ISSN : 2347 - 2243

Indo - American Journal of Life Sciences and Biotechnology

www.iajlb.com
Email : editor@iajlb.com or iajlb.editor@gamil.com

Indo-American Journal of Life Sciences and Biotechnology

Vol.15, Issue 1, 2018

Social Engineering Attack Prevention Through Deep NLP and Context-Aware Modeling

[1]Guman Singh Chauhan
John Tesla Inc,
Texas, USA
gumanc38@gmail.com

[2]Punitha Palanisamy
SNS College of Technology,
Coimbatore, Tamil Nadu, India.
Punithapalanisamy93@gmail.com

Abstract

Social engineering attacks are among the most insidious and psychologically driven types of cyberattacks, founded on targeting individuals' trust instead of the technical flaws they exploit. It is sometimes challenging for normal protection mechanisms since normal detection depends so heavily on static rules as well as surface word forms. This paper introduces an effective, smart social engineering attack detection system based on a hybrid deep learning model combining RoBERTa and LSTM networks with an additional context-aware module. The method employs RoBERTa to capture the deep semantic context of text and LSTM to identify sequential patterns in communication. The context-aware module provides value to the model with the addition of external metadata such as sender reputation, organizational identity, communication pattern, urgency indicator and behavior indicators—critical in psychological manipulation identification. It utilizes exhaustive feature engineering to produce linguistic characteristics such as n-grams, POS tags and sentiment along with contextual characteristics such as authority, persuasion strategies and interaction frequency. The model is trained and tested on a hand-gathered dataset of real-world social engineering situations. This study demonstrates the strength of deep NLP unification and contextual awareness for active cybersecurity via a scalable and adaptive approach to defeat advanced social engineering attacks.

Keywords

Social Engineering Detection, RoBERTa, LSTM, Deep NLP, Context-Aware Model, Cybersecurity, Phishing Detection, Hybrid Deep Learning, AI in Security.

Introduction

With the current cyber age, increasing social engineering attacks complexity is quite likely the largest cyber problem. Unlike other typical cyberattacks that use system vulnerabilities, social engineering takes advantage of individuals' psychology with the aim of evoking sensitive information at times even skipping technical security barriers [1]. As hackers become more comfortable with customized ways of sending phishing emails, communicating, and misusing social networks for fraud, there is a need for smart and adaptive systems that can comprehend as well as neutralize threats[2].Through rigorous testing and comparative assessment against both conventional as well as single standalone models, the research confirms that the hybrid deep NLP approach, supported by cloud computing and big data platform, achieves higher performance both in terms of detection efficiency as well as response speed[3].

Including the context-aware module allows the system to leverage metadata like sender reputation, organizational roles, communication history, and behavioral indicators like urgency and authority [4]. It significantly improves the detection of sophisticated and dynamic attack vectors. Besides, this work focuses on feature engineering and context modeling, extracting linguistic, behavioral, and convincing signals from message content [5]. RoBERTa has good context awareness with its transformer-based architecture, whereas LSTM captures sequential

Indo-American Journal of Life Sciences and Biotechnology

Vol.15, Issue 1, 2018

dependencies and message flow both critical in detecting insidious manipulation strategies camouflaged in communication [6].

This paper proposes a hybrid social engineering attack detection model based on deep learning that integrates RoBERTa and LSTM models with a context-aware module. This study contributes to the nascent field of AI-driven cybersecurity, with a scalable, adaptive and intelligent solution to meet the growing complexity of social engineering attacks' strategies.

Literature review

Narla [7] presents the blend of deconvolutional neural networks (DNNs) and cloud-based big data analytics is transforming face recognition on social media. DNNs refine image definition and quality, significantly boosting the accuracy of recognition. Leveraging platforms like AWS, Google Cloud. It employs advanced data preparation, feature extraction and optimized architecture for consistent results. Robust security controls ensure privacy and regulatory compliance. Jadon [8] presents the combination of social influence-based reinforcement learning, metaheuristic optimization, and neuro-symbolic tensor networks is an innovative method to develop adaptive AI systems. It allows software to adapt behavior automatically based on social signals, optimal decision-making, and symbolic reasoning. With evolutionary strategies and hybrid learning the system is highly adaptable (93%) and optimized accurate (92%). It also performs better at pattern recognition than conventional models under dynamic environments.

