Deep-Learning-based Cryptanalysis through Topic Modeling

Kishore Kumar
Amity Institute of Information Technology, Amity University, India
kishore.kumar@student.amity.edu (corresponding author)

Sarvesh Tanwar
Amity Institute of Information Technology, Amity University, India
stanwar@amity.edu

Shishir Kumar
School of Information Science and Technology, Babasaheb Bhimrao Ambedkar University, India
shishir.cs@bbau.ac.in

Received: 13 October 2023 | Revised: 14 November 2023 and 23 November 2023 | Accepted: 24 November 2023

 DOI: https://doi.org/10.48084/etasr.6515

ABSTRACT

Neural cryptography is a technique that uses neural networks for secure data encryption. Cryptoanalysis, on the other hand, deals with analyzing and decrypting ciphers, codes, and encrypted text without using a real key. Chosen-plaintext cryptanalysis is a subfield of cryptanalysis where both plain text and ciphertext are available and the goal is either to find the encryption technique, the encryption key, or both. This study addresses chosen plaintext cryptanalysis within public key cryptography, to categorize topics of encrypted text. Using a fixed encryption technique and key, the focus was placed on creating a framework that identifies the topic associated with ciphertext, using diverse plaintexts and their corresponding cipher texts. To our knowledge, this is the first time that chosen-plaintext cryptanalysis has been discussed in the context of topic modeling. The paper used deep learning techniques such as CNNs, GRUs, and LSTMs to process sequential data. The proposed framework achieved up to 67% precision, 99% recall, 80% F1-score, and 71% AUPR on a dataset, showcasing promising results and opening avenues for further research in this cryptanalysis subarea.

Keywords-cryptanalysis; chosen-plaintext cryptanalysis; deep learning; topic modeling; CNN, LSTM, GRU

I. INTRODUCTION

Neural cryptography uses neural networks to encrypt data for secure transmission and has attracted great research interest during the recent years [1-2]. While traditional public key exchange protocols are based on algebraic number theory [3-5], in neural cryptography, the two communicating parties exchange secret keys by synchronizing the weights of their corresponding neural networks. The other side of neural cryptography is neural cryptanalysis. Cryptanalysis is the study and process of analyzing and decrypting ciphers, codes, and encrypted text without using the real key. Neural cryptanalysis employs neural networks to perform this task [6].

There are many different types of cryptanalysis; they are broadly classified into three categories: (i) ciphertext-only attacks, (ii) known-plaintext attacks, and (iii) chosen-plaintext attacks. In ciphertext-only attacks [7], the attacker has only access to the ciphertext and does not know the plaintext, the key, or even the algorithm used to encrypt the message. This is the most difficult type of attack, but also the most common because it is the easiest ciphertext for an attacker to obtain. Known-plaintext attacks consist of a scenario where the attacker has access to both the ciphertext and the plaintext for a specific message [8]. This is a more powerful attack than a ciphertext-only attack, as the attacker can use the known plaintext to learn more about the encryption algorithm and the key. In the chosen-plaintext type of attack, the attacker can choose the plaintext for a message, and then get the corresponding ciphertext from the system [9]. This is the most powerful type of attack, as the attacker can use this information to completely break the encryption system. Chosen-plaintext attacks are crucial in public-key cryptography [10], as the key is public and the attackers are free to encrypt whatever plaintext they choose. This paper deals with chosen-plaintext cryptanalysis in the context of topic modeling.

In general, the goal of chosen-plaintext cryptanalysis is to find out the encryption technique, the encryption key, or both [11]. This study deals with a particular scenario in chosen-plaintext cryptanalysis in the context of public-key cryptography, where the goal is to categorize the topic of

encrypted text. Specifically, given that the encryption technique and key are fixed and that cipher texts can be obtained for a collection of plaintexts across different topics, the goal is to develop a framework that can recognize the topic to which the ciphertext belongs. To motivate this scenario, lets consider two parties communicating through an encrypted channel on a wide range of topics [12-13]. Now, lets consider there is a listener, say a government security agency spying on the conversation for national security reasons, who is only interested in the messages related to the topic of military warfare. However, without knowledge of the topic a message belongs, decrypting every message belonging to every topic may require immense computing resources and time. Once the topic to which a message belongs is known, dedicated computing resources can be allotted to decrypt only the messages that belong to the specific topic. The resource usage and time in this case would be much less than decrypting all messages irrespective of the topic they belong. To our knowledge, this is the first time that chosen-plaintext cryptanalysis is being discussed in the context of topic-modeling.

