JOURNAL OF ARTIFICIAL INTELLIGENCE AND ROBOTICS
Jul-Sep 2025, VOL. 2, ISSUE 3, pp. 25-30
https://doi.org/10.61577/jaiar.2025.1000014

RESEAPRO JOURNALS

ORIGINAL ARTICLE

OPEN ACCESS

A phishing recognition framework leveraging web page code and textual features using recurrent neural network (RNN) algorithm

J.A. Benya[1] and K.O Nasirudeen[2]

[1] Department of Computer Science, Institute of Media Studies (IMS) College of Innovation and Computing Technology, Summit University, Offa, Nigeria

[2] Department of Computer Science, Al-Ikmah University, Ilorin, Nigeria

ABSTRACT

Phishing detection focusses on identifying one of the most common and emerging forms of cybercrime exploits user in a fake form. Manual detection strategies do not dynamic phishing attacks, particularly when criminals understand web page structures and textual content. To solve this problem, this research proposes a phishing recognition framework leveraging web page code and textual features using Recurrent Neural Network (RNN) technique in global phishing discovery that uses web page code and textual content. By adding structural attributes of code in HTML with meaning representations of textual content, the design effectively trains sequential dependencies and contextual relationships that differentiate phishing pages from lawful page. Experimental evaluation using benchmark phishing data shows that the proposed RNN-based framework performs better than (ML) Analysis. The investigations show the potential of (DL) models in improving web security, offering a scalable and strong solution for phishing detection software across diverse global cyber communities.

KEY WORDS

Phishing detection; Recurrent neural networks (RNN); Web page code analysis; Text feature extraction; Cyber security; Deep learning

ARTICLE HISTORY

Received 03 July 2025;
Revised 25 July 2025;
Accepted 06 August 2025

Introduction

Phishing websites are common cyber threat that attacks both individual and organizations in this present generation. Attackers use different strategies like fake emails, social engineering and harmful hyperlink to deceive the victims in order to carry out their Scams. The fake websites resemble the real websites and deceive the users into sharing sensitive credentials data through the user's password or financial details [1].

Cyber attackers use modern methods to distort communication, always using malware and phishing methods, intending to steal important data, emphasizing the justification of serious cyber threat methods and increased client awareness to guarantee the internet's ongoing benefits while reducing the related risks. These lead to serious information by tracking client's phishing sites. The procedures of web page phishing are usually conducted in a typical manner. The attackers send out link that mimics the normal web and watches for victims. When a user falls for the phishers threats and believes the mimicked page, the attacker is successful; the phisher targets the user to steal the credentials of the victim.

Detecting websites phishing is crucial for protecting sensitive data like personal information and financials details. It helps to maintain trust and good reputation for both industrial and individuals from cyber attackers [2].

Furthermore, phishing websites leverage an advantages of security alerts like File Transfer protocol, Hypertext Transfer Protocol Secure (HTTPS) and a green lock, making the situation a problem for the clients to differentiate between legitimate and illegitimate websites [2].

Phishing is one of the common to cybersecurity by exploring the credentials clients' credentials ignorantly and surrender their personal data. (RNNs) have gained recognition as powerful tools for detecting cyber-attacks [3].

The capabilities of RNN in the previous research was used for enhancing the performance of phishing websites discovery systems in terms of robustness, flexibility and accuracy. The study proposes a novel model for identifying phishing within the context of RNN framework compare to traditional classification methods by using web content [4].

Cyber-attacks have posed significant threats to organization and individuals which leads to financial losses and less reliance and absolute trust on online communications. These attacks leverage system vulnerabilities and human mistakes which the attacker used to gain access. Organization and individuals must be vigilant of the current nature of cyber attacks and implement effective necessary measures to alleviate the impact of the phishing attacks [5].

Problem Statement

Phishing attack persists as a major challenge in cyber security, using deceptive web page structures and confusing textual content to steal critical client's credentials. Based on the deployment of numerous detection models, that characterize sophisticated phishing methods. These challenges are further compounded in a global context, where difference in web design, and linguistic diversity, and evolving criminals' strategies reduce the accuracy and generalizability of existing solutions, Furthermore, there is a need for higher detection

***Correspondence:** Dr. J.A. Benya, Department of Computer Science, Institute of Media Studies (IMS) College of Innovation and Computing Technology, Summit University, Offa, Nigeria, e-mail: benya.jamiu@summituniversity.edu.ng

models capable of learning sequential and contextual dependencies within both web page source code and textual content to encourage the robustness, scalability, and adaptability.