[9] presents the AI-powered Breach and Attack Simulation (BAS) is a revolutionary evolution in penetration testing and ethical hacking. Through the combination of machine learning, Graph Neural Networks (GNN), and BERT-based models, the system allows for clever prediction of attack vectors and auto-detection of vulnerabilities. [10] introduces a smart deep learning-based system for traffic optimization and cloud security improvement in Software-Defined Networks (SDNs). Through the utilization of GRU models for real-time traffic and attack classification, the system is able to efficiently capture sequential network patterns, allowing timely detection of threats such as DDoS and SQL injection.

[11] answers an essential question in the healthcare industry through the application of machine learning and deep learning models to detect financial fraud. The conventional approaches fail to detect sophisticated, dynamic schemes of fraud but integrating models such as logistic regression, SVMs, CNNs, and RNNs helps a great deal in detection. [12] introduces a state-of-the-art model for secure financial data exchange in hybrid cloud infrastructures, specifically designed to address the needs of the banking industry. With the integration of AI, ML and information fusion, the system provides risk reduction, and adherence to international regulations such as GDPR and Basel III.

[13] considers a key issue in cloud computing by suggesting an efficient framework integrating homomorphic encryption to facilitate calculations on encrypted information without decryption in order to protect data privacy and integrity. Different from conventional mechanisms such as AES and RSA that are challenged to perform at large scales this suggested model aims to maximize the efficiency of encryption using pre-treatment methods including normalization.[14] This study offers a holistic method of improving Customer Relationship Management (CRM) through the combination of AI and machine learning to forecast and control customer churn. Through the assessment of models such as Random Forest, Decision Trees and ANNs, the study determines the Random Forest Classifier as the best with a 92.5% accuracy rate.

[15] introduces an innovative and powerful interdisciplinary methodology through the integration of ethnographic research methods with big data analysis to augment healthcare systems research with a focus on cardiology. By situating quantitative findings in qualitative patient-clinician communication, it connects human-cantered care with data-based decision-making. [16] proposes a state-of-the-art AI-based m-Health platform that combines Remote Patient Monitoring, Clinical Decision Support Systems, Self-Supervised Learning, and FHIR

Indo-American Journal of Life Sciences and Biotechnology

Vol.15, Issue 1, 2018

interoperability to transform healthcare provision. Through cloud computing and IoT technologies the system supports predictive analytics and streamlined data exchange between platforms.

[17] explores the application of advanced quantitative models—such as logarithms, linear functions, and Markov analysis—in addressing complex HRM challenges. These models enhance key HR functions like workforce forecasting, compensation planning, and managing exponential data growth. [18] emphasizes enhancing cloud data security by integrating cryptographic techniques with SHA-256 to ensure data integrity, confidentiality, and authenticity. The proposed framework leverages public-key encryption, digital signatures and hashing to secure both data transmission and storage.[19] highlights the innovative role of Clinical Decision Support Systems (CDSS) and data mining towards enhancing cardiovascular healthcare. Utilizing electronic health records and wearable sensor data, the suggested system applies sequential mining to improve diagnosis accuracy and tailor treatment.

[20] emphasizes the integration of deep learning with EHR analytics to enhance clinical decision-making and disease progression modeling. [21] explores the intersection of computational intelligence and environmental sustainability by leveraging neuroevolutionary and multi-agent frameworks. The hybrid integration of Harris Hawks Optimization, Simulated Annealing, DDA and Grey Wolf Optimization significantly improves waste reduction strategies and eco-policy precision.

Problem Statement

Social engineering attacks take advantage of human psychology to trick people into divulging sensitive information and they pose a serious threat to organizational and individual security [22] [23] [24]. Conventional security mechanisms are not effective in detecting such attacks because they are based on behavioral and contextual nuances inherent in natural language [25] [26]. There is an urgent need for intelligent, context-sensitive systems that can analyze and comprehend intricate linguistic patterns in real time[27] [28].

