ISSN 2616-5775 Vol. 4, Issue 4: 82-88, DOI: 10.25236/AJCIS.2021.040415

Blockchain Model of Sensitive Information Identification in Social Online Games

Bai Jie[1,2,a], Du Yanhui[1,b*], Lu Tianliang[1,c]

[1]College of Information Network Security, People's Public Security University of China, Beijing, China
[2]College of International Education, Wenzhou University, Wenzhou, China
[a] wxbaijie@163.com, [b] dyh6889@126.com , [c] lutianliang@ppsuc.edu.cn
**Corresponding Author*

Abstract: *This paper studies the sensitive information recognition and processing system in social online games. A real-time data mining framework for sensitive information on online games in the blockchain mode is proposed. A large-scale social online game chat room database is selected for testing, with SKLearn library based on Python is used for data preprocessing. The model training and verification are implemented through tensorflow. The results show that the accuracy of TextCNN is over 5% higher than that of Naive Bayes and CNN models for short text recognition in online game context, so TextCNN model can meet the requirements for high efficiency and accuracy of sensitive information recognition in large-scale online games. The conclusion proves that the blockchain-based online game sensitive information mining framework has the advantage of alliance chain hierarchical management, the characteristics of the distributed ledgers leaving traces in the whole process of information dissemination, and enhanced contract enforcement through the smart contracts and consensus mechanisms.*

Keywords: *Network sensitive information; Social online games; Blockchain model; Deep learning*

1. Introduction

China has 940 million Internet users and 932 million mobile Internet user[1] , the utilization rate of online games reached 57.4%[2], according to the 46th statistical report on the development of Internet in China issued by China Internet Network Information Center. Every player will publish and receive information through the game platform in social online games. It will also increase the amount of information, such as forwarding, broadcasting and other behaviors, when there is a hot topic or a speech guide. The group of game players is usually emotional and easily angered. A small social event with emotional views can easily attract the discussion of the players and spread widely on the Internet, thus becoming a hot spot in the network community. Sensitive information should be identified quickly and effectively in a large amount of network information. Internet users are protected away from reactionary, violence, pornography and other adverse public opinions by filtering and preventing the spread of sensitive information. Although many countries have adopted a game classification system in order to protect minors, the dissemination and prevention of online game sensitive information are insufficient.

With the rapid development of artificial intelligence technology recent years, various models based on intelligent methods have made remarkable achievements in practice. These Tools are provided for the discovery of sensitive information (including text, image and voice), such as , deep learning is widely used in text classification of natural language processing [3-5]， accurate text classification and the establishment of thesaurus are the prerequisites for the discovery of sensitive information in social mobile games. Blockchain is a shared distributed database technology, and its advantages are decentralized and non-tamperable encryption security [6-8].Blockchain has made great progress in industry and finance. It was first applied to the field of Internet trial and evidence deposit in 2018, which provides a valuable reference for the development of digital evidence.

The main contributions of this paper are:

1) This study analyzes the advantages of block chain model in the discovery, judgment and processing of sensitive information. The distributed accounting system of blockchain can improve the efficiency of sensitive information mining. The digital signature of blockchain can realize the rapid traceability of sensitive information sources and effectively improve the processing accuracy of sensitive information in online games.

ISSN 2616-5775 Vol. 4, Issue 4: 82-88, DOI: 10.25236/AJCIS.2021.040415

2) The data model layer is improved in the blockchain model, and the optimized deep learning algorithm is applied to improve the accuracy and efficiency of text classification and annotation. The high efficiency is achieved through database testing, which provides a theoretical basis for the network security monitoring of subsequent rumors.

2. Summary of rumor handling methods

We Sensitive network information includes multimedia forms such as text, pictures, voice and video. The main communication method is Chinese/English text classification in large-scale mobile games. An effective means to prevent sensitive information from spreading on the Internet or even fermenting into public opinion is information discovery-traceability-filtering. Dialogues with bad texts are finding by analyzing online information content, For example, Filtering politically sensitive information; blocking website links, which contain pornographic and violent information; tracing the source of accounts that have long-lived sensitive information, these build a common system for online public opinion prevention.