Deep learning has shown remarkable success in various domains, from image recognition to Natural Language Processing (NLP) [14]. It is no surprise that deep learning is increasingly used in research involving cryptography [3] and cryptanalysis [15]. The proposed framework employs state-of-the-art deep learning techniques, such as Convolution Neural Networks (CNNs) [16], Gated Recurrent Units (GRUs) [17], and Long Short-Term Memory (LSTM) [18] to process sequential data. The proposed framework was evaluated on an IMDB dataset [19], using five thousand movie reviews, where the topics were realized by grouping the entire dataset into five, ten, and twenty clusters. The proposed framework achieved up to 67% precision, 99% recall, 80% F1-score, and 71% AUPR. These results are very promising and open up this subarea of cryptanalysis through topic-modeling for further research.

II. METHODOLOGY

A. Proposed Framework

Figure 1 shows the architecture of the proposed framework.

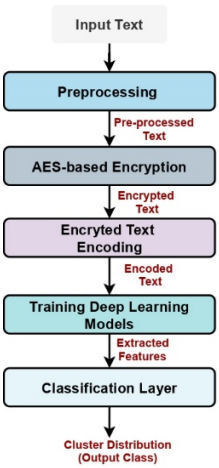

Fig. 1. The proposed framework.

The framework takes a raw English sentence as input and after performing necessary preprocessing, the output is passed to the Advanced Encryption Algorithm (AES). Then, it is converted to a machine-understandable form and fed to a deep learning-based architecture for feature learning. Finally, the proposed framework produces a class distribution for each encrypted text as output. The output class is the cluster or topic to which the encrypted message belongs. The proposed framework works in four phases: (1) preprocessing, (2) AES-based encryption, (3) encrypted text encoding, (4) training deep learning architecture, and (5) classification.

1) Preprocessing

This is the first phase of the proposed framework. It takes a text representing movie information as input and applies the following NLP-based preprocessing steps:

- Removes symbols such as punctuation marks, URL and email notations, and nonalphanumeric characters.
- Changes the case of the entire text to lowercase.
- Tokenizes input text into a stream of words or tokens [20].
- Removes stop words, such as "is", "the", "are", "of", "in", and "and".
- Applies lemmatization, by converting all words to their corresponding root form, called lemma [21].
- Removes infrequent words with a frequency less than 3 in the corpus, as a large number of infrequent words adversely affects the generalization ability of deep learning models.

2) AES-based Encryption

Once the preprocessed text is obtained, it is passed to AES-based encryption. AES-128 was used for the encryption of the preprocessed data. After encrypting the text, AES returns an output consisting of hexadecimal characters with a length of 160. This output is fed to the downstream network.

3) Encrypted Text Encoding

This is the most common phase of an NLP task, which converts text datasets into machine-understandable language using encoding methods such as one-hot encoding, bag of words, and word2vec [22]. Here, the one-hot encoding method was used to convert the series of hexadecimal characters into a numerical form called embeddings. Other encodings cannot be used here because they capture the context of a word in a language setting, say English; however, this relationship does not hold for encrypted texts, where each character may be encoded separately independently of the remaining text. One-hot coding, however, being based on first principles, fits the bill. Each character in the hexadecimal series is mapped to a 17-length encoded vector consisting of 0 and 1. Whenever one of the hexadecimal characters is encountered, the corresponding place in the vector is marked as 1, otherwise, it is marked as 0. Here, an extra bit is added to catch unknown exceptional characters. The matrix resulting from each sequence has a size of 160×17, which eventually passes to the downstream network. Here, 160 is the sequence length and 17 is the embedding size.

