ISSN: 2454-9940

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

E-Mail :
editor.ijasem@gmail.com
editor@ijasem.org

www.ijasem.org

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN2454-9940

www.ijasem.org

Vol 18, Issue 2, 2024

A Spam Transformer Model for SMS Spam Detection

[1]MR.A N L KUMAR, [2]ASWINI BANDARU

[1](Associate Professor), MCA, Swarnandhra College

[2]MCA, scholar, Swarnandhra College

ABSTRACT

Our goal in writing this study is to investigate whether or not the Transformer model may be used to identify spam SMS messages by suggesting a tweaked version of the model specifically for this purpose. We utilize UtkMl's Twitter Spam Recognition Rivalry dataset and SMS Spam Assortment v.1 dataset to test our proposed spam Transformer. We utilize various notable AI classifiers and state of the art techniques for SMS spam recognition as our benchmarks. The proposed better spam Transformer beats any remaining choices in our SMS spam discovery studies, with a review of 0.9451 percent, a precision of 98.92 percent, and a F1-Score of 0.9613 percent. Likewise, the proposed model excels on UtkMl's Twitter dataset, which bodes well for applying it to other comparable issues.

1.INTRODUCTION

Due to the explosion in mobile phone and mobile network use over the last few decades, the Short Message Service (SMS) has become an invaluable tool for communication. Still, SMS spam is a problem for SMS users as well. Distractions sent over mobile networks are referred to as SMS spam, or drunk message. There are a number of factors that contribute to the widespread use of spam messages. Firstly, the potential number of victims of the spam message assault is considerable since there are a big number of people who use mobile phones worldwide. Two, spammers may be pleased to hear that sending out spam doesn't cost much. On a final note,

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT
ISSN2454-9940
www.ijasem.org
Vol 18, Issue 2, 2024

most mobile phones' spam classifiers aren't very good at what they do since they lack the processing power to properly and effectively detect spam messages.

There are a plethora of categorization applications based on machine learning across several study domains, and machine learning has been one of the most fashionable subjects in recent decades. In particular, there are a number of well-established approaches to spam identification, which is an area of study that has been around for a while. To be sure, a large number of machine learning classifiers relied on manually derived features from training data

With the exponential increase in computing power over the last several decades, deep learning—a subfield of machine learning—has been booming in popularity and innovation. Applications built on deep learning are becoming more important in modern culture, simplifying many parts of our daily lives. Among the most popular and successful deep learning architectures, Recurrent Neural Networks (RNNs) and its derivatives, such as Long Short-Term Memory (LSTM), have recently shown remarkable effectiveness in spam identification

The Transformer is an attention-based sequence-to-sequence model that succeeded admirably in translating between English and German and English and French. Its initial purpose was to do translation tasks. In addition, certain new and better Transformer-based models have been suggested to tackle various NLP issues, including GPT and BERT. Successors to the Transformer have shown via their achievements just how strong and promising they are. It is our hope that this research will help shed light on the possibility of using the Transformer model to the challenge of SMS spam identification. Hence, to detect SMS spam, we provide a modified model that is based on the classical Transformer. In addition, we evaluate and contrast the efficacy of conventional ML classifiers, a long short-term memory (LSTM) deep learning approach, and the spam Transformer model that we have developed for detecting spammed SMS.

2.LITERATURE SURVEY

ISSN2454-9940

www.ijasem.org

Vol 18, Issue 2, 2024

1. "A Survey of SMS Spam Detection Techniques & quot; : A wide range of methods for identifying spam SMS messages are covered in detail inthis article. It goes over both older and newer methods of machine learning, including decision trees, support vector machines, and naivebayes, as well as deep learning techniques like CNNs and RNNs. It outlines the challenges and limitations of each approach and sets thestage for exploring newer models like the Transformer in spam detection.

2. "Models for Natural Language Processing Based on Transformers & quot; : The improvements in natural language processing tasks brought about by Transformer-based models are explored in this survey report. It delves into the inner workings of the Transformer model, covering topics like positional encoding and self-attention processes, and how it has been used to tasks like sentiment analysis, text summarization, and machine translation. If we want to modify the Transformer to recognize SMS spam, we must master these ideas.