Sensitive text information in mobile games can be divided into two categories, One is thematic text, and the other is emotional text[9].Thematic texts, such as texts of violence, pornography, fraud, spam, etc., have obvious subject words, and WEB crawlers can usually be used to grab specific keywords and block the grabbed messages. Sensitive information texts with emotional tendencies, involve political, economic and other reactionary speeches, often contain information such as the opinions, attitudes, and positions of the information publisher,so that is difficult to identify in time. so that it is difficulty to control the fermentation of bad public opinion. Manual identification marks are used by game companies, which consume a lot of manpower and inefficiently Therefore, it is necessary to adopt an intelligent method to deal with it in time. Single point-to-point input-output is often inefficient. The processing sequence of closed-loop feedback of sensitive information is usually based on game player→information terminal→network control center→public security network security department→network control center →game terminal→player. This process is difficult to meet the time-critical task in public opinion control. The game developers are mainly technical personnel, and the definition of sensitive information is relatively lack of professionalism. This requires a lot of police force to investigate and trace the source.

Distributed decentralization is the feature of blockchain technology. The process of data mining, verification, storage and transmission in blockchain network is based on distributed system structure[10], According to the model of the blockchain architecture, ordinary players are used as nodes, sensitive information (consensus mechanism) can be marked (reported) by several common players in a short period of time , and quickly fed back to the blockchain center (in each game zone),causing early warning from the cybersecurity department . It can quickly improve the efficiency of mining and processing public opinion information.

Representative algorithms for web mining mainly include decision trees, rule induction, Bayesian methods, support vector machines, neural networks, etc[11-13]. Research on mining algorithms and mining applications has gradually increased as a research hotspot. It is worth noting that deep learning in artificial intelligence is widely used in text classification for network sensitive information mining [14,15]. Deep learning strengthens machine learning and abstracts data through multiple processing layers composed of multi-level hidden layer perceptrons, so the efficiency of crawling is improved by replacing manual feature acquisition. Deep learning models such as convolutional neural networks and recurrent neural networks are used to improve the accuracy of text classification In web mining text classification tasks [16]. Processing the more complex network text requires more training data according to actual condition, Pre-trained word vectors can improve the classification results, This reflects the advantages of deep learning in the mining of sensitive information.

3. Network sensitive information model of online game in blockchain mode

In this section, the mobile game sensitive information mining model in the blockchain mode is introduced. Structure and module definition of sensitive information mining model is defined; the characteristics of the sensitive information mining system in the blockchain modle is described; application methods and comparative advantages of deep learning algorithms in the data model layer is analyzed.

ISSN 2616-5775 Vol. 4, Issue 4: 82-88, DOI: 10.25236/AJCIS.2021.040415

3.1. Network sensitive information mining system in blockchain mode

3.1.1. P2P network of bottom layer

The text message published by game players, accessed through the P2P network interface, when each node keeps all data, In this way, even if sensitive information is deleted by one node, evidence remains in other nodes. sensitive words are crawled by web crawlers by sampling nodes, sensitive information vocabulary is established for the subject text, it is reported by nodes belonging to the same block and uploaded to the district server to realize the sensitive information data collection function. Each server regularly sends the identified data to the trusted storage service module after signing it by asymmetric encryption communication technology.

3.1.2. Protocol layer (consensus mechanism)

In the sensitive information-mining model, if a consensus is reached between nodes, it is determined that a certain piece of information is bad public opinion, and then proceed to the next step. The main function of the consensus mechanism is to maintain the consistency of the authentication of the underlying blockchain sensitive data. Malicious false reports or players' wrong report clicks are prevented, and a large amount of pseudo-sensitive information is eliminated, thereby saving calculation space and reducing invalid calculations [17].The authenticity of sensitive information is determined by the consensus mechanism, then the hash value generated by the current block is added to the parent block,Stored in are encrypted blockchain for tamper-proof protection.