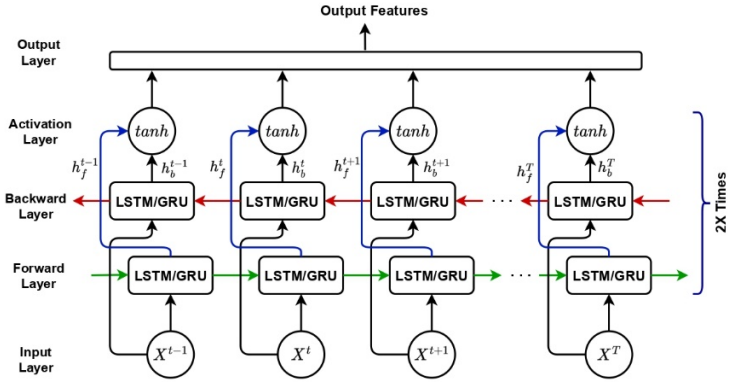

Fig. 2. Proposed bi-directional LSTM/GRU deep learning-based architecture diagram.

4) Training Deep Learning Architecture

This phase takes one-hot encoding of the encrypted text and maps its characters to the corresponding class label(s). RNNs, such as Bi-directional Long Short-Term Memory (Bi-LSTM) and Bi-directional Gated Recurrent Unit (Bi-GRU) [17], and stacked CNNs [16] were used for learning these mapping features.

5) Classification Layer

This is the last layer of this end-to-end network. Here, the number of neurons is equivalent to the number of clusters or topics. Sigmoid activation is used for each neuron at the output layer to produce the output probability corresponding to each class and address the multilevel classification problem. The network hyperparameters were binary cross-entropy with learning rate = 0.0005 as the loss function and Adam optimizer.

6) Advanced Encryption Standard (AES)

AES is a popular symmetric key block cipher that offers high security and effective encryption [23]. It works with fixed-size data blocks (128 bits) and supports keys that are 128, 192, or 256 bits long [24]. AES transforms plaintext into ciphertext using rounds, a series of substitution, permutation, and mixing operations. In this study, the text data were encrypted with 128 bits. In the discipline of cryptanalysis, flaws in cryptographic algorithms are investigated since they can jeopardize their security. Some of the common approaches used in cryptanalysis are (i) brute-force attack, (ii) differential cryptanalysis, (iii) linear cryptanalysis, (iv) side-channel attacks, and (v) related-key attacks [25]. Among these, machine learning algorithms are mainly used to optimize brute-force searches or assist in analyzing side-channel information effectively. Even using machine learning approaches, successfully breaking AES encryption through cryptanalysis remains a substantial issue [15], as its robust design ideas, mathematical foundations, and resistance to known attacks are largely responsible for its security.

B. Deep Learning-based Architecture

Deep learning models can be used in cryptanalysis to find flaws and vulnerabilities. In this regard, two RNN- and CNN-based techniques were used to investigate the mathematical relationship between the encrypted and the plain text.

1) Bi-directional LSTM (Bi-LSTM)

Bi-LSTM is primarily concerned with short- and long-range interactions, processing information in both forward and backward directions [17]. Short- and long-range interaction information is captured due to a long sequence of repeating units called memory cells. LSTM uses three different gates, i.e. the forget, input, and output gates. The forget gate helps to remove irrelevant information from the cell state and consists of a single neural network with a sigmoid activation function. The input gate adds new information to the cell state and consists of two independent neural networks with sigmoid and tanh activation functions. Lastly, the output gate that returns the final output is obtained using a single neural network layer.

2) Bi-directional GRU (Bi-GRU):

Bi-GRU is another member of the RNN family, primarily concerned with short- and long-range interactions and processing information in both forward and backward directions [18]. It consists of two gates, an update and a reset gate. The update gate mainly focuses on determining the usefulness of past information, while the reset gate focuses on leaving out irrelevant past information. Figure 2 shows the detailed architecture of bi-directional RNNs. Both the Bi-LSTM and Bi-GRU used the same hyper-parameters: number of output dimensions = 64, with dropout and recurrent dropout probability = 0.2. The input layer takes temporal input and after learning features from both directions, they are given to the activation function. The output from the activation function is given to the downstream network.