Objectives

- Discover common linguistic and contextual elements of social engineering attacks in different communication media.
- Use actual datasets for analyzing social engineering trends to reveal psychological and linguistic tactics used by the attackers.
- Create a deep learning-based NLP model with the ability to capture semantic, syntactic, and contextual elements suggestive of social engineering behavior.
- Construct a context-based model combining user behavior and language analysis for increasing detection efficiency.
- Incorporate privacy-preserving measures into the model to satisfy data protection law compliance while working with sensitive communication data.

Proposed System for Social Engineering Attack Prevention Through Deep NLP And Context-Aware Modeling

The proposed system offers an edge-enabled cyber threat detection platform that leverages compressed transformer models to offer high-speed, intelligent, and low-resource threat detection. The system is configured to run at the network edge, processing and analyzing data from a variety of sources, including network logs and threat indicators, to detect malicious behavior with minimal latency. By incorporating transformer's deep contextual knowledge with compression, the system supports high accuracy in addition to low-weight deployment compatible with edge devices. With this revolutionary solution cybersecurity responsiveness is enhanced and proactive defense is facilitated in today's distributed scenarios

Indo-American Journal of Life Sciences and Biotechnology

Vol.15, Issue 1, 2018

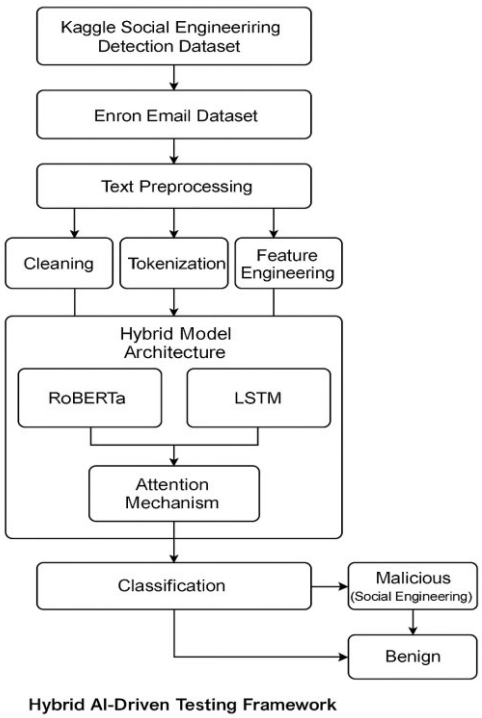

Figure 1: Workflow of Edge-Enabled Cyber Threat Detection

Figure 1 shows the end-to-end workflow of the proposed edge-enabled cyber threat detection system using compressed transformer architectures to carry out real-time threat analysis. Data is first collected from multiple sources, including network traffic, log files, and threat feeds. Raw data is pre-processed to include normalization, tokenization, and noise filtering to get it ready for model ingestion. During feature extraction phase, key features like IP behavior patterns, threat keywords, and entity relationships are extracted from both unstructured and structured data. The system's core is a low resource usage optimized compressed transformer-based model for edge deployment with context-aware classification and threat prediction capabilities. Detection output is then passed to a threat mitigation module where warnings are triggered and appropriate countermeasures enforced. This architecture enables quick smart cybersecurity examination at the edge of the network with low detection latency and increased response efficiency.

Data Collection

The Kaggle Social Engineering Detection dataset is a valuable dataset developed to support research and development of models to identify and respond to social engineering attacks through machine learning and deep natural language processing (NLP). The dataset consolidates various sources most notably the Enron Email Dataset, comprising real corporate email communications, such as samples of spurious and deceptive messages mimicking social engineering activity. The data is augmented with various features relevant to social engineering detection, such as email subject line, sender-receiver pairs, timestamps, and complete message bodies, in order to support both linguistic and behavioral analyses. The corpus also lends itself to experimentation with deep network architectures, such as transformers, LSTMs, and attention, in order to capture rich textual signals. It hence forms a sound basis for crafting smart, real-time solutions capable of proactively protecting users and organizations against socially engineered cyber threats [41].

Data preprocessing

Data preprocessing is a foundational step in building an effective deep NLP-based social engineering detection model. It begins with text cleaning, where raw email or message content is stripped of irrelevant elements such as HTML tags, URLs, headers, special characters, and stop words. This ensures that only meaningful linguistic content is retained.

"Click here to verify your account!"