3.1.3. Data model layer:

Blockchain is a distributed storage database that saves game player information, account numbers, and information statement records instantly. In the blockchain, each data block consists of two parts: a block header and a block body.The characteristic value of the current block, such as the information generation time, the hash value of the block data, the hash value of the previous block, etc. is recorded in the blockchain head. In the process of dissemination of sensitive information, the first generation 0 block (no Hash address) is generated, and the subsequent transaction blocks point to the 0 generation block in turn, with the Hash address of the previous block (the characteristic identifier of the block) retained. Block generations are connected by Hash address (characteristic) to form a chain structure of information. The first issuer of sensitive information in the block chain can be recorded and traced, easily tracked by the network security department. The hash function is a public function that can map information of any length to a certain fixed length, which has the characteristics of one-way, weak collision resistance, strong collision resistance, etc. The hash value plays a decisive role in the message mining blockchain. Each block (message) has its particular hash value，the hash value changed with the content of the block changes.

3.1.4. Implementation and application

The main process of sensitive information mining:

①Hash generation: The information inspector executes an improved deep learning algorithm locally, grabs documents, and obtains a set of keywords. Then take the timestamp, document collection and keyword collection as input, and get a certain hash index that can be used as output.

②Encryption consensus: asymmetric encryption algorithm technology is used in blockchain, for example, a private key generated during player registration, private key and Secp256k1generate a 65-byte random number in elliptic curve algorithm called a public key, The system takes the public key with SHA256[10] and RIPEMD160Double hashing ,when the player posts information to the game client. Generate summary results with a length of 20 bytes, as the main information, add the version prefix 0X00, and the address check code, and perform two SHA256 operations on the summary result. Take the first four bits of the hash, the version prefix + main body information + check digit is processed by Base58 to obtain the address finally [7], and then uploaded to the cloud server.

③Permission granted: After the control terminal of each district server confirms that the released information is non-sensitive information through the algorithm, it sends the key and related parameters to the data user to grant legal authority (release).

④Data decryption: The decryption algorithm is executed locally by the data user, the key and the encrypted document are set as input, and the output plaintext document set is obtained.

⑤Dynamic update: When the data publisher initiates a document update request to the district server, the message is added or deleted. The confirmation of the original hash and the classification of the newly

ISSN 2616-5775 Vol. 4, Issue 4: 82-88, DOI: 10.25236/AJCIS.2021.040415

generated hash will be dynamically updated, and sensitive vocabulary judgments will be made.

3.2. The characteristics of network sensitive information mining model in the blockchain mode

Blockchain is a new type of decentralized data architecture, which is jointly owned, managed and supervised by all nodes in network, without accepting a single aspect of control. In the blockchain modle, the mining process of sensitive information is equated with the transaction (reporting) behavior between nodes. The specific characteristics of the impact on the network sensitive information-mining model are as follows:

3.2.1. Decentralization of sensitive information mining nodes

The original sensitive information mining is based on player reports or system detection, uploaded to the Tencent network library, confirmed by the game security department, and then processed. The difficulty of confirmation gradually increases with the deformation, rewriting, and multiple expressions of sensitive information. So it is difficult to meet the timeliness requirements of public opinion handling.

The detection method for deformed words is to strengthen the testing of sensitive words by machine learning algorithms, adding the deformed sensitive information into the lexicon to achieve more accurate results, which requires a process of feedback and learning. In the blockchain model, when the sensitive information is authenticated by more than two nodes, the consensus between the nodes will be reached, and then uploaded to the blockchain module, so that the sensitive information quickly discovered by the security department. The overall efficiency of sensitive information mined in the network depends on all nodes in the network, which have mining (reporting) capabilities. Each node records the detected sensitive information, authenticity verification is performed when data is exchanged between nodes. It is determined that belongs to the network sensitive information, when the verification is successful, then the information it receives is submitted to the network security department for identification and shielding, which greatly improves the efficiency of information mining.

