accuracy of 85.38%. The second model employed SoftSign and linear activation functions with RMSPROP optimizer. It achieved an accuracy of 93.16% for 100 epochs at a batch size of 1000, 92.97% for 200 epochs at batch size of 1000, and 93.72% for 100 epochs at a batch size of 1000. The third model was based on GRU architecture, and it achieved an accuracy of 85.01%.

However, the model showed an absurd plot at some points, which indicated that the model overfitted the training data. The fourth model was based on BiLSTM architecture, and it achieved the best results with an accuracy of 93.25%. The BiLSTM model was not overfitting as it had a close match between the training and testing accuracy curves as shown in Fig.3.

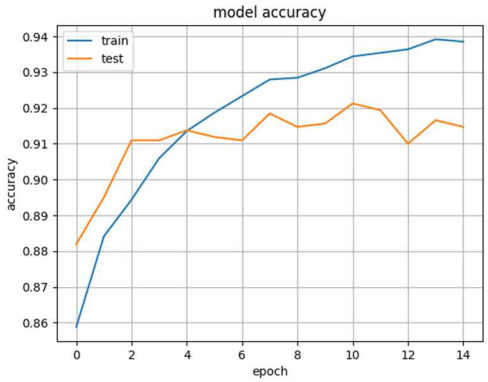

Fig. 3. The graph depicts the test vs train accuracy of model for 14 epochs wherein the accuracy of model hovers around 93.25%

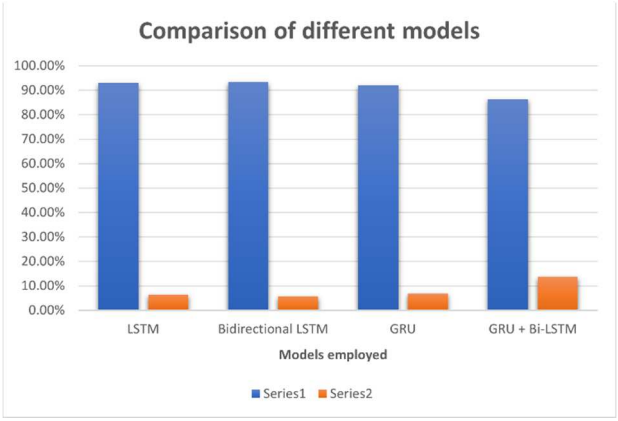

Fig. 4. The above graph represents the accuracy and loss of all 4 approaches used

Thus, this study demonstrated the effectiveness of deep learning models in classifying malware data. The BiLSTM architecture, with its appropriate hyperparameters and activation functions, yielded the best results, achieving an accuracy rate of 93.25% and loss of 5.72%. The findings emphasize the significance of architecture selection, activation functions, and optimization techniques in achieving superior performance. Future studies can further explore alternative deep learning architectures and optimization strategies to enhance the accuracy of malware classification. Evaluation metrics of different models are listed in Table. II.

TABLE. II. METRIC EVALUATION FOR DIFFERENT MODELS

Model	Activation Function		Optimizer	Accuracy	Loss
	Initial Layers	*Output Layer*			
LSTM	Relu	Softplus	Adam	85.38%	13.99%
	Softsign	Linear	Rmsprop	93.06%	6.46%
Bidirectional LSTM	Softsign	Linear	Adam	93.25%	5.72%
GRU	Softsign	Linear	Adam	91.94%	6.80%

V. CONCLUSION

The challenge of detecting metamorphic malware remains a pressing issue in the field of information security. This study proposes a novel deep learning-based approach using Bidirectional LSTM (BiLSTM) to detect metamorphic malware based on attack vectors. The performance of BiLSTM is compared against other recurrent neural networks (RNNs) such as Long Short-Term Memory (LSTM) and Gated Recurrent Unit (GRU), as well as a hybrid model of BiLSTM and GRU. The models are trained on a comprehensive dataset containing eight categories of metamorphic malware. The results demonstrate that BiLSTM outperforms other RNNs with the highest accuracy of 93.25%. This approach could significantly enhance current malware detection techniques and improve the overall security of computer systems. By focusing on utilizing attack vectors based on API calls, the research contributes a practical and effective approach to detect metamorphic malware in real-world scenarios. This practicality enhances the applicability of the proposed method and reinforces its potential for implementation in diverse information security systems. While the paper focuses on metamorphic malware, the proposed approach can be extended to detect and classify other types of malware and cyber threats. This flexibility and generalizability expand the impact of this work beyond the specific problem of metamorphic malware, contributing to the broader field of malware detection. Additionally, this method could be extended to other types of malware and cyber threats. One limitation of this study is the reliance on a specific dataset, which may not fully capture the diversity and complexity of metamorphic malware encountered in real-world scenarios but future research can explore more advanced deep learning models to improve detection accuracy and the development of more comprehensive datasets for training and testing.

REFERENCES

[1] Javaheri, D., Lalbakhsh, P., & Hosseinzadeh, M. (2021). A novel method for detecting future generations of targeted and metamorphic malware based on genetic algorithm. IEEE Access, 9, 69951-69970.

[2] Mumtaz, Z., Afzal, M., Iqbal, W., Aman, W., & Iltaf, N. (2021). Enhanced Metamorphic Techniques-A Case Study Against Havex Malware. IEEE Access, 9, 112069-112080.

[3] Vinayakumar, R., Alazab, M., Soman, K. P., Poornachandran, P., & Venkatraman, S. (2019). Robust intelligent malware detection using deep learning. IEEE Access, 7, 46717-46738.

[4] Korine, R., & Hendler, D. (2021). DAEMON: dataset/platform-agnostic explainable malware classification using multi-stage feature mining. IEEE Access, 9, 78382-78399.