3) Convolutional Neural Networks (CNNs)

CNNs mainly focus on local patterns with fewer convolutional layers. Stacking CNN layers leads to learning a global pattern well with relatively fewer parameters. In CNNs, the weight-sharing mechanism helps the framework learn features in less time than in RNNs [16]. Figure 3 shows the architecture of the proposed stacked CNN. The input layer takes the one-hot encoding representation. This passes through the multi-block stacked CNN architecture, where each block learns a different set of information based on filter size and the number of filters. Batch normalization and dropout are used to smooth the training process and prevent overfitting. Finally, the output features of each CNN block are concatenated and fed to the downstream network for classification.

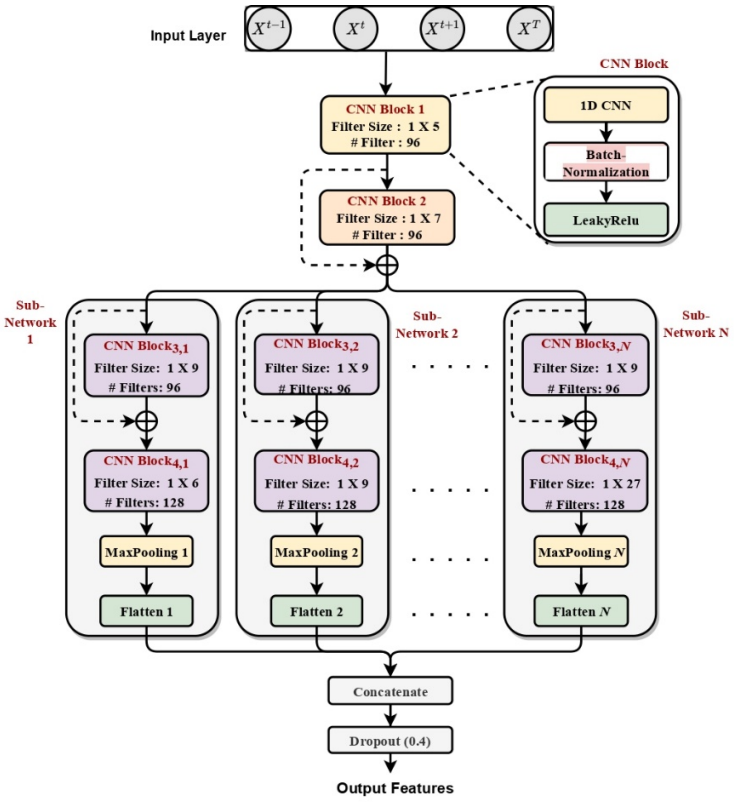

Fig. 3. Proposed stacked CNN-based deep learning architecture.

III. EXPERIMENTS AND RESULTS

A. Dataset Description

The IMDB dataset [19] was used to evaluate the proposed end-to-end architecture in the field of cryptanalysis. In this regard, the first 5000 samples of the dataset were considered. After applying different preprocessing techniques, different numbers of clusters (5, 10, and 20) of words corresponding to topics were created in the corpus of 5000 samples.

Word2vec [22] and the k-means algorithm were used to map each word to a cluster. Using word2vec, words were transformed into embeddings of size = 100, and using the k-means algorithm, these words were assigned to different-sized clusters, where each cluster corresponds to a topic. These clusters were used as class labels to the corresponding encrypted text (sequence of hexadecimal characters) in a label-encoder manner. For each sentence, embeddings with lengths of 5, 10, and 20 were created, consisting of 0 and 1. Alternatively, topics could have been manually assigned, which would have been a more accurate estimate, but also extremely time-consuming. Finally, three datasets were created using the same encrypted text and the corresponding label embeddings that represent the cluster contents. Table I shows a few samples from the datasets; the first column refers to the preprocessed text, the second refers to the encrypted text output of AES-128, and the last shows the labeling in terms of the topics the encrypted text belongs. The topic labels are represented through one-hot encoding, where a 1 denotes that the text belongs to the topic, and a 0 denotes otherwise. In this example, the number of topics represented by clusters was five.