Aim of the Research

The aim of this study is to develop a phishing recognition framework leveraging web pages code and textual features using recurrent neural network technique for enhancing robustness, accuracy and flexibility.

Objectives

- To gather and preprocess benchmark phishing and genuine web datasets, capturing both HTML code structures and textual content.
- To design a RecurrentNeural Network (RNN) based model capable of learning sequential and contextual dependencies from the integrated features.
- Model Optimization and Performance Enhancement.
- Model evaluation using standard metrics.

Literature Review

Phishing is a cyberattack where attackers impersonate big organizations to gain access to client's confidential personal data. Phishing has emerged as one of the major current era caused by existence of internet and dependent on online transactions which led to significant rise in phishing attacks [3].

In another study explored on protecting and saving sensitive datasets from being used legitimately has become a problem task. Small safeguarding data can be exploited by phishing attacks to expose sensitive data such as passwords or financial credentials data to an attacker. Phishing has now proven so successful, that it is the most attacker vector [6].

In a related development, posited a rapidly rising in cyberspace, The author declared that phishing attacks have caused a considerable financial damage on organizations and individuals. The attackers use different strategies to steal sensitive data through fraudulent websites, emails and instant messages [7].

In similar research by proposed a framework for detecting genuine and phishing URLs by using the data containing spyware and malwares. Furthermore, Pharming Universal Resources Locator sourced from the open-source Phish Tank site available in the formats like JSON, CSV, and XLS which are incorporated into the dataset [7].

Furthermore, proposes Internet has opened up new opportunities, it has also led to a rise in cyber-attacks. One common and serious threat is phishing, where attackers uses confusing link to explore important data from the users. This research addresses pharming Challenges introducing a higher identifying system that actually focuses on HTML content. The contribution extends to establishing an up-to-date dataset, which were openly share with the community [8].

Another contributor presents a study on web phishing detection using five ML classifiers. The research explored the Phish Tank dataset of 3000 URLs. In addition, Ahammad et al, provided detailed analysis of URLs recognition using ML techniques. At the feature selection stage of the ML pipeline, Recursive Feature Elimination (RFE) can be used to remove the redundant from the datasets. Datasets were acquired from Phish Tank and Alexa data. Among the evaluated models, Random Forest classifier performed best than others model with an accuracy of 97.5% in a cloud environment [9].

In a related study, Jain presented an improved approach for detecting web Phishing pages with Machine Learning algorithms. The work used an effective feature of ensemble algorithms to identify Zero-Day attack and utilized the Alexa datasets. The model used five ML classifiers, and the Random Forest classifier achieving the highest accuracy of 93.85% [9].

A similar work explores by architecture of the proposed model comparing data collection, data preprocessing, feature extraction [9]. deep learning classifiers, optimization and performance evaluation as illustrated in figure 3. Acquisition of datasets module collects data from different sources and organizes it into primary dataset. The data collected is cleaned and preprocessed, then key features are extracted, Deep learning algorithms with an optimization technique are used to develop the framework for evaluating performance in detecting planning attacks, as shown in figure 1.

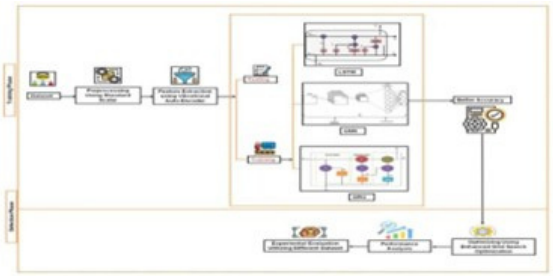

Figure 1. Proposed model.

proposes the sample URL image represents the structure of a simple URL, the actual URLs an have a significantly morre complex organization as shown in the figure 2. Domain experts can identify features which includes path, domain name, top level domain, second level domain, subdomainand protol. The research combines expert knowledge with a machine learning features engineering algorithm [10].