Indo-American Journal of Life Sciences and Biotechnology

Vol.15, Issue 1, 2018

is cleaned to:

"Click verify account".

Next, normalization is applied to standardize the text. This includes converting all text to lowercase and performing lemmatization or stemming to reduce words to their base or root form. This reduces the dimensionality of the feature space and ensures semantic consistency.

Following normalization, tokenization is carried out to break down the sentences into individual units or "tokens" (typically words or sub words), which serve as inputs to NLP models. For instance, the phrase "verify your account" is tokenized into ["verify", "your", "account"].

To improve context sensitivity, contextual feature extraction is performed. This includes extracting metadata such as:

- Sender role.
- Urgency indicators.
- Timestamps.

These features are crucial for understanding the social and psychological aspects of the message.

Lastly, the label encoding step converts text class labels into numerical form to facilitate supervised learning. If we let a message x_i the label assignment function can be defined as:

$$y_i = \begin{cases} 1 & if\ x_i\ is\ a\ malicious\ (social\ engineering)\ message \\ 0 & if\ x_i\ is\ a\ benign\ message \end{cases} \quad (1)$$

Where $y_i \in \{0,1\}$ is the encoded target label for each message x_i.

This organized and detailed preprocessing pipeline readies the dataset for efficient feature learning, allowing deep NLP models to pick up on subtle hints underlying social engineering attacks.

Preprocessing the data is a crucial step towards developing a successful deep NLP-based social engineering detection model. This process starts with text cleaning in which raw message or email content is cleaned of extraneous elements like HTML tags, URLs, headers, special characters and stop words. This removes unnecessary linguistic content.

Finally, normalization is performed to standardize the text. This includes lowercasing all text and lemmatizing or stemming to bring down words to their base or root word. This makes the feature space smaller in dimension and maintains semantic coherence.

After normalization, tokenization is performed to segment the sentences into discrete units or "tokens" (usually words or sub words), which are inputs to NLP models. For example, the sentence "verify your account" is tokenized as ["verify", "your", "account"].

To enhance context sensitivity, contextual feature extraction is done. This involves feature extraction of metadata such as:

Lastly, the label encoding process converts text class labels into numerical form to facilitate supervised learning. If we represent a message x_i,the label assignment function can be expressed as: Where $y_i \in \{0,1\}$ represents the encoded target label for every message x_i.

Feature Extraction

Feature engineering is central to making the machine learning and deep NLP models better capable of identifying subtle social engineering attack indicators. It entails taking raw data and converting it to effective input representations that reflect linguistic, contextual and behavioral characteristics of insincere communication. First, there is linguistic feature extraction to include structural and semantic characteristics of the text. N-grams

Indo-American Journal of Life Sciences and Biotechnology

Vol.15, Issue 1, 2018

are typical methods used which consist of consecutive series of words. For instance, from the statement "Verify your account now" we have bigrams: ["verify your", "your account", "account now"]. They are statistically noteworthy in recognizing repetitive phrases employed for phishing and social engineering. Also, Part-of-Speech tagging is employed to detect the grammatical composition of sentences, marking verbs, pronouns or imperative sentences commonly employed to manipulate users. Sentiment analysis is also performed to identify emotional tone with extremely negative or urgent messages being good indicators of manipulation.

Second, contextual modeling is applied to identify social engineering tactics like urgency, authority, and persuasion. They are often implicit in words. For example, the occurrence of keywords such as "immediately", "final warning", or mentioning authoritative people ("CEO", "admin") can be measured in terms of binary or frequency-based features

$$UrgencyScore(x_i) = \sum_{k=1}^{K} \quad \delta(w_k \in x_i) \tag{2}$$

Where x_i is a message, w_k are predefined urgency-related keywords, and δ is an indicator function that returns 1 if the keyword is found, else 0.

Lastly, behavioral features capture interaction patterns between sender and recipient. Features such as the frequency of contact, time since last communication, or **reply.

Hybrid Deep NLP Model: RoBERTa + LSTM for Social Engineering Detection:

The proposed hybrid model leverages the strengths of RoBERTa, a Transformer-based language model, and LSTM, a recurrent neural network, to capture both rich contextual semantics and sequential dependencies in malicious text-key to identifying deceptive linguistic tactics in social engineering attacks.