3.2.2. Traceability of sensitive information

In the transaction process, each information release (transaction) generated an ID by timestamp mechanism in blockchain technology, which adds a time dimension to the data, the sequence of conversion of sensitive information can be recorded in this way, which making data mining traceable. The continuously generated text information is added to all blocks in the system. The current block is added to the main blockchain when the new block generation conditions are authenticated by all users.Each block uses a hash value generated by a certain algorithm to identify its uniqueness. This process is irreversible. In this way, the evolution process of sensitive information on the network and the future direction can be judged. The time stamp method not only guarantees the originality of the data, but also reduces the cost of mining (transaction) traceability. The immutability of information is strengthened by t time series data. The long-term release of sensitive information sources will attract the attention of the cyber security department of the game company and submit it to the national security department for investigation and processing.

3.2.3. Information publisher identity data encryption and information chain contract

Blockchain uses asymmetric cryptography to encrypt data. Its data encryption can ensure the security of mining (transaction) data in the network and reduce the risk of transaction data loss. If an attacker wants to tamper with certain data, he must modify the data in all blocks. For a mature blockchain, this is impossible to achieve, thus realizing the encryption of mining (transaction). In sensitive data mining under the blockchain model, digital signatures are required when the mining data is disseminated in the network to indicate the identity of the signer and the recognition of the content of the transaction data. The combination of real-name registration and mobile phone registration is required in large-scale social mobile games to ensure the security of the player's identity (trader). The characteristic of blockchain technology is that the smart contract of the automatic guarantee program is set up on the blockchain instead of the server, which greatly improves the efficiency of distributed processing under a large amount of data .The authentication of the personal identity of the information publisher in social online games has been changed from the authentication uploaded to the entire district server to authentication on the blockchain (a server in a specific district), which greatly accelerates the authentication efficiency. Therefore, the outcome of each contract can be predicted by programmable smart contracts. The code contract will be automatically executed when the conditions for contract establishment are met. The content of the information that the node release is predicted according to the initial brief information release and the regularity of the text which the node sending, Early warning and processing before the

ISSN 2616-5775 Vol. 4, Issue 4: 82-88, DOI: 10.25236/AJCIS.2021.040415

release of sensitive public opinion information, and blocking in advance to prevent the source information.

4. Text classification scheme based on deep learning algorithm in data model layer

According to the characteristics of sensitive text information in online games: Thematic texts are expressed in the form of homophonic, split words, etc., so simple statistical methods are difficult to detect, increasing processing accuracy requires the machine learning. This article attempts to apply the deep learning method to the data model layer of the sensitive information mining process in the blockchain mode for the first time.

The deep learning method has three main levels for thematic text operations: text preprocessing, word vector representation and deep learning model. The ability of the learning data characteristics during the training process can be improved by the multi-layer structure of the deep learning model, then realize the approximation of complex functions.

4.1. Text preprocessing

Regardless of whether the text sample used has been marked when training a deep learning model, the text data needs to be preprocessed. Including filtering non-Chinese information (numbers, English letters, punctuation, special symbols, full-width characters, etc.), template extraction (according to specific classification requirements, extracting key information in text samples, and eliminating other information), Text segmentation (the word segmentation algorithm performs matching recognition or tagging training on samples according to a preset dictionary) and de-stop words (filtering some words or words that do not effect on classification).

For example, pornographic information ads were published by someone on a game platform, which was reported by netizens. The summary extraction template is "content + cost + contact information" after filtering non-Chinese; The word segmentation dictionary usually uses the National Language Commission Corpus and Sogou Corpus. User-defined dictionaries are professional words that are not included in general dictionaries. The dictionary in the online game information requires us to build a user-defined dictionary based on actual application scenarios. update at any time. The realization of the deep learning algorithm is: by labeling a large number of Chinese characters and words, machine learning tools are used to recognize words in the text.