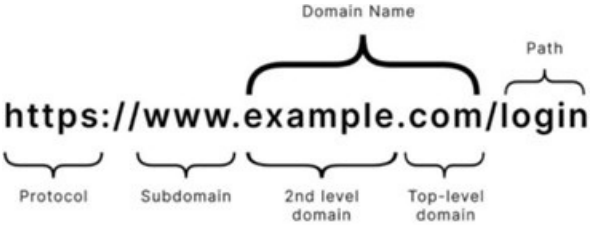

Figure 2. Simple URL example breakdown which includes the protocol, subdomain, second-level domain, domain name, top-level domain and path.

In addition, Proposes Phishing URLs that are commonly used by online fraudsters to trick the users into clicking or visiting fraudulent web pages that imitates genuine web and appear almost similar [11]. This deception succeeds because users do not verify the URLs very well due carelessness or ignorant. Attackers misled the users with convincing fraudulent pages by duplicating authentic websites, as shown in Figure 3 below.

https://doi.org/10.61577/jaiar.2025.1000014

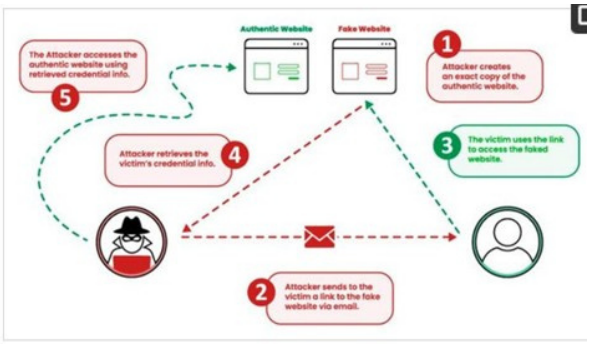

Figure 3. Pharming websites sample.

Phishing websites and legitimate ones are similar; attackers replicate legitimate sites with high precision and making it difficult for users to differentiate between the two sites [12].

Methodology

This section translates theoretical foundations of cybercrime, information security, and sequential learning into a practical framework for phishing detection. Given that phishing attacks exploit both structural manipulation of web pages and semantic deception [13]. The research proposes a Recurrent Neural Network (RNN) based model that integrates webpage source code and textual content features into a unified deep learning framework. The methodology is broken down into four key phases, including capturing both HTML code structures and textual content into structured sequential data suitable for designing an RNN model, RNN based model design, model optimization and performance enhancement, and model evaluation and combative analysis [14].

System analysis and design

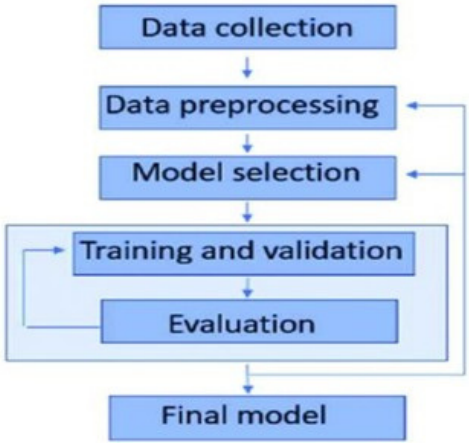

Figure 4. RNN-based model workflow diagram.

This proposed model adopts the qualitative experimental research design to develop and evaluate a Recurrent Neural Network (RNN) based on phishing detection framework. Figure 4 shows the model of Webpage HTML code and text content features that were used to detect phishing websites.

The methodology structures are:

Data acquisition

The data collected contains both legitimate and phishing websites collected from publicly available and reliable cybersecurity repositories like Phish Tank and Open Phish, which monitor and report verified phishing URLs. Furthermore, the legitimate website samples are gathered from Alexa Internet rankings. The dataset is balanced to ensure equal representation of phishing and genuine samples in order to reduce classification bias, avoid data memorization and improve model reliability.

The PhishTank and OpenPhish provide real-time verified phishing URLs and OpenPhish maintained curated phishing URLs dataset. The total datasets include 5,000 samples of 3,000 phishing websites and 2,000 legitimate websites. The datasets are balanced between the HTML code and Textual datasets in Table 1.

Table 1 . Demographic details of the phishing datasets.

Data source	Legitimate URLs	Phishing URLs
PhishTank	1,600	2,000
OpenPhish	400	1,000
Total	2,000	3,000

Data preprocessing

The raw web data are transformed into structured sequential formats suitable for RNN training processing. The websites HTML codes undergo processing to extract the structure elements like <iframe>, <label>, <input>, <form> and <script> tags. These HTML tags are tokenized and converted into ordered sequences to preserve structure dependencies. The tags were tokenized and normalized to get the structure that will make training to be easy for a recurrent neural network.