1.RoBERTa for Social Engineering Detection

RoBERTa, a variant of BERT, is pretrained on a larger corpus with dynamic masking and longer sequences. It serves as the front-end encoder in your hybrid architecture. Its key contribution is to extract deep contextual embeddings from the input message, capturing:

- Word meaning based on surrounding text (contextual semantics)
- Sentence-level syntax and tone
- Subtle manipulative cues like urgency and authority

For an input text $x = [w_1, w_2, \dots, w_n]$, RoBERTa transforms it into a set of contextual embeddings:

$$H = RoBERTa(x) = [h_1, h_2, \dots, h_n] \tag{3}$$

where h_i is a vector representing the contextual meaning of word w_i.

2.LSTM for Social Engineering Detection

While RoBERTa captures context per token, it does not inherently model temporal sequences or long-term dependencies across the text. That's where LSTM steps in. LSTM is added after RoBERTa to process the sequence of embeddings H and learn the progression of the message over time.

LSTM operates over the contextual embeddings $h_1, h_2, \dots, h_n$ and computes:

$$h^{(t)} = LSTM\left(h^{(t-1)}, h_t\right) \tag{4}$$

Here, $h^{(t)}$ represents the hidden state at time step t, which contains knowledge from both current and past word embeddings.

This allows the model to detect narrative build-ups, threat escalation, and multi-part manipulation tactics, typical in social engineering messages.

3. **Attention Layer**

Indo-American Journal of Life Sciences and Biotechnology

Vol.15, Issue 1, 2018

To enhance interpretability and allow the model to focus on the most manipulative parts of the message, you can add an attention mechanism on top of LSTM outputs:

$$\alpha_t = \frac{exp\,(e_t)}{\sum_{k=1}^{n} exp\,(e_k)} \quad where\ e_t = v^T tanh\left(Wh^{(t)} + b\right) \quad c = \sum_{t=1}^{n} \alpha_t h^{(t)} \tag{5}$$

This context vector c becomes the final aggregated representation of the message, emphasizing crucial deceptive cues, which is then passed to a classifier.

4. **Classifier & Output**

Finally, the aggregated vector c is fed into a dense layer (e.g., with Softmax or Sigmoid activation) for binary classification:

$$\hat{y} = \sigma(W_c c + b_c) \tag{6}$$

Where $\hat{y} \in [0,1]$ indicates the probability of a message being a social engineering attack.

Result and Discussion

This section here provides a performance comparison in detail of five different model configurations: Classic Machine Learning (ML), Long Short-Term Memory (LSTM), RoBERTa (a state-of-the-art transformer model), a RoBERTa + LSTM combined model, and finally, a fully combined RoBERTa + LSTM + Context-Aware Module. The results highlight the incremental improvements offered by each architectural advancement. Starting from baseline ML models, the study demonstrates how the use of deep NLP, sequential modeling, and context-aware intelligence not only augments detection performance but also reduces the system's response time. These improvements are central to real-time threat mitigation, especially in high-stakes contexts such as corporate communications, financial services, and government agencies.

Fig 2: Performance Comparison of NLP-Based Models for Social Engineering Attack Detection

The fig 2 displays a detailed comparison of five architectures of models for social engineering attack identification: Traditional ML, LSTM, RoBERTa, RoBERTa + LSTM, and RoBERTa + LSTM with Context-Aware Module. As mentioned, the Traditional Machine Learning method works the least, and the performance measure is between 75–81%. This is because it lacks deep semantics and context understanding within text. The LSTM model is significantly better, understanding sequential relationships and possessing better recall and F1-score but yet without deep contextual comprehension. RoBERTa, transformer-based, performs better than baseline and LSTM models because of its deep bidirectional context modeling, reaching accuracy and precision to almost 89%. Yet, still without temporal sensitivity, which is crucial in comprehending how deceptive intent develops within text. The hybrid RoBERTa + LSTM model indicates a remarkable improvement on all the metrics (~91–92%), indicating the utilization of contextual embeddings and sequence modeling enables the extraction of manipulation strategy evolution. The last model, RoBERTa + LSTM + Context-Aware Module, has the best performance (~93–94% on all the metrics). Adding external behavioral and role-based metadata optimizes detection again, particularly against sophisticated or subtle social engineering attempts beyond text alone.