4.2. Word vector representation

In order to better recognized and processed by the deep learning model. high-dimensional and high-sparse text samples are needed to be word vector representation after text preprocessing, for to achieve high-quality feature extraction and format conversion. The output of the word vector is a vector matrix containing each word vector, which converts the text data from a high-dimensional and high-sparse encoding method to continuous dense data. This article uses Word2Vec tool.

4.3. TextCNN model

The process of building deep learning classification model:

a) Training process:training classification with sufficient labeled text sample set;

b) Verification process: The classification accuracy of the model is tested by removing labeled text samples. Through multi-round training and optimization of the model, the stability of the classification model is achieved.

In this paper, several text test results of the improved deep learning model are compared with the common naive Bayes text classification results, and the test results are shown in Figure 3.Online dialogue is mainly short text. TextCNN has a strong ability to extract shallow features of text. It has good effect, wide application and fast speed when focusing on intention classification in short text fields (such as search and dialogue fields), and has obvious advantages [17].

The word vector constitutes the text matrix, and the volume kernel size of the filter is 2,3 and 4, respectively. The feature vector is obtained by convolution pooling. The dimension is equal to the number of convolution kernel sizes multiplied by the number of convolution kernels of each size. TextCNN is

ISSN 2616-5775 Vol. 4, Issue 4: 82-88, DOI: 10.25236/AJCIS.2021.040415

divided into four layers.

Convolution layer : In the TextCNN model of this paper, there are three filters (convolution kernel sizes are 2, 3 and 4) that can extract different text features. The filter converts the node matrix with the size of3×3×1 into the unit node matrix. For the node i in the unit node matrix, assuming that the weight of the input node of the filter is represented by , and bi represents the bias parameter corresponding to the i output node, the value of the i node in the unit matrix is :

$$a(i) = f(\sum_{x=1}^{3}\sum_{y=1}^{3} c_{x,y} \times wi_{x,y} + b_i) \quad (1)$$

In model:is the value of the node in the filter. Represents the activation function. The unit vector of all components is the feature map derived from the convolution layer as input to the pooling layer.

Pooling layer: the convergence operation of pooling layer can reduce the dimension, reduce the amount of calculation and the number of parameters, and prevent the occurrence of overfitting.

Fusion layer: The features obtained from three pooling layers are merged into a more representative vector for text vector.

Full link layer: By adding the hidden layer and the final softmax layer after the fusion layer to act as a classifier for the final text classification.

In order to test the performance of TextCNN model on the data set, the experimental data set selects the chat text information of 《King of chaos》 in May 2019. Naive Bayes, CNN and TextCNN are used to classify the data sets. The experimental steps are as follows:

1) Mark and preprocess the short text corpus, perform data cleaning, word segmentation, stop words and other operations;

2) The trained (Chinese) Word2Vec model is used to vectorize the segmentation results;

3) Naive Bayes, CNN and TextCNN are used to classify data sets and calculate their accuracy.

The experimentally verified data table 1 is the chat text information of "The King of Chaos" in May 2019, in which data set 1 contains 14792 training samples, 2324 test samples, and the number of categories is set to 15; data set 2 contains 11487 training samples Bar, test sample 1794, the number of categories is set to 5. The experiment verifies the accuracy of the Naive Bayes and TextCNN models on the two data sets. The verification results are shown in the table 1.Data preprocessing is implemented based on Python SKLearn library, and model training and verification are implemented based on TensorFlow.

Table 1. Comparison results of text classification models

classification model	Training set Number of samples	Test set Number of samples	Number of categories	Accuracy
Naïve-Bayes	14792	2324	15	65.92
CNN	14792	2324	15	66.17
TextCNN	14792	2324	15	69.89
Naïve-Bayes	11487	1794	5	70.56
CNN	11487	1794	5	72.34
TextCNN	11487	1794	5	75.76

5. Conclusions

This paper analyzes the common problems of sensitive information mining in social online games based on the actual data, Combined with the distributed accounting method and decentralized characteristics of blockchain technology, the deep learning algorithm is improved, and the network sensitive information model under blockchain mode is proposed. The data level and control level are decoupled. The data level classification uses TextCNN for feature extraction and text classification. The experimental results show that the network sensitive information model based on block chain model has

