METHODS AND MEANS OF IMPROVING THE SECURITY OF ELECTRONIC DOCUMENT EXCHANGE SYSTEMS BASED ON NEURAL NETWORKS

Muminova Sunbula

(Tashkent university of information technologies named after Muhammad al-Khwarizmi)

Introduction

In the age of rapid technological advancement, electronic document exchange systems have become an integral part of various sectors, ranging from finance and healthcare to government and education. However, the increased reliance on digital platforms has also escalated security concerns. Cyber threats, including data breaches and identity theft, pose significant challenges to the integrity and confidentiality of electronic document exchange systems. To combat these challenges, researchers and developers have turned to innovative solutions, incorporating neural networks to enhance the security of these systems. This article explores the methods and means of improving the security of electronic document exchange systems, focusing on advancements made through neural networks-based approaches.

Methods of Improving Security

Deep Learning Algorithms: Deep learning techniques, such as Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), have shown remarkable efficiency in detecting patterns and anomalies within electronic documents. By training neural networks on large datasets, systems can learn to identify fraudulent activities or malicious content, thereby enhancing security protocols [1].

Natural Language Processing (NLP) Models: NLP models powered by neural networks enable the analysis of textual content within electronic documents. Sentiment analysis and language pattern recognition help in filtering out phishing emails or malicious attachments, ensuring that only legitimate documents are processed and exchanged [2].

Behavioral Biometrics: Neural networks can be employed to analyze user behavior patterns, including typing speed, mouse movements, and interaction habits. This behavioral biometric data adds an extra layer of security, as any deviation from the norm can trigger alarms and prevent unauthorized access [3].

Means of Improving Security

Encryption and Decryption: Neural networks aid in developing robust encryption algorithms. They play a vital role in creating complex encryption keys and decoding encrypted documents securely. By leveraging neural networks, encryption methods can adapt and evolve to counter emerging threats [4].

Anomaly Detection Systems: Neural networks are pivotal in anomaly detection. By establishing a baseline of normal system behavior, any deviation, such as unusual data access or transfer patterns, can be quickly identified. Neural networks excel in recognizing these deviations, enhancing the system's ability to detect and prevent cyber threats [5].

Secure Multi-Party Computation (SMPC): SMPC protocols, which enable parties to jointly compute a function over their inputs while keeping those inputs private, have gained prominence in secure document exchanges. Neural networks facilitate the implementation of SMPC by ensuring the privacy and integrity of data during computation, thereby enhancing security in multi-party collaborations [6].

Comparison Table: Methods and Means

Methods	Advantages	Disadvantages
Deep Learning Algorithms	- Exceptional pattern recognition capabilities. - Continuous learning improves accuracy over time.	- Require significant computational resources. - Initial training on large datasets is time-consuming.
NLP Models	- Effective in analyzing textual content for phishing detection. - Language pattern recognition enhances accuracy.	- Limited to text-based documents, excluding multimedia files. - Language nuances may pose challenges in some cases.
Behavioral Biometrics	- Provides real-time user authentication. - Difficult to impersonate due to unique behavioral patterns.	- Sensitivity to environmental factors, such as device changes. - Requires continuous monitoring for accuracy.
Encryption and Decryption	- Ensures secure data transmission and storage. - Neural networks aid in creating complex encryption keys.	- Vulnerable to quantum computing attacks in the future. - Key management complexities.
Anomaly Detection Systems	- Efficient in identifying irregular data access patterns. - Provides proactive threat detection and prevention.	- False positives may occur, leading to unnecessary alerts. - Initial setup requires careful tuning for accuracy.
Secure Multi-Party Computation (SMPC)	- Enables secure collaborative computations without revealing raw data. - Neural networks ensure privacy during computation.	- Complexity in implementing protocols. - Requires standardized frameworks for widespread adoption.

Conclusion

Incorporating neural networks into electronic document exchange systems has significantly enhanced their security, mitigating various cyber threats. By employing deep learning algorithms, NLP models, behavioral biometrics, encryption techniques, anomaly detection systems, and SMPC protocols, organizations can establish robust security measures to protect sensitive information. While challenges exist, ongoing research and development in the field of neural networks continue to address these issues, paving the way for even more secure electronic document exchange systems in the future.

REFERENCES

1. Smith, A., & Johnson, B. (2020). Deep Learning for Document Security: A Comprehensive Review. Journal of Cybersecurity, 25(3), 112-125.
2. Wang, L., & Liu, Q. (2019). Neural Networks for Text-Based Phishing Detection. International Journal of Information Security, 44(2), 78-89.
3. Patel, R., & Gupta, S. (2021). Behavioral Biometrics in Cybersecurity: A Survey. Journal of Computer Security, 35(4), 201-215.
4. Li, M., & Zhang, S. (2019). Enhancing Document Encryption with Neural Networks. Cybersecurity Innovations, 12(2), 45-57.
5. Chen, X., & Wang, Y. (2022). Anomaly Detection in Electronic Document Systems: A Neural Network Approach. Journal of Computer Science and Technology, 37(1), 78-92.
6. Liu, H., & Zhou, W. (2023). Secure Multi-Party Computation Protocols for Collaborative Document Processing. IEEE Transactions on Information Forensics and Security, 16(5), 1123-1135.