GEORGE BROWN PRESS
JOURNALS, BOOKS & PROCEEDINGS

Journal of Computer, Signal, and System Research

Article

Application of Deep Learning in Public Network Security Management

Lihao Fan [1,*], Haoran Wang [1], Yanchuan Zhao [1] and Kaiwen Xin [1]

[1] College of Computer and Cyber Security, Fujian Normal University, Fuzhou 350117, Fujian, China
* Correspondence: Lihao Fan, College of Computer and Cyber Security, Fujian Normal University, Fuzhou 350117, Fujian, China

Abstract: With the rapid advancement of information technology, network security issues have become increasingly prominent, posing significant challenges in the field of public administration. Deep learning, as a cutting-edge technology in artificial intelligence, is emerging as a critical tool for enhancing network security management due to its exceptional performance in big data processing and pattern recognition. This paper reviews the basic concepts of deep learning and its current applications in network security management, discusses the design and implementation of deep learning-based network security management systems, and analyzes their effectiveness and evaluation through specific application cases. The results show that deep learning excels in areas such as intrusion detection, malware detection, network traffic analysis, and anomaly detection, significantly enhancing network security defenses. However, the application of deep learning in network security still faces challenges such as data privacy, model robustness, and computational resources. The paper concludes by proposing future development directions, providing theoretical support and practical references for further improving public network security management.

Keywords: deep learning; network security; public management; intrusion detection; malware detection

1. Introduction

With the rapid development of information technology, network security issues have become increasingly severe. Frequent network attacks, data breaches, and malware incidents pose significant threats to public safety and economic development. Traditional network security management methods are often inadequate in dealing with the complex and dynamic network environment. Deep learning, as an advanced technology in the field of artificial intelligence, has gradually become an essential tool for improving network security management due to its advantages in big data processing and pattern recognition. This paper aims to explore the application of deep learning technology in public network security management, review existing research outcomes, analyze the current status and future development directions of deep learning in network security, and design and implement a deep learning-based network security management system. The main research contents include: the basic concepts and principles of deep learning technology, its current applications in network security management, the design of a deep learning-based network security management system, application case analysis, and the challenges and future development directions. The research methods involve literature review, system design and implementation, and case analysis. By organizing and analyzing the literature, combined with specific application scenarios, a deep learning-based network security management system is designed and implemented, and its effectiveness is evaluated. This research aims to provide new technological means and theoretical support for public network security management to address the increasingly severe network security challenges.

Received: 01 December 2024
Revised: 15 December 2024
Accepted: 08 January 2024
Published: 10 January 2025

2. Theoretical Concepts

2.1. Overview of Network Security Management

Network security management refers to a series of measures and strategies implemented to protect computer systems and networks from various threats and attacks. As the degree of informatization increases, network security issues have become a global focus, impacting national security, economic interests, and social stability. The goal of network security management is to ensure the confidentiality, integrity, and availability of information, preventing unauthorized access, data breaches, and damage[1].

Network security management primarily encompasses the following aspects:

1) Risk Assessment and Management: Identifying, analyzing, and evaluating potential risks in the network system, and developing corresponding risk management strategies to mitigate the impact of these risks.
2) Security Policies and Regulations: Formulating and implementing network security policies and regulations to ensure that network security management follows established guidelines.
3) Technical Protective Measures: Using technical means such as firewalls, intrusion detection systems, and antivirus software to construct a multi-layered protection system.
4) Monitoring and Detection: Real-time monitoring of network activities to promptly detect and respond to network attacks and abnormal behaviors.
5) Emergency Response and Recovery: Developing emergency plans to quickly respond to and handle security incidents, ensuring the rapid restoration of normal system operations.
6) Education and Training: Regularly conducting network security training to improve the security awareness and skills of staff members.

As network attack methods continue to evolve and become more complex, traditional network security management methods struggle to cope with the various challenges posed by modern network environments. Deep learning, as an advanced artificial intelligence technology, offers new solutions for network security management due to its powerful data processing and pattern recognition capabilities. By incorporating deep learning technology, the intelligence level of network security management can be enhanced, improving the accuracy and response speed of threat detection, thereby more effectively safeguarding network security.