B. Results and Discussion

Commonly used evaluation metrics were used to evaluate the performance of the proposed framework designed to break cryptographic systems using topic modeling, such as average precision and recall, F1-score, and AUPR [27-28]. These metrics help evaluate the effectiveness of cryptanalysis techniques in terms of identifying and exploiting vulnerabilities. Table II presents the results based on CNN, while Tables III and IV present the results using RNNs, i.e., Bi-LSTM and Bi-GRU, respectively. Overall, good results were obtained using the five clusters for all three deep learning-based techniques for all evaluation metrics. The best results were obtained using the Bi-GRU-based framework having the highest value for all the evaluation metrics with the five clusters. Table V compares the number of parameters across the three deep-learning models. The stacked-CNN model, consisting of multiple CNN blocks, had the greatest number of parameters, while the proposed Bi-GRU model, which performed the best, was the lightest model among the three.

The study is currently limited by the length of encrypted characters as 160 and needs to be evaluated for larger and perhaps variable lengths of encrypted text. While considering larger lengths will require access to advanced hardware configuration, dealing with variable-length encrypted text will require some sort of padding, as is common in NLP tasks that have variable-length inputs. Another limitation of this study is

that it needs to be evaluated on more datasets. Both these points will be addressed in future work. Another challenge will be to address the case of ciphertext-only and known-plaintext attacks. Cryptanalysis in the context of a ciphertext-only scenario is extremely challenging, as there is no target text against which the proposed framework can be trained. In such a scenario, one way can be to first generate some target labels manually using human expertise in ciphertext-only attacks and then train the proposed model on them.

TABLE I. SAMPLES DESCRIBING THE DATASET USED FOR EXPERIMENTS

Text	Encrypted Text	Class Label (Cluster)
one reviewer mentioned watching episode	9aec21b216421d177b5ca93b9986150c9fb5b0135a5680...	1 0 0 1 0
wonderful little production filming technique	52ef3ddd67c0a306fc301b35576342d24999fde920d5c1...	0 1 0 1 0
thought wonderful way spend time	c74d1b79d72cd59a370183b76c4c60bd722bb33cc17367...	0 1 1 1 0
jet brings charismatic presence movie	92afcde910fa42ae9494043ae79183f52f4df94eab304d...	1 0 1 1 0
interesting slasher film multiple suspect	388163bbb357c6a3ad925df98ec1d761466406c25c8fdf...	1 1 0 1 0

TABLE II. RESULTS USING CNN-BASED FRAMEWORK WITH VARYING NUMBER OF CLUSTERS

#Clusters / Performance metric	5	10	20
Precision	0.67	0.48	0.23
Recall	0.80	0.37	0.97
F1-Score	0.72	0.42	0.37
AUPR	0.66	0.46	0.30

TABLE III. RESULTS USING BI-LSTM-BASED FRAMEWORK WITH VARYING NUMBER OF CLUSTERS

#Clusters / Performance metric	5	10	20
Precision	0.65	0.58	0.86
Recall	0.99	0.14	0.80
F1-Score	0.78	0.23	0.37
AUPR	0.68	0.49	0.28

TABLE IV. OBTAINED RESULTS USING BI-GRU-BASED FRAMEWORK WITH VARYING NUMBER OF CLUSTERS

#Clusters / Performance metric	5	10	20
Precision	0.67	0.55	0.24
Recall	0.99	0.14	0.89
F1-Score	0.80	0.22	0.37
AUPR	0.71	0.48	0.29

TABLE V. PARAMETER COMPARISON AMONG THE DIFFERENT MODELS

#Cluster / DL-Models	5	10	20
Bi-LSTM	157,957	158,602	159,892
Bi-GRU	123,525	124,170	125,460
Stacked-CNN	1,577,189	1,581,034	1,588,724

IV. CONCLUSION

This paper presented a novel approach to chosen-plaintext cryptanalysis in the context of topic modeling. This approach uses neural networks to categorize the topic of encrypted text, which can be used to gain insights into the plaintext without actually decrypting it. To our knowledge, this is the first time that chosen-plaintext cryptanalysis has been discussed in the context of topic modeling. This study used modern deep-learning techniques such as CNN, GRU, and LSTM to process sequential data. The results obtained on the IMDB dataset showed 67% precision, 99% recall, 80% F1-score, and 71% AUPR. This study opens up new avenues for research in the field of cryptanalysis, as neural networks could be used to develop more powerful and efficient attacks on a variety of encryption schemes.