3. "Recent Advances in SMS Spam Detection": Focusing specifically on SMS spam detection, this review paper discusses recent advancements in the field. In doing so, it draws attention to the shortcomings of current methods and the need for more powerful alternatives, including both conventional and deep learning techniques. The suggested updated Transformer model is only one example of how this article lays the groundwork for investigating fresh avenues of inquiry.

4. "Evaluation Metrics for Text Classification": The article delves into the assessment measures often used in text categorization tasks, such as F1-score, recall, accuracy, and precision. In order to evaluate the suggested updated Transformer model against other machine learning classifiers and cutting-edge methods for detecting SMS spam, familiarity with these measures is crucial.

5. " Presented by UtkMl: The Twitter Spam Detection Results": This report details the outcomes of a competition focused on detecting spam on Twitter, providing valuable insights into the challenges and strategies employed in spam

ISSN2454-9940

www.ijasem.org

Vol 18, Issue 2, 2024

detection for social media data. While the dataset differs from SMS data, the techniques and insights gained from this competition can inform the adaptation of the proposed model to similar problems. Researchers may learn everything they need to know about the current state of SMS spam detection methods, the improvements made by Transformer- based models, and the evaluation criteria needed to measure the proposed model's effectiveness by reading these articles. Additionally, insights from related competitions and surveys provide valuable context for the proposed research and its potential applications beyond SMS spam detection.

3. SYSTEM DESIGN

Developing and designing systems

INPUT DESIGN

Since Information Configuration is so essential to the product advancement life cycle, designers should give close consideration to it. The objective of the information configuration is to give the application with highly accurate data. Therefore, inputs should be carefully structured to reduce feeding mistakes to a minimum. The goal of designing input forms or screens with validation controls over input range, limit, and associated validations is to adhere to software engineering concepts. Almost every module in this system has an input screen. In order to prevent users from making erroneous inputs, error messages are designed to notify them anytime they make a mistake and provide guidance on how to proceed correctly. In the context of module design, let's take a close look at this. Designing input is taking user-created content and transforming it into a computer-readable format. A logical and error-free data entering process is the aim of the input design. The input design controls the input errors. A user-friendly approach was used in developing the program. A pointer is automatically put in the field that needs to be filled out during processing because of how the forms were constructed. In certain instances, the user is additionally given the opportunity to choose the most suitable input from a list of choices that are relevant to the field. All input data must undergo validations. After finishing all the fields on the current page, the user may go to the next

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN2454-9940

www.ijasem.org

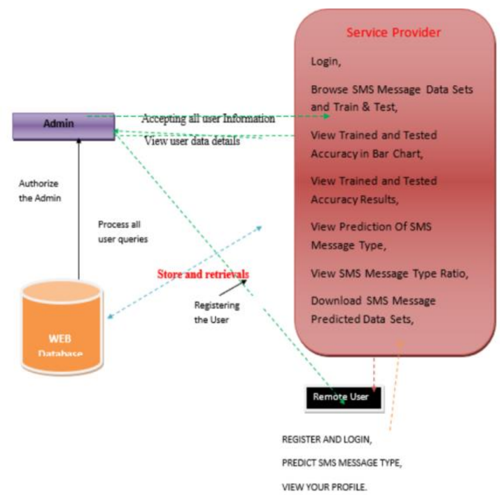
Vol 18, Issue 2, 2024

ones if an error message is shown whenever they submit incorrect data.

