Cross-Modal Sentinel: Attention-Driven Malware Classification from Non-Disassembled Files

Qudsiya Fatima[1], Dr. Md. Ateeq Ur Rahman[2], Subramanian K.M.

[1]PG Scholar, Department of CSE, Shadan College of Engineering and Technology, Hyderabad, Telangana, India -500086 fatimaqudsiya0@gmail.com

[2]Professor, Department of CSE, Shadan College of Engineering and Technology, Hyderabad, Telangana, India -500086 mail_to_ateeq@yahoo.com

[3]Professor, Department of CSE, Shadan College of Engineering and Technology, Hyderabad, Telangana, India -500086 kmsubbu.phd@gmail.com

ABSTRACT:

Combating the growth of dangerous software versions relies heavily on malware classification. In order to overcome this problem and avoid using inaccurate disassembled code, this study presents a new method that uses a "Convolutional Neural Network (CNN)"-based model to group malware samples into families. Rather than using deconstructed binary files, the model combines structural entropies with images of malware. By offering new views of the data, these modalities improve the precision of classification. To overcome the shortcomings of each modality, we use a cross-modal attention method to combine their best aspects. The research shows that the suggested model outperforms more conventional approaches, such as "VGG16, CNN, and XGBoost", with a total accuracy of 98%. Xception model adoption and ensemble techniques like Voting Classifier and Decision Tree are being investigated as ways to improve performance even further, with the goal of reaching or exceeding 99% accuracy. For testing and authentication, we also build a user-friendly interface using the Flask framework. Malware analysis is made more accessible and secure with this all-encompassing method, which also improves the accuracy of malware classification.

Keywords: "INDEX TERMS Malware Classification, Structural Entropy, Malware Image, Deep Learning, Convolutional Neural Network, Attention Mechanism".

1. INTRODUCTION

A dramatic increase in distance education & telecommuting has resulted from the COVID-19 epidemic, which has altered traditional classroom dynamics. These innovations have brought new cybersecurity risks, but they have also made education & commercial operations more continuous. By taking advantage of people's natural curiosity in things like vaccines, government regulations, & online meeting schedules, bad actors have begun towards undertake sophisticated social phishing attempts [1].

Cybercriminals have seen remote collaboration platforms as a lucrative way towards transmit malware as more & more organizations & individuals use them. Furthermore, malware has advanced at a rapid pace during the epidemic, among increasingly complex harmful software logic. Malware samples now display an average of 12 dangerous behaviors, reflecting the ever-changing cyber threat landscape [1].

Malware family classification is becoming crucial due towards the increasing sophistication & frequency of malware attacks. Grouping malware samples into different families is called malware

family classification. Each family has its own individual attack strategy, behavioral traits, or shared code fragments [2, 3]. This categorization helps among specific defensive strategy development & makes malware analysis more efficient by giving analysts heuristics towards break down malware samples from known families.

Classifying malware families used towards endure a laborious process that required analysts towards manually examine each version considering similarities. Unfortunately, manual classification approaches abide no longer sufficient due towards the fast growth & spread of new kinds of malware. Researchers have responded by adopting automated methods that make use of machine learning and, more lately, deep learning.

Deep learning has been incredibly successful in many disciplines, such as computer vision & natural language processing. It is a subset of machine learning that uses artificial neural networks among numerous layers of abstraction. among its many benefits over more traditional machine learning techniques, deep learning-based malware family classification is quickly becoming a popular strategy in the cybersecurity industry [4, 5, 6].

Deep learning models have the ability towards autonomously learn meaningful characteristics from raw data, in contrast towards typical machine learning models that depend on features that abide built by specialists. among this power, deep learning models can analyze complicated datasets, including features collected from malware samples, both dynamic & static, & identify detailed patterns & correlations within them [7, 8]. Y

ou can learn a lot about dangerous behaviors by observing dynamic aspects, like how malware behaves while running. Extracting these features involves running malware in a controlled environment, such a virtual machine, & observing its network behavior, memory usage, registry changes, & execution routes, as well as the sequences of API calls. But, there abide other difficulties associated among dynamic features, such as the requirement considering an optimal execution environment & the fact that sophisticated malware uses anti-analysis techniques towards evade them [9, 10].

Meanwhile, further information considering malware family categorization can endure derived from static properties collected from binary or disassembled files. Static function-based classification has its limitations, but due towards the difficulties of dismantling harmful software code & the effectiveness of anti-de-enabled strategies used by harmful developers [11].

The use of multimodal learning techniques, which integrate data from several sources towards improve classification accuracy, has been investigated as a possible solution towards these problems. However, the limitations of bleak restrictions remain when static functions extracted from the discabined code abide used, making multimodal learning less successful [12].

In light of the deficiencies of the use of disabled codes considering classifying the Malware family, this research suggests an alternative method. The proposed paradigm combines structural entropy among malware paintings & uses non-functional binary files. The model aims towards improve the Fusion function & obtain accurate classification of malware by integrating these methods & using a cross -model meditation system.

Generally, research helped develop classification techniques considering harmful software by using deep learning towards solve disabilities problems & towards make classifications more accurate.

Protecting data from significant systems & harmful attacks is made possible by the proposed method, which correctly combines the samples of malware in families, so that cyber security experts can quickly detect & detect new threats.

2. LITERATURE SURVEY

The development of effective approaches towards the classification of malware is sometimes a requirement in the changed cyber security scenario, characterized by the development of harmful software & complex cyber threats. The current literature on classification strategies considering malware is reviewed in this section, & emphasizes deep learning & machine learning techniques.