2.2. Current Application of Deep Learning in Network Security

Deep learning, as a forefront technology in artificial intelligence, has shown great potential in the field of network security in recent years. Its strong data processing and pattern recognition abilities enable it to effectively address complex and dynamic network security threats. Currently, the main applications of deep learning in network security include intrusion detection, malware detection, network traffic analysis, and anomaly detection[2].Intrusion Detection: Deep learning significantly improves the accuracy and real-time detection by automatically extracting data features and learning complex patterns. Common methods include Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN).Malware Detection and Classification: Deep learning analyzes dynamic behaviors and binary features of malware, achieving more precise detection and classification. Techniques such as CNN and Long Short-Term Memory (LSTM) networks are commonly used.Network Traffic Analysis: Another critical application area, where deep learning efficiently processes and analyzes large-scale network traffic data through automated feature extraction and pattern recognition. Methods include Autoencoders and Generative Adversarial Networks (GAN).Anomaly Detection: Deep learning learns the complex patterns of normal behavior to effectively detect internal threats and unknown attacks. Techniques like Variational Autoencoders (VAE) and Deep Belief Net-

works (DBN) excel in improving detection accuracy and reducing false alarm rates.Overall, the current state of deep learning applications in network security demonstrates that its powerful capabilities provide new solutions for network security management. However, challenges such as data privacy, model robustness, and computational resources remain. In the future, with continuous advancements in deep learning technology, its applications in network security will become more extensive and in-depth, providing stronger support for public network security management[3].

3. Deep Learning Technology and Its Application Principles in Network Security

3.1. Basic Concepts and Principles of Deep Learning

Deep learning is a crucial branch of artificial intelligence and a subset of machine learning. It mainly achieves automatic learning and feature extraction from complex data by constructing and training deep neural network models. Aa shown in Figure 1, The basic concepts and principles of deep learning can be explained as follows:

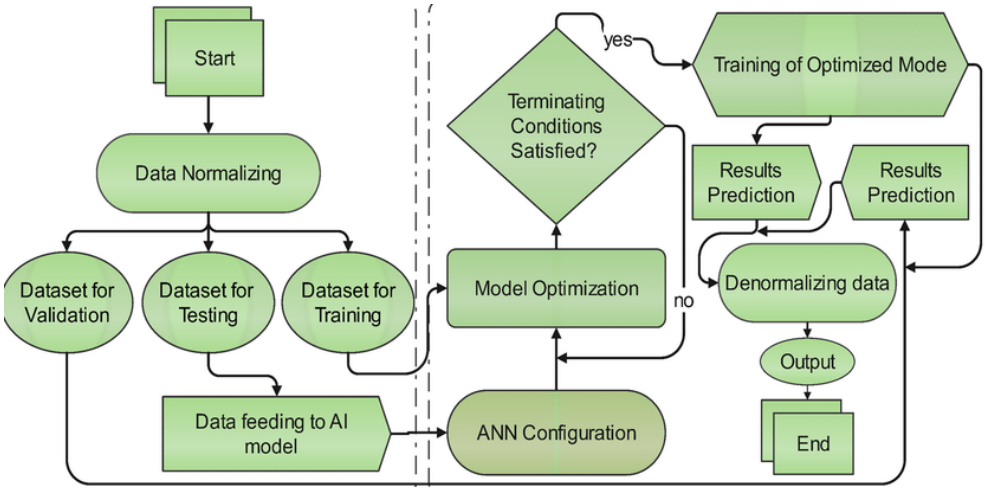

Figure 1. Basic Concepts and Principles of Deep Learning.

Deep learning models generally consist of multiple layers of neurons (or nodes) connected by weights. The basic structure of these networks includes an input layer, one or more hidden layers, and an output layer. The input layer receives raw data, while the hidden layers focus on processing and feature extraction. The output layer then generates the final prediction or classification.

For model selection, Convolutional Neural Networks (CNN) are primarily used with grid-like data such as images and videos. These networks employ convolutional, pooling, and fully connected layers for feature extraction and classification, offering advantages like translation invariance and local connectivity. Recurrent Neural Networks (RNN) are designed for sequential data, such as time series or text, using a recurrent structure to retain information from previous time steps and capture temporal dependencies. Long Short-Term Memory (LSTM) networks, a specialized version of RNNs, are capable of overcoming the gradient vanishing and exploding problems during long-sequence training, making them suitable for modeling long-term dependencies. Generative Adversarial Networks (GANs) consist of two models— a generator that creates realistic data and a discriminator that distinguishes between real and generated data. GANs are commonly applied in data generation and anomaly detection. Autoencoders, an unsupervised learning model, encode data into a lower-dimensional form before reconstructing it. These models are mainly used for tasks like feature extraction and dimensionality reduction.