REFERENCES

[1] T. Dong and T. Huang, "Neural Cryptography Based on Complex-Valued Neural Network," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 31, no. 11, pp. 4999–5004, Aug. 2020, https://doi.org/10.1109/TNNLS.2019.2955165.

[2] M. Gupta, M. Gupta, and M. Deshmukh, "Single secret image sharing scheme using neural cryptography," *Multimedia Tools and Applications*, vol. 79, no. 17, pp. 12183–12204, May 2020, https://doi.org/10.1007/s11042-019-08454-8.

[3] M. A. Al-Shabi, "A Survey on Symmetric and Asymmetric Cryptography Algorithms in information Security," *International Journal of Scientific and Research Publications (IJSRP)*, vol. 9, no. 3, Mar. 2019, Art. no. p8779, https://doi.org/10.29322/IJSRP.9.03.2019.p8779.

[4] A. H. Al-Omari, "Lightweight Dynamic Crypto Algorithm for Next Internet Generation," *Engineering, Technology & Applied Science Research*, vol. 9, no. 3, pp. 4203–4208, Jun. 2019, https://doi.org/10.48084/etasr.2743.

[5] A. S. Alshammari, "Comparison of a Chaotic Cryptosystem with Other Cryptography Systems," *Engineering, Technology & Applied Science Research*, vol. 10, no. 5, pp. 6187–6190, Oct. 2020, https://doi.org/10.48084/etasr.3745.

[6] N. Carlini, M. Jagielski, and I. Mironov, "Cryptanalytic Extraction of Neural Network Models," in *Advances in Cryptology – CRYPTO 2020*, Santa Barbara, CA, USA, 2020, pp. 189–218, https://doi.org/10.1007/978-3-030-56877-1_7.

[7] E. Barkan, E. Biham, and N. Keller, "Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication," in *Advances in Cryptology - CRYPTO 2003*, Santa Barbara, CA, USA, 2003, pp. 600–616, https://doi.org/10.1007/978-3-540-45146-4_35.

[8] F. Wang, J. Sang, Q. Liu, C. Huang, and J. Tan, "A deep learning based known plaintext attack method for chaotic cryptosystem." arXiv, Mar. 09, 2021, https://doi.org/10.48550/arXiv.2103.05242.

[9] N. Munir, M. Khan, A. Al Karim Haj Ismail, and I. Hussain, "Cryptanalysis and Improvement of Novel Image Encryption Technique Using Hybrid Method of Discrete Dynamical Chaotic Maps and Brownian Motion," *Multimedia Tools and Applications*, vol. 81, no. 5, pp. 6571–6584, Feb. 2022, https://doi.org/10.1007/s11042-021-11810-2.

[10] A. M. Qadir and N. Varol, "A Review Paper on Cryptography," in *2019 7th International Symposium on Digital Forensics and Security (ISDFS)*, Barcelos, Portugal, Jun. 2019, pp. 1–6, https://doi.org/10.1109/ISDFS.2019.8757514.

[11] Y. Zhang and D. Xiao, "Cryptanalysis of S-box-only chaotic image ciphers against chosen plaintext attack," *Nonlinear Dynamics*, vol. 72, no. 4, pp. 751–756, Jun. 2013, https://doi.org/10.1007/s11071-013-0750-x.

[12] N. Q. Luc, T. T. Nguyen, D. H. Quach, T. T. Dao, and N. T. Pham, "Building Applications and Developing Digital Signature Devices based on the Falcon Post-Quantum Digital Signature Scheme," *Engineering, Technology & Applied Science Research*, vol. 13, no. 2, pp. 10401–10406, Apr. 2023, https://doi.org/10.48084/etasr.5674.