The concept of "automated gatekeeping" has emerged to describe how algorithms rather than editors now control what information reaches the public [15]. This shift in power dynamics has profound implications for democratic discourse, especially when commercial or political interests influence algorithmic design.

Model selection

The selection strategy enables the RNN model to identify phishing websites more effectively than shallow learning methods.

The RNN variants are:

Input layer : Receives each element of the sequence at a time.

Hidden layer : This is the core area of the RNN model where the data learn the hidden pattern in datasets rather than memorizing the data.

Output layer : The model generates a prediction and classification based on the current hidden station learned by the model.

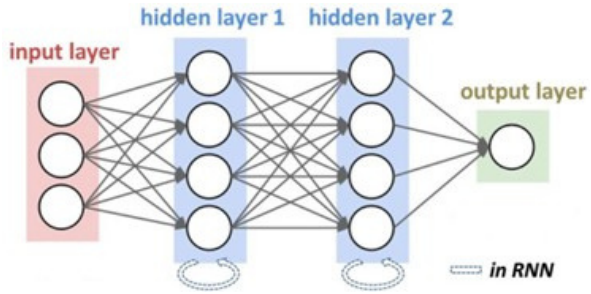

Figure 5. Recurrent neural networkRNNs.

https://doi.org/10.61577/jaiar.2025.1000014

Optimization and regularization

After designing the RNN based model, optimization techniques are applied to improve performance and generalization. To safeguard against overfitting, regularization techniques like dropout layers are embedded into the model. In addition, training is stopped using early stopping when validation performance no longer improves. Cross validation techniques, specifically five-fold cross validation will also be applied in the training to ensure robustness and reduce variance in model training and evaluation. The optimization strategies collectively improve the model accuracy and stability.

Training, validation and testing

Effective training of data using a Recurrent Neural Network (RNNs) for phishing URL recognition necessitates a systematic approach to achieve good generalization while avoiding overfitting and underfitting. The strategy involves dividing the dataset and validate and applying cross-validation to assess model stability.

Model Training Division is Train / Validation / Test – 70 / 20 / 10.

Effectively training data using a Recurrent Neural Network (RNN) for phishing website detection necessitates a systematic approach to achieve good generalization while preventing underfitting and overfitting.

Evaluation metrics analysis

The model, after training, validation and testing is assessed using classification metrics, a confusion matrix is used to explain the true positives, true negatives, false positives and false negatives. Classification effectiveness is measured using accuracy, precision, recall and F1-score.

Final model

The final step involves deploying the model for phishing website recognition which involves evaluating technical feasibility, computational requirements, time processing capability and usability. The Trained RNN model can perform effectively in a practical cybersecurity environment. It returns phishing probability and classification label (Phishing / Legitimate). This can be integrated with security dashboards or alerting systems. The final step involves deploying the model for phishing website detection.

Result Analysis

Infrastructure

Infrastructure for the model development includes:

- The Integrated Development Environment (IDE): Python
- The memory: 15.3 GB
- Storage: 120 GB
- Libraries Used: Scipy, Scikit-Learn, Matplotlib, Seaborn, Pandas, Numpy

Dataset demography

Model training was executed on a balanced dataset of 5,000 legitimate and 5,000 phishing instances, which enhances training effectiveness.

This methodology enhances the model's generalization to unseen data, enables reliable phishing recognition systems in a genuine settingand support robust,scalable deployment. Performance evaluation accuracy is achieved if the datasets are well balanced. The graph is illustrated in the figure 6.

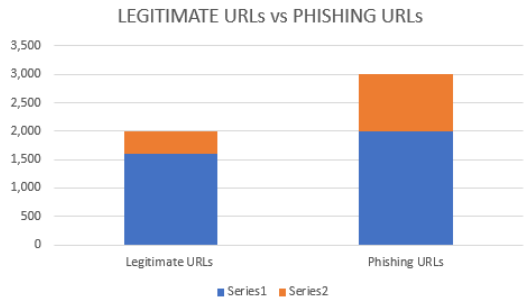

Figure 6. Demographics detail of the datasets for training.