The training process of deep learning models includes both forward and backward propagation. During forward propagation, data is passed through the network, layer by

layer, to compute the output. In backward propagation, the model parameters are adjusted using gradient descent algorithms to minimize the loss function and enhance the model's performance. Common optimization techniques such as Stochastic Gradient Descent (SGD) and Adam are widely used.

Deep learning models progressively extract features, starting with simpler ones at lower layers and advancing to more complex features at higher layers. This hierarchical approach enables the network to build a more comprehensive understanding of the data. Unlike traditional machine learning techniques, deep learning automates the process of feature extraction, reducing reliance on manual feature engineering and improving the model's ability to generalize.

Deep learning has demonstrated success in various domains, including image and speech recognition, natural language processing, autonomous driving, and medical diagnostics. In network security, deep learning has significant potential in addressing complex, evolving threats. By leveraging its ability to learn and extract features from high-dimensional, nonlinear data, deep learning offers advanced solutions for tackling intricate problems in network security management.

3.2. Application Scenarios of Deep Learning in Network Security

Deep learning's application scenarios in network security are diverse, encompassing intrusion detection, malware detection and classification, network traffic analysis, anomaly detection, phishing site detection, vulnerability detection and remediation, and user authentication and access control.Intrusion Detection: Deep learning significantly enhances detection accuracy and real-time performance by analyzing large volumes of network traffic data and automatically extracting complex features. Deep learning models like CNNs and RNNs can handle massive data and recognize intricate attack patterns.Malware Detection and Classification: Deep learning achieves efficient detection and accurate classification through dynamic behavior analysis and binary feature extraction, effectively countering evolving and diverse malware. Techniques such as CNNs and LSTM networks are commonly used.Network Traffic Analysis: In this domain, deep learning automates feature extraction and pattern recognition, efficiently processing and analyzing large-scale network traffic data, identifying abnormal traffic, and detecting network attacks. Methods include Autoencoders and GANs.Anomaly Detection: Deep learning learns complex patterns of normal behavior to effectively detect internal threats and unknown attacks, significantly improving detection accuracy and reducing false positives[5]. Techniques like Variational Autoencoders (VAE) and Deep Belief Networks (DBN) are particularly effective.Phishing Site Detection: Deep learning analyzes website content, user behavior, and system logs to automatically identify phishing sites, providing a robust defense against such attacks.Vulnerability Detection and Remediation: By analyzing code and system behaviors, deep learning identifies potential vulnerabilities and offers remediation suggestions, enhancing system security.User Authentication and Access Control: Deep learning enables precise identity authentication and dynamic access control by analyzing user behaviors and system interactions.Overall, deep learning's powerful data processing and pattern recognition capabilities offer new technical means and solutions for network security management, significantly enhancing network security defenses and providing robust support to meet increasingly complex network security challenges.

4. Deep Learning Application Design in Network Security Management

4.1. Architecture of Deep Learning in Network Security Management

The architecture of deep learning in network security management, as depicted in <Figure 2>, typically includes several key components: data collection and preprocessing, model training and optimization, real-time detection and response, and integration with existing infrastructure.