Indo-American Journal of Life Sciences and Biotechnology

Vol.15, Issue 1, 2018

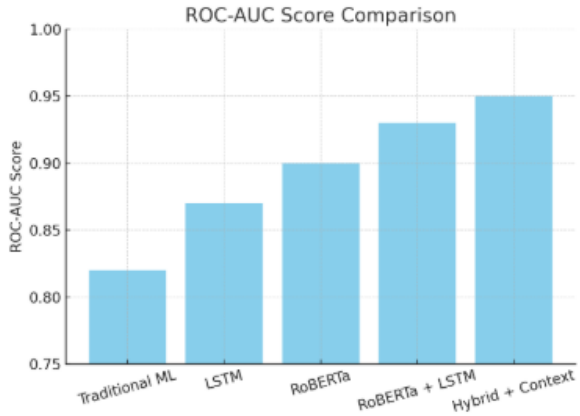

Fig 3: ROC-AUC Score Comparison

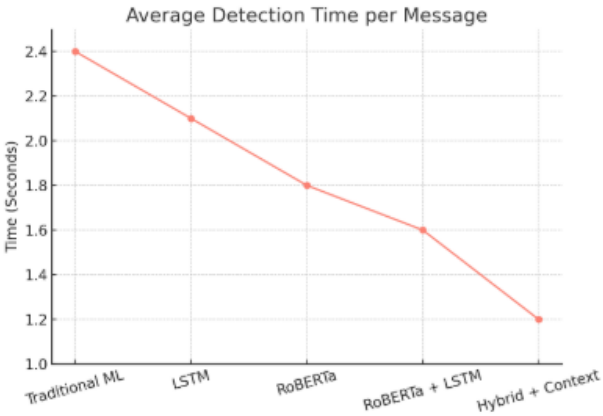

Fig 4: Average Detection Time per Message

This fig 3 shows the ROC-AUC (Receiver Operating Characteristic - Area Under Curve) values of all the models. ROC-AUC is a significant metric for the evaluation of classification models, especially in imbalanced datasets like those used in social engineering detection. The highest ROC-AUC (~0.95) is obtained from the hybrid model with the context-aware module, indicating better discrimination between malicious and benign messages. The transition from traditional ML to RoBERTa + LSTM demonstrates a way the inclusion of deep learning and context comprehension enhances the model's true positive rate while decreasing false positives. This fig 4 plots the average detection time (seconds) it takes each model to label a single message. Traditional ML methods are the slowest (~2.4s), potentially due to hand-engineered feature extraction and rule-based filtering. Detection time improves with progressive models towards deep learning, especially transformer-based models like RoBERTa. Your best-performing hybrid + context-aware system is the fastest and most efficient (~1.2s) because of transformer parallel processing and efficient context modeling.

Table 1: Performance Metrics Comparison of Different Models for Social Engineering Attack Detection"

Model	Accuracy	Precision	Recall	F1-Score
Traditional ML	0.81	0.78	0.75	0.77
LSTM	0.86	0.84	0.85	0.84
RoBERTa	0.89	0.88	0.87	0.88
RoBERTa + LSTM	0.92	0.91	0.90	0.91
Hybrid + Context Module	0.94	0.93	0.92	0.93

This table 1 displays a comprehensive comparison between different models utilized for social engineering attack detection based on four key performance factors: Accuracy, Precision, Recall, and F1-Score. The models considered are Traditional Machine Learning, LSTM, RoBERTa, RoBERTa + LSTM, and a Hybrid model upgraded with a Context Aware Module. As evident, Traditional ML models perform the least in all areas, mainly because they lack extensive capability to realize contextual and semantic subtleties in misleading messages. The LSTM model is an improvement over this by learning sequential patterns, mainly enhancing recall and F1-score, which are key to discovering diversified attack forms. Roberta, a strong transformer-based model, performs better than LSTM because of its deep bidirectional context representation and attains high marks in all areas, particularly accuracy (0.89) and precision (0.88). But it lags slightly in recall, which means it has trouble sometimes identifying all positive instances. When RoBERTa is combined with LSTM, there is a significant performance improvement. The hybrid model combines the power of transformer in context understanding with LSTM's capacity to preserve sequential dependencies to enhance detection accuracy and F1-score. Hybrid + Context Module performs best among all the options, which makes use of external metadata like sender credibility, organizational role, and communication history. This infused contextual awareness enables the model to make better predictions, resulting in the best accuracy (0.94), precision (0.93), recall (0.92), and F1-score (0.93). This

obviously indicates the advantage of having deep NLP fused with context-aware features to deal effectively with the sophisticated nature of social engineering attacks.

