOT.2022.3150363 (Feb. 2022).
28. Ghasemi, P., Goodarzian, F., Gunasekaran, A. & Abraham, A. A bi-level mathematical model for logistic management considering the evolutionary game with environmental feedbacks. *Int. J. Logist Manage.* **34** (4), 1077–1100. https://doi.org/10.1108/IJLM-04-2021-0199 (Jun. 2023).
29. Kilicay-Ergin, N., Barb, A. & Chaudhary, N. Knowledge elicitation methodology for evaluation of internet of things privacy characteristics in smart cities. *Syst. Eng.* **27** (2), 354–367. https://doi.org/10.1002/sys.21726 (Oct. 2024).
30. Kalapaaking, A. P. et al. Blockchain-based federated learning with secure aggregation in trusted execution environment for internet-of-things. *IEEE Trans. Ind. Inf.* **19** (2), 1703–1714. https://doi.org/10.1109/TII.2022.3170348 (Apr. 2022).

Author contributions

Y.L. processed the numerical attribute linear programming of communication big data, and the mutual information feature quantity of communication big data numerical attribute was extracted by the cloud extended distributed feature fitting method. Y.L. and H.M.L. Combined with fuzzy C-means clustering and linear regression analysis, the statistical analysis of big data numerical attribute feature information was carried out, and the associated attribute sample set of communication big data numerical attribute cloud grid distribution was constructed. H.M.L. and L.L. did the experiments, recorded data, and created manuscripts. All authors read and approved the final manuscript.

Funding

This research received no external funding.

Declarations

Competing interests

The authors declare no competing interests.

Additional information

Correspondence and requests for materials should be addressed to H.L.

Reprints and permissions information is available at www.nature.com/reprints.

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.