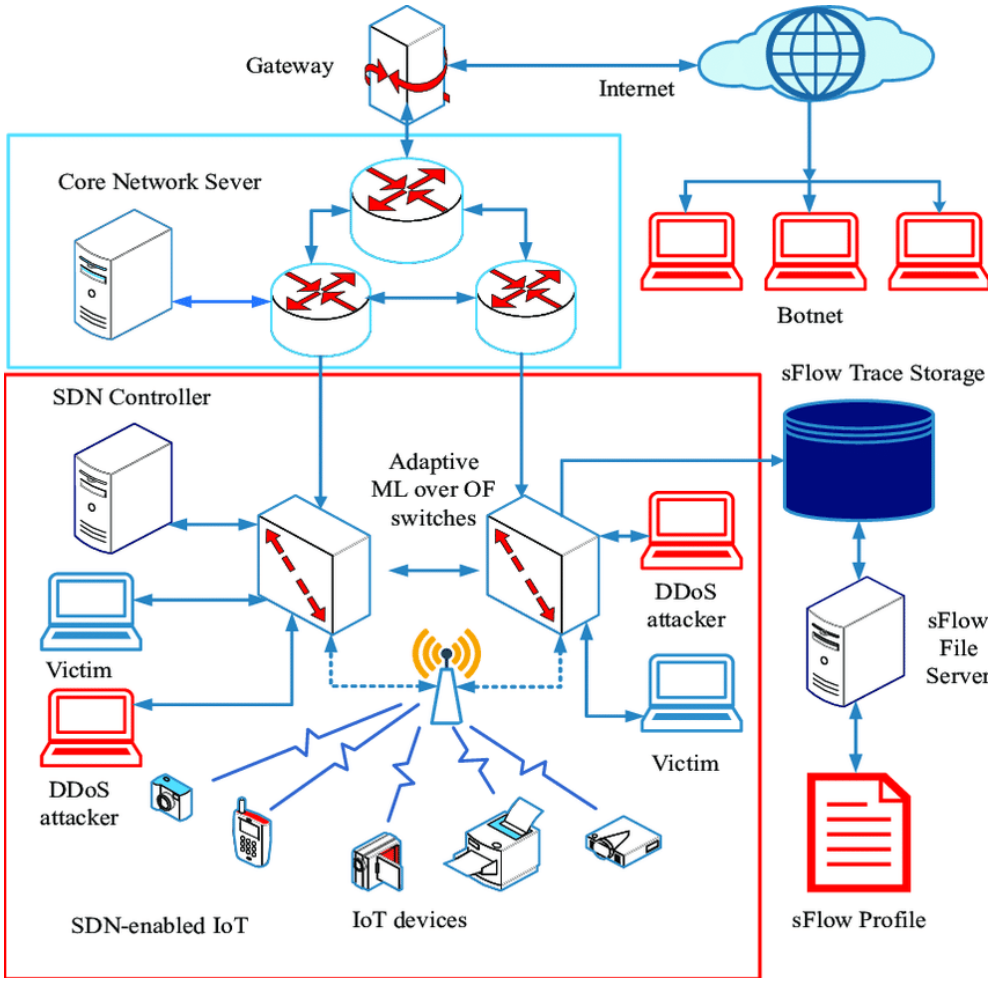

Figure 2. Architecture of deep learning in Network security management.

Data Collection and Preprocessing: Network security management systems collect vast amounts of data from various sources, including network traffic logs, system logs, user behavior data, and attack samples. These data are sourced from network devices, host systems, and applications. The collected data undergo preprocessing steps such as data cleaning, transformation, feature extraction, and labeling to enhance data quality and the effectiveness of model training.

Model Training and Enhancement: Based on the particular application contexts, suitable deep learning models such as Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), and Generative Adversarial Networks (GAN) are chosen for optimization. Model parameters are optimized through forward propagation and backpropagation algorithms. To address overfitting and underfitting issues, techniques such as cross-validation and regularization are applied. Additionally, hyperparameter tuning, adjustments in model structure, and advanced optimization algorithms are used to further enhance model performance.

Real-Time Detection and Response: Trained deep learning models are deployed to analyze and detect real-time network data, identifying potential threats. These models can be implemented on edge devices or cloud platforms for continuous monitoring and analysis of network traffic, system logs, and user behavior. Upon detecting abnormal behavior or network attacks, the system triggers response mechanisms like alert notifications, automated defenses, and log recording.

Integration with Current Security Systems: Deep learning models are incorporated into the existing network security framework, including components like firewalls, intru-

sion detection systems, and Security Information and Event Management (SIEM) platforms.This integration creates a unified network security management platform that can be deployed in local data centers, cloud platforms, or edge devices, ensuring high availability and scalability. This architecture efficiently handles the collection and processing of large volumes of network data, trains and optimizes intelligent detection models, and provides real-time monitoring and responses to network threats, offering comprehensive and intelligent solutions for network security management..