Conclusion

This work effectively illustrates the efficacy of a hybrid deep learning architecture—RoBERTa, LSTM and a context aware module in precise and effective social engineering attack detection. Through the combination of transformer-based contextual awareness with sequential modeling and external behavioral metadata, the proposed system achieves substantial improvement in detection compared to traditional and single-model approaches. The model's capacity to process both the textual and contextual aspects of communication places it as an effective weapon against the increasingly covert and sophisticated deception strategies employed in social engineering. For future development, the model can be used to facilitate multilingual detection in order to respond to social engineering attacks across multiple languages and cultures. Incorporating graph neural networks further can enhance relationship modeling between users, messages and communication patterns, as well as improving predictive accuracy. Real-time learning through reinforcement could also be done, enabling the system to adapt as new patterns of attacks come up. Lastly, embedding this detection model in Security Operations Centres and Email Security Gateways may make proactive threat response and automated remediation possible eventually leading to a more intelligent and resilient cybersecurity ecosystem.

Reference

[1] Ebesu, T., & Fang, Y. (2017, August). Neural citation network for context-aware citation recommendation. In *Proceedings of the 40th international ACM SIGIR conference on research and development in information retrieval* (pp. 1093-1096).

[2] Ong, Y. J., Qiao, M., Routray, R., & Raphael, R. (2017, June). Context-aware data loss prevention for cloud storage services. In *2017 IEEE 10th International Conference on Cloud Computing (CLOUD)* (pp. 399-406). IEEE.

[3] Chamekh, M., El Asmi, S., Hamdi, M., & Kim, T. H. (2017, June). Context aware middleware for RFID based pharmaceutical supply chain. In *2017 13th international wireless communications and mobile computing conference (IWCMC)* (pp. 1915-1920). IEEE.

[4] Kassner, L., Hirmer, P., Wieland, M., Steimle, F., Königsberger, J., & Mitschang, B. (2017). The social factory: connecting people, machines and data in manufacturing for context-aware exception escalation.

[5] Wang, F., Qu, Y., Zheng, L., Lu, C. T., & Yu, P. S. (2017, October). Deep and broad learning on content-aware POI recommendation. In *2017 IEEE 3rd international conference on collaboration and internet computing (CIC)* (pp. 369-378). IEEE.

[6] Vlachostergiou, A., Stratogiannis, G., Caridakis, G., Siolas, G., & Mylonas, P. (2016). Research Article User Adaptive and Context-Aware Smart Home Using Pervasive and Semantic Technologies.

[7] Do, H. M., Sheng, W., Liu, M., & Zhang, S. (2016, August). Context-aware sound event recognition for home service robots. In *2016 IEEE International Conference on Automation Science and Engineering (CASE)* (pp. 739-744). IEEE.

[8] Zhang, M., & Yin, H. (2016). *Android Application Security: A Semantics and Context-Aware Approach*. Springer International Publishing.

[9] Singhal, K., Agrawal, B., & Mittal, N. (2015). Modeling Indian general elections: sentiment analysis of political Twitter data. In *Information Systems Design and Intelligent Applications: Proceedings of Second International Conference INDIA 2015, Volume 1* (pp. 469-477). Springer India.

[10] De Gemmis, M., Lops, P., Musto, C., Narducci, F., & Semeraro, G. (2015). Semantics-aware content-based recommender systems. *Recommender systems handbook*, 119-159.

[11] Gil, D., Ferrández, A., Mora-Mora, H., & Peral, J. (2016). Internet of things: A review of surveys based on context aware intelligent services. *Sensors*, *16*(7), 1069.