Model

Recurrent Neural Network (RNNs) was used for as the model for the research

Performance metrics analysis of a phishing website recognition model

A Recurrent Neural Network (RNNs) Model was developed with a focus on ability to efficiently differentiate between legitimate and phishing websites using both structural and textual features. Themodel is implemented using TensorFlow/Keras and trained end-to-end on a labeledlegitimate and phishing datasets as illustrated in Table 2 and Figure 7.

Result

Table 2 . Result of the model.

Metrics	Values
accuracy	94
precision	92
recall	96
f1-score	94

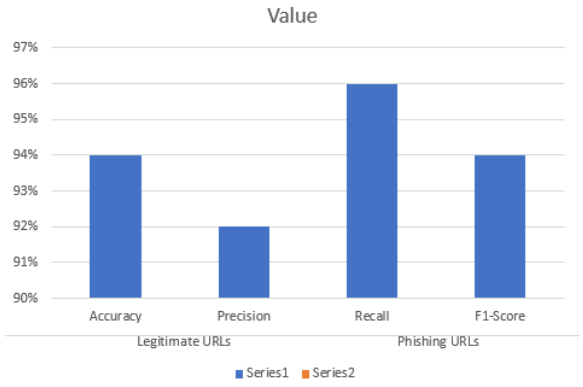

Figure 7. Model performance result.

Interpretation of results

The interpretation of results indicates a critical analysis of the model performance beyond numerical metric values, while

https://doi.org/10.61577/jaiar.2025.1000014

evaluation metrics like accuracy, precision, recall, and F1-Score offer a qualitative measure of predictive performance, as illustrated in the table and figure.

Accuracy- 94%

The model correctly classified 94% of all websites in the test datasets accurately, which indicates that the model's overall performance is very strong and has better generalization ability.

Precision - 92%

The precision shows a mature, produxtion ready with the model, out of all websites predicted as phishing, 92% were actually phishing. This indicates that the model produces very few false negatives. High precision is important to avoid blocking safe websites, legimate sites are rarely misclassified as phishing.

Recall - 96%

The model successfully detected 96% of all actual fishing websites. This implies very few phishing websites escaped detection. The model is very effective in catching malicious attacks.

F1-score - 94%

A value of 94% indicates the model maintains an excellent balance between detecting phishing attacks and avoiding false alarms.

Confusion matrix

The model's classification performance is further assessed by a confusion matrix. The breakdown of prediction outcomes facilitates deeper analysis of classification errors as shown in Figure 8.

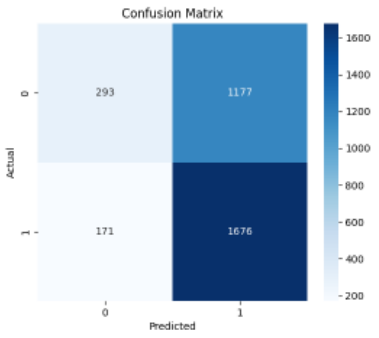

Figure 8. Confusion matrix.

Discussion

Recurrent Neural Network (RNNs) features phishing detection model was evaluated on a phishing and legitimate datasets, the model also integrates text-based features with structured URLs to classify websites as phishing or legitimate. The result indicates that the model capability to accurately detect phishing sites using sequential and contextual patterns from URL, code and textual features. It balances between high precision and recall which makes it an effective AI-driven cybersecurity defense system.

Conclusion

The experimental result indicates that proposed RNNs based phishing detection system is robust, reliable and effective for phishing website detection. The combination of textual analysis and URLs structure provides superior performance compared to single feature model.

Limitations

Dependence datasets

The RNNs model performance relies heavily on the characteristics of the training datasets. If the model is deployed on websites with different structures, languages phishing detection patterns might be reduced and can lead to misclassification.

URL Feature Limitations

The URL based features in the model developed might fail to detect higher phishing threats that use short URLs or domain spoofing techniques.

Future Work

- Phishing websites commonly employ deceptive text and fake login prompts, which make it necessary for the framework to differentiate between malicious and real websites.
- Embedding multi-modal features, like URLs, email headers and network traffic, can improve the framework's ability to recognize phishing comprehensively.

Disclosure Statement

No potential conflict of interest was reported by the authors.