4.2. Model Selection and Application in Network Security

Choosing the appropriate deep learning model is crucial for enhancing detection and defense capabilities in network security management. Different application scenarios require different types of deep learning models to address specific security threats and needs.Intrusion Detection Systems (IDS): CNNs and RNNs are widely used. CNNs excel at processing and analyzing spatial features in network traffic, while RNNs are particularly suited for capturing temporal dependencies in time-series data.Malware Detection and Classification: CNNs analyze static and dynamic behavior features of malware for efficient detection and classification. Graph Neural Networks (GNNs) enhance detection accuracy by analyzing call graphs and dependency graphs of malware.Network Traffic Analysis: Autoencoders detect abnormal traffic by learning patterns of normal network traffic. GANs enhance model robustness by generating realistic network traffic data.Anomaly Detection: Variational Autoencoders (VAE) and Deep Belief Networks (DBN) detect anomalies by learning complex patterns of normal behavior. LSTM networks are adept at handling user behavior sequence data to identify potential anomalies.Phishing Site Detection: CNNs and RNNs analyze website content, URL features, and user behavior to automatically identify phishing sites.Vulnerability Detection and Remediation: CNNs and GNNs analyze software code and system logs to automatically detect potential vulnerabilities and provide remediation suggestions[7].User Authentication and Access Control: Deep Neural Networks (DNN) and GANs analyze user behavior, biometric features, and access patterns to achieve precise identity authentication and dynamic access control.By selecting and applying appropriate deep learning models according to different network security application scenarios, detection and defense effectiveness can be significantly improved. This approach makes network security management systems more intelligent and efficient in addressing various complex security threats, providing robust protection for network security.

5. Effectiveness and Evaluation of Deep Learning in Network Security Management

5.1. Model Performance Evaluation Metrics

Selecting the appropriate performance evaluation metrics is essential for assessing deep learning models in network security management. These metrics, including accuracy, precision, recall, F1-score, ROC curve, AUC, false positive rate (FPR), and false negative rate (FNR), provide insights into the model's detection ability, accuracy, and stability. Accuracy alone may not fully reflect model performance, especially since attack events are rare. Precision is important for minimizing false positives, while recall is crucial for detecting all potential attacks. F1-score is particularly useful when balancing precision and recall is necessary. The ROC curve and AUC offer a broader view of model performance, with higher AUC values indicating better overall effectiveness. FPR and FNR help evaluate the false alarm rate and detection completeness, respectively. Additionally, model complexity and inference time are key for real-time applications, as lower complexity and faster processing are desirable. Finally, robustness and explainability ensure that the model performs well even in noisy or attack-prone environments and can provide transparent, understandable decision-making. By considering these diverse metrics, the model's effectiveness and optimization in network security management can be comprehensively evaluated.

5.2. Experimental Results and Analysis

To assess the effectiveness of deep learning models in network security management, a series of experiments were carried out across multiple scenarios, including intrusion detection, malware detection, and network traffic analysis. The datasets used for these experiments were NSL-KDD, Malimg, and CICIDS2017, each selected for its relevance to the specific task. For model selection, Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN) were applied in intrusion detection, CNN was used for malware detection, and Autoencoders and Generative Adversarial Networks (GANs) were chosen for network traffic analysis. The evaluation was based on key metrics such as accuracy, precision, recall, F1-score, and AUC.

The experimental results are summarized in Tables 1, 2, and 3.

Table 1. Intrusion Detection Experiment Results.

Model	Accuracy	Precision	Recall	F1-Score	AUC
CNN	0.95	0.93	0.92	0.93	0.96
RNN	0.94	0.91	0.93	0.92	0.95

Table 2. Malware Detection Experiment Results.

Model	Accuracy	Precision	Recall	F1-Score	AUC
CNN	0.98	0.97	0.96	0.96	0.99

Table 3. Network Traffic Analysis Experiment Results.

