PROJECT REPORT

On

“AI/ML FOR NETWORKING”

Submitted as part of the requirements for Industrial Training under Intel Corporation.

SUBMITTED BY

Baibhav Kumar
Hetav Desai

TABLE OF CONTENTS

1. Acknowledgment
2. Abstract
3. Introduction
4. Methodology and Optimization
5. System Architecture
6. Result and Discussions
7. Implementation
8. Conclusion
9. References

1.ACKNOWLEDGMENT

We extend my heartfelt gratitude to **Dr Meenakshi K** for their invaluable mentorship and support throughout this project. We would also like to express my appreciation to my peers and institution for their unwavering encouragement and provision of essential resources.

2.ABSTRACT

XSS (Cross-site scripting) is a web security vulnerability where attacker inject malicious scripts into web pages or web application when we give a request to the server, the main motivation behind this project was to detect these attacks before hand and reduce the risks of the users .Traditional approaches fail to handle this security flaw so in order to tackle this we propose a deep learning hybrid CNN and BiLSTM model to detect the XSS attacks from raw HTML/Javascript inputs. We use character level tokenizer to ensure that we can detect even the granular learning of patterns within the given payloads .The model that we developed achieved a 99% accuracy on real world application across various diverse inputs.

This provides a scalable and effective way to improve web application security using deep learning.

3.INTRODUCTION

In todays time where people mostly depend on the internet for shopping, social media ,banking and transactions making it easier for cybercriminals to hack online portals and steal users sensitive information. On the other hand the common public is unaware of the black ethics that are used by the hackers and it is impractical to spread cyber awareness among all the individuals ,so to make a system that detects it beforehand so that we can mitigate the effects of these attacks.

Cross-site scripting (XSS) continues to be one of the major threat in case of cyberattacks allows attackers to execute arbitrary JavaScript in a user's browser, enabling data theft, session hijacking, and defacement .Traditional approaches struggle to handle this security flaw.

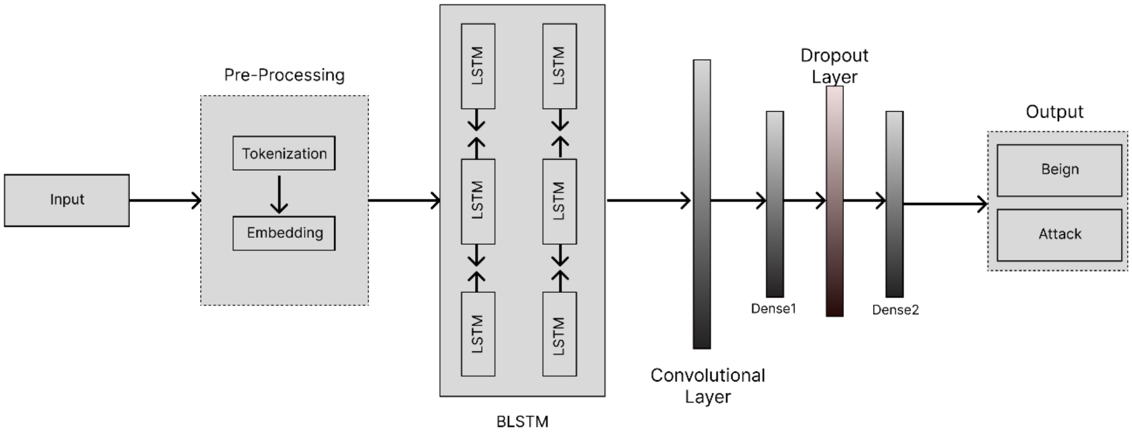
Recent advancements in deep learning have shown promise in text-based classification tasks, including cyber threat detection. In this project, we use a hybrid deep learning architecture combining CNN for feature extraction and BiLSTM for learning sequential patterns. We tokenize input data at the character level to capture fine-grained syntactic patterns and train the model to distinguish between safe and malicious HTML inputs.

4.METHODOLOGY& OPTIMIZATION

Models based on CNN to detect XSS attacks automatically extracts features in the data. This avoids the manual feature extraction. However, CNN models cannot learn the temporal correlation of intrusion data. BiLSTM models for Cross-Site Scripting can discover persistent attack behavior by extraction of the bidirectional features in data. Therefore, combining the advantages on CNN and BiLSTM mechanism, this project proposes XSS Attacks detection Using model based on CNN-BiLSTM.

The CNN layer helps in generating spatial features by providing multiple convolutional and pooling layers.The BiLSTM layer captures bi-directional features learning the throughput given by CNN layer. Unlike classical ML or basic deep learning model our is CNN combined with BiLSTM hybrid model excels in both structural and contextual recognition of XSS-Attacks, which achieved more than 99 percent accuracy.

5.SYSTEM ARCHITECTURE



6.RESULT & DISCUSSIONS

Performance Metrics

- Training Accuracy: In training we achieved a performance of a staggering 98% which suggest the model was trained perfectly
- Validation Accuracy: As for the validation accuracy it maintained a 99.8 %showing excellent results during training.
- Test Accuracy: Achieved over 99%, confirming robust real-world performance.