References

1. Aljofey A, Bello SA, Lu J, Xu C. Comprehensive phishing detection: A multi-channel approach with variants TCN fusion leveraging URL and HTML features. J Netw Comput Appl. 2025;238:104170. https://doi.org/10.1016/j.jnca.2025.104170
2. Zara U, Ayyub K, Khan HU, Daud A, Alsahfi T, Ahmad SG. Phishing website detection using deep learning models. IEEE Access. 2024;12:167072-167087. https://doi.org/10.1109/ACCESS.2024.3486462
3. Perfecta JE, Ehikhamenle M. A PhishingDetection Model Using Recurrent Neural Network in Web-Based Services. International Journal of Research Publication and Reviews. 2024;5(10):4842-4853. Available at: https://ijrpr.com/uploads/V5ISSUE10/IJRPR34414.pdf
4. Lamda J, Singh A, Singh TR. Detecting PhishingWebsites Using MachineLearning (RNN). 2023;8(10). Available at: https://www.ijnrd.org/papers/IJNRD2310122.pdf
5. Gupta BB, Gaurav A, Attar RW, Arya V, Alhomoud A, Chui KT. Optimized Phishing Detection with Recurrent Neural Network and Whale Optimizer Algorithm. Computers, Materials & Continua. 2024;80(3). https://doi.org/10.32604/cmc.2024.050815
6. 1.Taofeek AO. Development of a novel approach to phishing detection using machine learning. ATBU J Sci Technol Educ. 2024;12(2):336-351. Available at: https://www.researchgate.net/profile/Taofeek-Agboola/publication/381717458_Development_of_a_Novel_Approach_to_Phishing_Detection_using_Machine_Learning/links/667c1eaa1846ca33b8524749/Development-of-a-Novel-Approach-to-Phishing-Detection-using-Machine-Learning.pdf

https://doi.org/10.61577/jaiar.2025.1000014

7. Amaefule IA, Ubochi CI, Anamelechi FC. Detection of phishing website using machine learning and features extraction. Int J Adv Res Ideas Innov Eng. 2025;11(1). Available at: https://www.researchgate.net/profile/Amaefule-A/publication/388220390_Detection_of_Phishing_Website_Using_Machine_Learning_and_Features_Extraction/links/678f938398c4e967fa738fa5/Detection-of-Phishing-Website-Using-Machine-Learning-and-Features-Extraction.pdf
8. Colhak F, Ecevit MI, Uçar BE, Creutzburg R, Dağ H. Phishing website detection through multi-model analysis of html content. InInternational Conference on Theoretical and Applied Computing 2024:171-184. Singapore: Springer Nature Singapore. https://doi.org/10.1007/978-981-97-6957-5_15
9. Barik K, Misra S, Mohan R. Web-based phishing URL detection model using deep learning optimization techniques. Int J Data Sci Anal. 2025;20(5):4449-4471. https://doi.org/10.1007/s41060-025-00728-9
10. Ghalechyan H, Israyelyan E, Arakelyan A, Hovhannisyan G, Davtyan A. Phishing URL detection with neural networks: an empirical study. Scientific reports. 2024;14(1):25134. https://doi.org/10.1038/s41598-024-74725-6
11. Qazi A, Al-Mhdawi MK. Exploring critical drivers of global innovation: A Bayesian network perspective. Knowledge-Based Systems. 2024;299:112127. https://doi.org/10.1016/j.knosys.2024.112127
12. Jain AK, Gupta BB. Phishing detection: analysis of visual similarity based approaches. Security and Communication Networks. 2017;2017(1):542104. https://doi.org/10.1155/2017/5421046
13. Heartfield R, Loukas G. Protection against semantic social engineering attacks. InVersatile cybersecurity. 2018:99-140. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-97643-3_4
14. Hendriksen G, Fischer S, Gemmell C, Mackie I, Owoicho P, Rossetto F et al. Extracting Structured Web Content using Deep Neural Language Models. 2022. Available at: https://www.cs.ru.nl/masters-theses/2022/G_Hendriksen___Extracting_structured_web_content_using_deep_neural_language_models.pdf
15. Van Dalen A. Algorithmic gatekeeping for professional communicators: Power, trust, and legitimacy. Routledge; 2023. https://doi.org/10.4324/9781003375258

https://doi.org/10.61577/jaiar.2025.1000014