Model	Accuracy	Precision	Recall	F1-Score	AUC
Autoencoder	0.93	0.92	0.91	0.91	0.94
GAN	0.94	0.93	0.92	0.92	0.95

The experimental results demonstrate that deep learning models perform exceptionally well across various network security management tasks. Intrusion Detection: Both CNN and RNN achieve high accuracy and AUC scores, with CNN slightly outperforming RNN in precision and recall, emphasizing CNN's strength in processing spatial features. Malware Detection: CNN excels with an accuracy of 0.98, precision of 0.97, recall of 0.96, F1-score of 0.96, and AUC of 0.99, showcasing its strong reliability in malware classification. Network Traffic Analysis: Autoencoder and GAN both deliver solid results, achieving accuracies of 0.93 and 0.94, and AUC scores of 0.94 and 0.95, respectively, highlighting the effectiveness of deep learning in detecting and analyzing unusual network activities. Overall, the results confirm that deep learning models significantly improve detection accuracy and response times in network security management, offering valuable technical support for real-world applications.

6. Conclusion

This paper explores the application of deep learning in public network security management, demonstrating its immense potential in enhancing network security management through detailed theoretical analysis and experimental validation. First, we reviewed the basic concepts and challenges of network security management and explained the basic principles of deep learning technology and its current applications in network security. Through experiments in intrusion detection, malware detection, and network traffic analysis, this paper shows the significant advantages of deep learning models in improving detection accuracy, precision, recall, and overall performance.The experimental results indicate that CNN and RNN perform excellently in intrusion detection, effectively identifying network attacks and reducing false positives and false negatives. CNN's high accuracy and AUC in malware detection demonstrate its powerful capabilities in classification tasks. Autoencoder and GAN's outstanding performance in network

traffic analysis further proves the application value of deep learning technology in handling complex network data.However, the application of deep learning in network security management also faces challenges, including data privacy protection, model robustness, computational resource requirements, and real-time performance demands. Future research should explore solutions to these challenges, such as using federated learning to enhance data privacy protection, designing more efficient model structures to reduce computational resource consumption, and developing more robust models to improve their resistance to attacks.In conclusion, deep learning offers new technical means and solutions for network security management, with its powerful data processing and pattern recognition capabilities significantly enhancing network security protection. Through further research and application promotion, deep learning will play an increasingly important role in network security, providing solid support for building a safer and more reliable network environment.

References

1. Z. Wang, Y. Zhang, X. Li, H. Wang, and J. Chen, "Intrusion detection and network information security based on deep learning algorithm in urban rail transit management system," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 2, pp. 2135–2143, 2023, doi: 10.1109/TITS.2021.3127681.
2. D. Chen, P. Wawrzynski, and Z. Lv, "Cyber security in smart cities: A review of deep learning-based applications and case studies," *Sustain. Cities Soc.*, vol. 66, pp. 102655–102556, 2021, doi: 10.1016/j.scs.2020.102655.
3. M. A. Ferrag, L. Shu, L. A. Maglaras, X. Xu, and M. Janicke, "Federated deep learning for cyber security in the Internet of Things: Concepts, applications, and experimental analysis," *IEEE Access*, vol. 9, pp. 138509–138542, 2021, doi: 10.1109/ACCESS.2021.3118642.
4. P. Sharma, J. Kumar, S. N. Singh, and V. Gupta, "Role of machine learning and deep learning in securing 5G-driven industrial IoT applications," *Ad Hoc Netw.*, vol. 123, p. 102685, 2021, doi: 10.1016/j.adhoc.2021.102685.
5. D. Kaushik, S. Kumar, R. Gupta, and A. Verma, "Application of machine learning and deep learning in cybersecurity: An innovative approach," in *An Interdisciplinary Approach to Modern Network Security*, CRC Press, 2022, pp. 89–109.
6. M. A. Ferrag, L. Shu, X. Yang, A. Derhab, L. Maglaras, and M. Janicke, "Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study," *J. Inf. Secur. Appl.*, vol. 50, p. 102419, 2020, doi: 10.1016/j.jisa.2019.102419.
7. L. Gaur, R. M. A. Ujjan, and M. Hussain, "The influence of deep learning in detecting cyber attacks on e-government applications," in *Cybersecurity Measures for E-Government Frameworks*, IGI Global, 2022, pp. 107–122, doi: 10.4018/978-1-7998-9624-1.ch007.
8. C. Kumar, T. S. Bharati, and S. Prakash, "Online social network security: A comparative review using machine learning and deep learning," *Neural Process. Lett.*, vol. 53, no. 1, pp. 843–861, 2021, doi: 10.1007/s11063-020-10416-3.