DESIGN OF OUTPUT

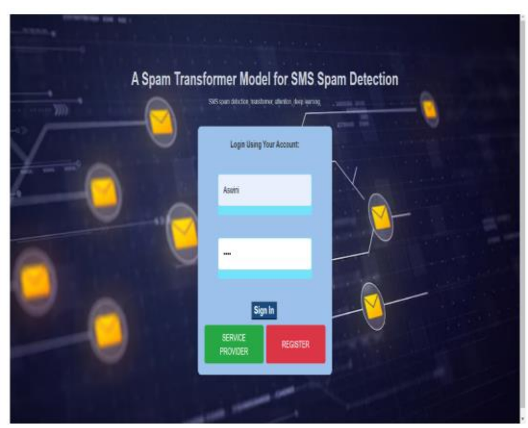
The primary purpose of the computer's output is to facilitate effective internal communication inside the organization, particularly between the project manager and his team members, or between the administrator and the customers. In terms of client management, VPN produces a system that lets the project manager create new clients, assign them projects, track when those projects are still active, and grant each client user-level access to folders based on the projects assigned to them. It is possible to assign the customer a new project when an existing one is finished. Authentication methods for users are up and running from the very beginning. Although either the administrator or an existing user may create a new user, only the administrator has the authority to validate a new user and give them projects. When started for the first time, the program begins operating. Before using Internet Explorer as a browser, the server must be launched. Working on a local area network allows the server computer to take on the role of administrator while the other linked systems play the role of clients for the project. Even someone using it for the first time will have no trouble understanding the built system because of how user pleasant it is.

Architecture Diagram



4.OUTPUT SCREENS

Login:



INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN2454-9940

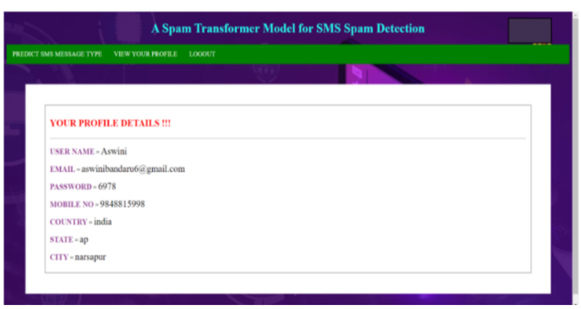
www.ijasem.org

Vol 18, Issue 2, 2024

Registration Form:

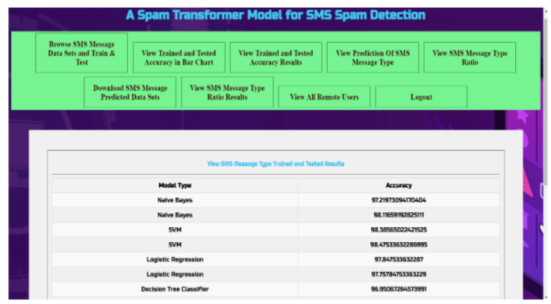
Predict SMS Type:

View Profile:

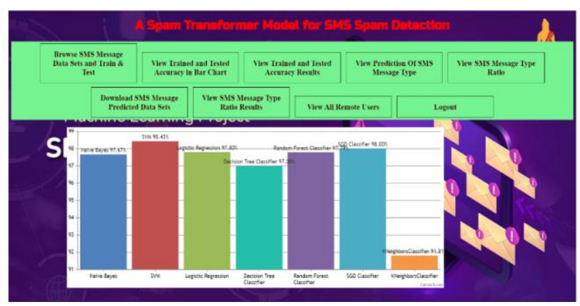


Service Provider Login:

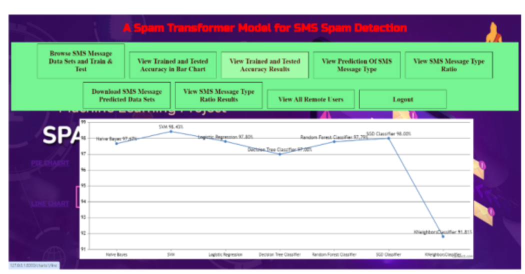
Train and Test Model:



Bar Chat:



Accuracy Results:



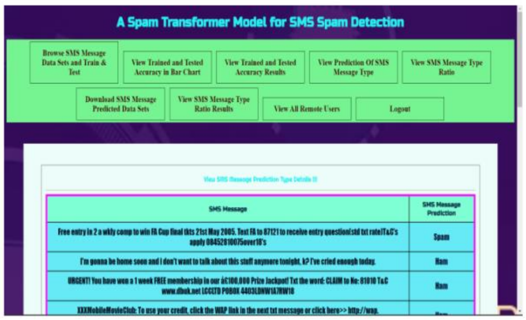
INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN2454-9940

www.ijasem.org

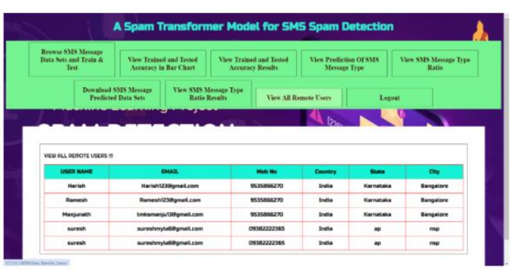
Vol 18, Issue 2, 2024

Predict SMS Type details:



SMS Ratio:

Remote User:



5.CONCLUSION

To combat SMS spam, we provide a tweaked Transformer model in this study. We compared our spam Transformer model to numerous different techniques for identifying SMS spam utilizing the SMS Spam Assortment v.1 dataset and UtkMl's Twitter dataset for assessment purposes. We found that our recommended spam Transformer model beats Calculated Relapse, Innocent Bayes, Irregular Woods, Backing Vector Machine, Long Momentary Memory, and CNN-LSTM [22] on both datasets. Our spam transformer beats contending classifiers on the SMS Spam Assortment v.1 dataset across a few measurements, including exactness, review, and F1-Score. Our changed spam Transformer technique specifically had a striking result on F1-Score. In addition, our updated spam Transformer model outperformed the other alternative techniques discussed in this study on all four metrics when tested on UtkMl's Twitter dataset. To be more specific, our spam Transformer has a high F1-Score because of its outstanding recall performance.

6. REFERENCES

[1] P. K. Roy, J. P. Singh, and S. Banerjee, ``Deep learning to _lter SMS spam,''

ISSN2454-9940

www.ijasem.org

Vol 18, Issue 2, 2024

Future Gener. Comput. Syst., vol. 102, pp. 524_533, Jan. 2020.

[2] G. Jain, M. Sharma, and B. Agarwal, ``Optimizing semantic LSTM forspam detection,'' Int. J. Inf. Technol., vol. 11, no. 2, pp. 239_250, Jun. 2019.

[3] A. Vaswani, N. Shazeer, N. Parmar, J. Uszkoreit, L. Jones, A. N.Gomez, L. Kaiser, and I. Polosukhin, ``Attention is all you need,'' in Proc. Adv.Neural Inf. Process. Syst., 2017, pp. 5999_6009.

[4] T. B. Brown et al., ``Language models are few-shot learners,'' 2020, arXiv:2005.14165. [Online]. Available: http://arxiv.org/abs/2005.14165

[5] J. Devlin, M.-W. Chang, K. Lee, and K. Toutanova, ``BERT: Pre-training of deep bidirectional transformers for language understanding,'' in Proc.

Conf. North Amer. Chapter Assoc. Comput. Linguistics, Hum. Lang. Tech- nol., vol. 1, Jun. 2019, pp. 4171_4186.

[6] G. Sonowal and K. S. Kuppusamy, ``SmiDCA: An anti-Smishing model with machine learning approach,'' Comput. J., vol. 61, no. 8, pp. 1143_1157, Aug. 2018.

[7] J. W. Joo, S. Y. Moon, S. Singh, and J. H. Park, ``S-detector: An enhanced security model for detecting Smishing attack for mobile computing,'' Telecommun. Syst., vol. 66, no. 1, pp. 29_38, Sep. 2017.

[8] S. Mishra and D. Soni, ``Smishing detector: A security model to detect Smishing through SMS content analysis and URL behavior analysis,'' Future Gener. Comput. Syst., vol. 108, pp. 803_815, Jul. 2020.

[9] C. Li, L. Hou, B. Y. Sharma, H. Li, C. Chen, Y. Li, X. Zhao, H. Huang, Z. Cai, and H. Chen, ``Developing a new intelligent system for the diagnosis of tuberculous pleural effusion,'' Comput. Methods Programs Biomed., vol. 153, pp. 211_225, Jan. 2018.

[10] T. K. Ho, ``Random decision forests,'' in Proc. Int. Conf. Document Anal.

Recognit. (ICDAR), vol. 1, 1995, pp. 278_282.