Machine Learning Models Implemented

Accuracy/Loss plot

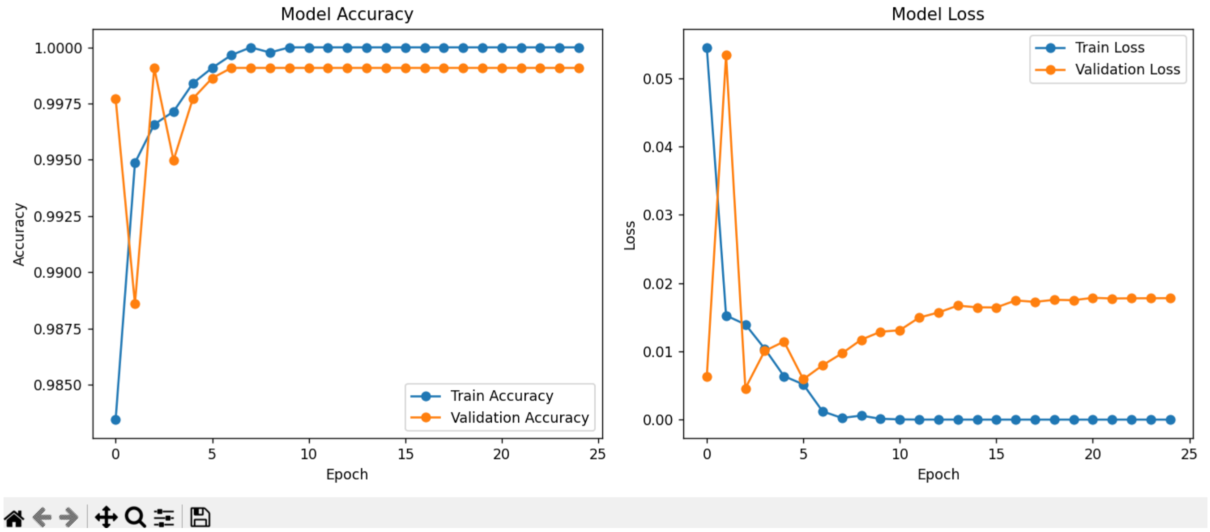


Figure 6.1

7.IMPLEMENTATION

7.1 Demo video

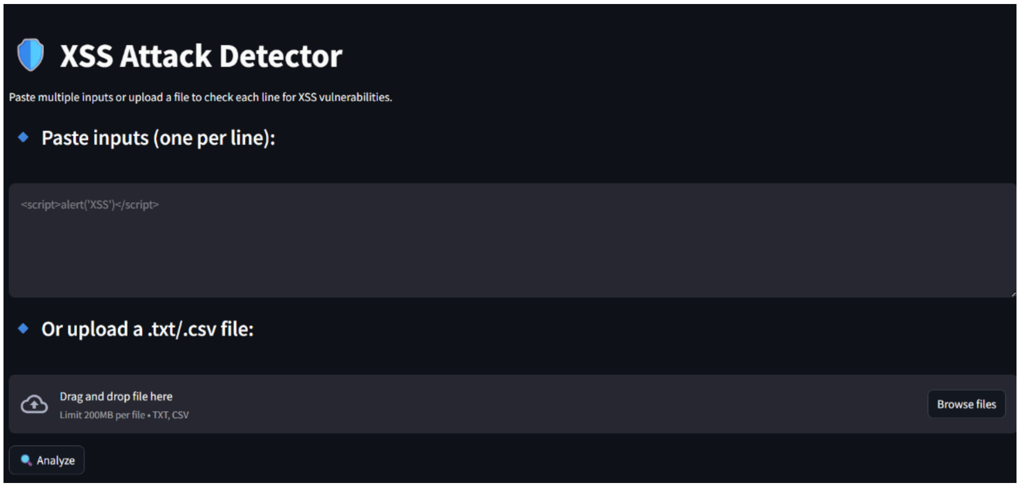
Video Link

7.2Github Link

Github Repository

7.3 Streamlit link

XSSdetector



XSS Attack Detector

Paste multiple inputs or upload a file to check each line for XSS vulnerabilities.

Paste inputs (one per line):

<script>alert('XSS')</script>

Or upload a .txt/.csv file:

Drag and drop file here

Limit 200MB per file • TXT, CSV

Figure 7.1

8.CONCLUSION

This AI-powered learning system successfully delivers a highly personalized educational experience. By implementing predictive analytics, content adaptation, and AI-driven search, the platform enhances student engagement and learning effectiveness. Despite challenges such as data integrity and computational efficiency, the system demonstrates strong potential for scalability and future enhancements. Ongoing improvements will focus on refining AI models, mitigating biases, and further optimizing user experience.

9.REFERENCES

- https://www.researchgate.net/publication/379687141_Network_Intrusion_Detection_Method_Based_on_CNN_BiLSTM_and_Attention_Mechanism
- https://ieeexplore.ieee.org/document/10273958
- https://www.researchgate.net/publication/368737792_Cross_Site_Scripting_Attack_Detection_Approach_Based_on_LSTM_Encoder-Decoder_and_Word_Embeddings
- https://link.springer.com/chapter/10.1007/978-981-99-1588-0_1