ISSN 2616-5775 Vol. 4, Issue 4: 82-88, DOI: 10.25236/AJCIS.2021.040415

strong security and error prevention ability, fast and efficient point-to-point recognition mechanism, which can effectively explore and establish the dictionary of sensitive information in online games, and maintain the characteristics of high efficiency and accuracy. The research and development of accurate and efficient public opinion prevention and control system for online games under the blockchain technology framework can provide the identification, processing and traceability of public opinion data in the whole process of beforehand, during and after the event for network security, which has extensive social needs, high technical feasibility and good application prospects.

References

[1] Internet Network Information Centen , "Statistical Report on China's Internet Development," Beijing, China. Rep. Sep. 2020.
[2] Information Center of China Culture and Entertainment Industry Association, "2019 China Game Industry Development Report," Beijing, China. Rep. Dec. 2019.
[3] Q. Q. Zhang, "Research on Text Sentiment Classification Based on Machine Learning," Ph.D.dissertation. Northwestern Polytechnical Univ.,Xi An,Shan Xi,China, 2016.
[4] Y. Yan, "Research on Text Representation and Classification Method Based on Deep Learning," Ph.D.dissertation. Beijing Science and Technology Univ., Beijing, 2016.
[5] T. T. Liu, W. D. Zhu,and G. Y. Liu, "Research progress of text classification based on deep learning," Electric Power Information and Communication Technology.,2018，16(03):1-7.
[6] W. J. Zhao, "Blockchain technology: development and prospects," National Science Review., vol. 6, no. 02, pp.363-373, Mar.2019.
[7] Z. B. Zheng et al., "Blockchain challenges and opportunities: a survey," Int. J. of Web and Grid Services., vol. 14, no. 4, Mar.2018.
[8] M.T.S.Climent. D.Kraus, T.Obrist etc, Blockchains, Smart Contracts, Decentralised Autonomous Organisations and the Law. European Review of Contract Law,2019,15(4):
[9] Y. D. Liu, H. Q. Zeng, and R. L. Li et al. "Tendency text filtering based on semantic analysis," Journal of Communications., vol. 25, no. 07, pp. 78-85, Jul.2004.
[10] H. Paik, X. Xu, H. M. N. D. Bandara, S. U. Lee and S. K. Lo, "Analysis of Data Management in Blockchain-Based Systems: From Architecture to Governance," IEEE Access, vol. 7, pp. 186091-186107, 2019,
[11] J. G. Samuel,M. B. David, "A tutorial on Bayesian nonparametric models," Journal of Mathematical Psychology., vol. 56, no. 1, pp. 1-30, Feb.2012.
[12] Z. Y. Li, J. F. Zhang,and S. H. Hu , "Incremental support vector machine algorithm based on multi-kernel learning," Journal of Systems Engineering and Electronics., vol. 22, no. 04, pp. 702-706, Aug.2011.
[13] F. R. Shen, Q. B. Ouyang,and W. Kasai, O. Hasegawa.,"A general associative memory based on self-organizing incremental neural network ,"Neurocomputing., vol. 104, pp. 57-61, Jun.2013.
[14] Q. Yang, "Research on Key Technologies of Clustering Based on Deep Learning, " M.S. thesis, Southwest Jiaotong Univ., Xi An,Shan Xi,China, 2016.
[15] T. Wu, "Research and Application of Classification Algorithm Based on Deep Learning,"M.S. thesis,Jilin Univ.,Changchun,Jilin,China, 2016.
[16] P. Y. Lee , S. C. Hui,and A C M Fong et al, "Neural networks for web content filtering," IEEE Intelligent Systems, vol. 13, no. 1, Jun.2003.
[17] J. Y. Li, X.H. Fan,and Y. Wang, "Design of a privacy protection mechanism for sharing economy based on blockchain ," Computer applications and software., vol. 36, no. 01, pp. 296-301, Jan.2019.