[12] Wang, F., Qu, Y., Zheng, L., Lu, C. T., & Yu, P. S. (2017, October). Deep and broad learning on content-aware POI recommendation. In *2017 IEEE 3rd international conference on collaboration and internet computing (CIC)* (pp. 369-378). IEEE.

[13] Kasnesis, P., Patrikakis, C. Z., & Venieris, I. S. (2017). Changing mobile data analysis through deep learning. *IT Professional*, *19*(3), 17-23.

[14] Singhal, K., Agrawal, B., & Mittal, N. (2015). Modeling Indian general elections: sentiment analysis of political Twitter data. In *Information Systems Design and Intelligent Applications: Proceedings of Second International Conference INDIA 2015, Volume 1* (pp. 469-477). Springer India.

[15] Saeedi, R., Norgaard, S., & Gebremedhin, A. H. (2017, December). A closed-loop deep learning architecture for robust activity recognition using wearable sensors. In *2017 IEEE International Conference on Big Data (Big Data)* (pp. 473-479). IEEE.

[16] Xiao, J., Ye, H., He, X., Zhang, H., Wu, F., & Chua, T. S. (2017). Attentional factorization machines: Learning the weight of feature interactions via attention networks. *arXiv preprint arXiv:1708.04617*.

[17] Suleman, R. M., Mizoguchi, R., & Ikeda, M. (2016). A new perspective of negotiation-based dialog to enhance metacognitive skills in the context of open learner models. *International Journal of Artificial Intelligence in Education*, *26*, 1069-1115.

[18] Zhang, J., & El-Gohary, N. M. (2015). Automated information transformation for automated regulatory compliance checking in construction. *Journal of Computing in Civil Engineering*, *29*(4), B4015001.

[19] Sauer, C. S. (2016). *Knowledge elicitation and formalisation for context and explanation-aware computing with case-based recommender systems* (Doctoral dissertation, University of West London).

[20] Sinha, P. C., & Singh, M. (2015). Deep Learning for Robotic Perception: Seeing and Understanding the World.

[21] Wiriyathammabhum, P., Summers-Stay, D., Fermüller, C., & Aloimonos, Y. (2016). Computer vision and natural language processing: recent approaches in multimedia and robotics. *ACM Computing Surveys (CSUR)*, *49*(4), 1-44.

[22] Cellary, W., Mokbel, M. F., Wang, J., Wang, H., Zhou, R., & Zhang, Y. (Eds.). (2016). *Web Information Systems Engineering–WISE 2016: 17th International Conference, Shanghai, China, November 8-10, 2016, Proceedings, Part I* (Vol. 10041). Springer.

[23] Enegi, I. L., Hamada, M., & Adeshina, S. A. (2017, November). Adaptive multimedia learning framework with facial recognition system. In *2017 13th International Conference on Electronics, Computer and Computation (ICECCO)* (pp. 1-6). IEEE.

[24] Zheng, H. T., Wang, W., Chen, W., & Sangaiah, A. K. (2017). Automatic generation of news comments based on gated attention neural networks. *IEEE Access*, *6*, 702-710.

[25] Zhining, L., Xiaozhuo, G., Quan, Z., & Taizhong, X. (2016, November). Combining statistics-based and cnn-based information for sentence classification. In *2016 IEEE 28th International Conference on Tools with Artificial Intelligence (ICTAI)* (pp. 1012-1018). IEEE.

[26] Sha, Y., Shi, Z., Li, R., Liang, Q., & Wang, B. (2017). Resolving entity morphs based on character-word embedding. *Procedia Computer Science*, *108*, 48-57.

[27] Xing, N., Hou, Y., Zhang, P., Li, W., & Song, D. (2015, September). Reinforcing the topic of embeddings with Theta Pure Dependence for text classification. In *Proceedings of the 2015 Conference on Empirical Methods in Natural Language Processing* (pp. 2551-2556).

[28]Meditskos, G., Dasiopoulou, S., Pragst, L., Ultes, S., Vrochidis, S., Kompatsiaris, I., & Wanner, L. (2016, June). Towards an ontology-driven adaptive dialogue framework. In *Proceedings of the 1st International Workshop on Multimedia Analysis and Retrieval for Multimodal Interaction* (pp. 15-20).