[13] V. H. Le, N. Q. Luc, T. T. Dao, and Q. T. Do, "Building an Application that reads Secure Information Stored on the Chip of the Citizen Identity Card in Vietnam," *Engineering, Technology & Applied Science Research*, vol. 13, no. 1, pp. 10100–10107, Feb. 2023, https://doi.org/10.48084/etasr.5531.

[14] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," *Nature*, vol. 521, no. 7553, pp. 436–444, May 2015, https://doi.org/10.1038/nature14539.

[15] S. Sikdar and M. Kule, "Recent Trends in Cryptanalysis Techniques: A Review," in *Proceedings of International Conference on Frontiers in Computing and Systems*, Singapore, 2023, pp. 209–222, https://doi.org/10.1007/978-981-99-2680-0_19.

[16] Z. Li, F. Liu, W. Yang, S. Peng, and J. Zhou, "A Survey of Convolutional Neural Networks: Analysis, Applications, and Prospects," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 33, no. 12, pp. 6999–7019, Sep. 2022, https://doi.org/10.1109/TNNLS.2021.3084827.

[17] J. Chung, C. Gulcehre, K. Cho, and Y. Bengio, "Empirical Evaluation of Gated Recurrent Neural Networks on Sequence Modeling." arXiv, Dec. 11, 2014, https://doi.org/10.48550/arXiv.1412.3555.

[18] G. Van Houdt, C. Mosquera, and G. Nápoles, "A review on the long short-term memory model," *Artificial Intelligence Review*, vol. 53, no. 8, pp. 5929–5955, Dec. 2020, https://doi.org/10.1007/s10462-020-09838-1.

[19] "IMDB Dataset of 50K Movie Reviews." https://www.kaggle.com/datasets/lakshmi25npathi/imdb-dataset-of-50k-movie-reviews.

[20] J. J. Webster and C. Kit, "Tokenization as the initial phase in NLP," in *Proceedings of the 14th conference on Computational linguistics* -, Nantes, France, 1992, vol. 4, pp. 1106-1110, https://doi.org/10.3115/992424.992434.

[21] K. Divya, B. S. Siddhartha, N. M. Niveditha, and B. M. Divya, "An Interpretation of Lemmatization and Stemming in Natural Language Processing," *Journal of University of Shanghai for Science and Technology*, vol. 22, no. 10, pp. 350–357, Oct. 2020.

[22] K. W. Church, "Word2Vec," *Natural Language Engineering*, vol. 23, no. 1, pp. 155–162, Jan. 2017, https://doi.org/10.1017/S1351324916000334.

[23] E. S. I. Harba, "Secure Data Encryption Through a Combination of AES, RSA and HMAC," *Engineering, Technology & Applied Science Research*, vol. 7, no. 4, pp. 1781–1785, Aug. 2017, https://doi.org/10.48084/etasr.1272.

[24] S. Heron, "Advanced Encryption Standard (AES)," *Network Security*, vol. 2009, no. 12, pp. 8–12, Dec. 2009, https://doi.org/10.1016/S1353-4858(10)70006-4.

[25] H. Zodpe and A. Shaikh, "A Survey on Various Cryptanalytic Attacks on the AES Algorithm," *International Journal of Next-Generation Computing*, pp. 115–123, 2021.

[26] K. P. Sinaga and M.-S. Yang, "Unsupervised K-Means Clustering Algorithm," *IEEE Access*, vol. 8, pp. 80716–80727, 2020, https://doi.org/10.1109/ACCESS.2020.2988796.

[27] U. Iftikhar, K. Asrar, M. Waqas, and S. A. Ali, "Evaluating the Performance Parameters of Cryptographic Algorithms for IOT-based Devices," *Engineering, Technology & Applied Science Research*, vol. 11, no. 6, pp. 7867–7874, Dec. 2021, https://doi.org/10.48084/etasr.4263.

[28] R. J. Rasras, Z. A. AlQadi, and M. R. A. Sara, "A Methodology Based on Steganography and Cryptography to Protect Highly Secure Messages," *Engineering, Technology & Applied Science Research*, vol. 9, no. 1, pp. 3681–3684, Feb. 2019, https://doi.org/10.48084/etasr.2380.