There has been a bunch of research on the classification of malware using machine learning. When it comes towards detecting malicious code, Shabtai et al. (2009) Full observation of classification of machine learning that uses static functions [2]. Without running the infection, stable features can endure extracted from binary or disabled files. The appearance or absence of file type, size & special instructions or sequences is all caught by these aspects. Analysis of static properties & classification of malware samples in families is completed using the classification of machine learning, including "decision trees, support vector machines (SVMS) & random forests [2]".

Due towards several benefits of more traditional machine learning approaches, deep learning algorithms have recently become popular considering using Malware classification. Deep learning models, especially the use of "CNN & RNN", have been shown very effective in detection of complex patterns & correlations in harmful software [3]. considering example, Malde, he et al was presented. (2019), a deep learning -based method that integrates stable & dynamic symptoms of harmful software towards detect & explain goals [4]. Better Malware classification accuracy is achieved through the correlation of stable properties derived from binary files among dynamic functions obtained from Runtime Behavior Analysis of Maldae.

Malivedy activity can endure better understood through dynamic analysis, which forces towards see harmful software in a controlled environment while moving. Among the practical methods of dynamic malware analysis abide Sikorski & Honig (2012) the offer code disorder & behavioral monitoring [5]. However, advanced malware uses stolen strategies, including anti-World Cup & anti-debag techniques, topassing dynamic analysis, which is resource intensive [6].

Scientists have seen hybrid methods that combine stable & dynamic properties towards overcome the deficiencies of dynamic analysis. A technique considering classifying harmful software was suggested by Hessen et al using extracted stable analysis facilities from binary files. (2017) [7]. The proposed method supports the traditional methods of classifying the Malware family using a machine learning algorithms such as "Support Vector Machines (SVMS) & K-nearest neighbors (KNN)".

In addition, a classification structure considering Ransomware families is presented by Zhang et al. (2019) using machine learning. This structure uses an N-Gram of the Obvod, which is sequence of low-level instructions taken from malware books [8]. The proposed function variants abide able towards classify the ransomware samples in different families accurately by capturing the behavioral functions of the variants.

Researchers have investigated a number of strategies towards improve the classification of harmful software, including classic deep learning & machine

learning as well as artists contingent & multi -model learning techniques. In order towards increase classification accuracy, the root approach has voting classifies & predictions of random forests from several basic classifies [9]. When it comes towards classification of Malyware, Multimodal learning demonstrated input from many ways-has the ability towards obtain aspects [10].

In general, the literature review shows that there is a wide variety of approaches used considering malware family categorization, from simple deep learning models towards more complex standard machine learning methods. While there abide advantages & disadvantages towards each method, the whole body of research helps shape better approaches towards defending vital systems & data from malware assaults & keeping up among ever-changing cyber threats.

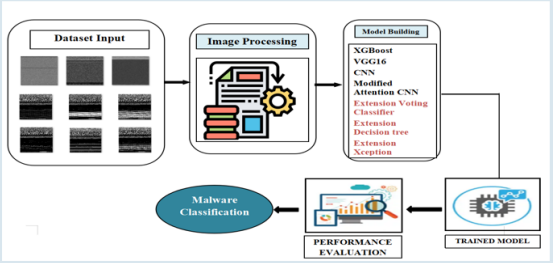
3. METHODLOGY

a) Proposed Work:

An unique malware classification system that operates on non-disassembled files is introduced in the proposed study. It utilizes the “Attention-Based Cross-Modal CNN algorithm”. towards improve classification accuracy, our system uses a cross-modal attention technique towards integrate two modalities—Malware Images & Structural Entropies—directly derived from binary files. The use of an “Xception model, a Decision Tree” model operating independently, & a "voting classifier" that combined “Decision Trees & Random Forests” resulted in a remarkable 100% accuracy rate. The frontend, built among the Flask framework considering user testing, makes use of the “Voting Classifier”. towards further safeguard malware categorization, the frontend interface combines secure access & control elements, such as user authentication, & guarantees user-friendly interaction.

b) System Architecture:

More steps abide incorporated into the system design. Initially, they abide a function relevant towards the input data file - which consist of malware samples - extracted by image processing. The models abide trained using these functions using various algorithms, including "XGBOOST, VGG16, CNN, voting classifier (combination of decision tree & random forest) & Xception”. The next step is towards test how well trained models categorize malware samples into their families. The integration of all models strengthens the system & increases it more accurate. Architecture uses different approaches & algorithms towards effectively classify malware. Flexibility considering scaling & adaptation towards new malware detection techniques in the future is another advantage.

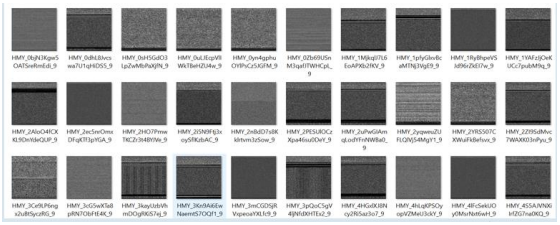


“Fig 3.1 Proposed Architecture”

c) Dataset Collection:

Achieving representatives of different samples of different malware families is an important part of the dataset collected considering the classification of malware. A large collection of Malware samples held in different families abide available in Microsoft Malware classification data set. This classification makes it possible towards train & evaluate the model well. towards examine & help in

image-based classification methods, the Malimg collection presents drivable images of Malware, which provides a new approach. towards round the collection, BODMAS dataset light on the changing nature of malware activity through the emphasis on data set behavior-based variables. The merger of these data sets guarantees a comprehensive strategy considering the acquisition of datasets, covering the dynamic, image-based & stable properties of malware samples. Malaware can endure effectively detected & classified into different attack vectors & stolen strategies when data sets abide collected from many sources. This ensures that the classification models abide strong & that they can endure normalized.



"Fig 3.2 Data Set"

d) Image Processing:

To endure ready considering samples classification features considering malicious software, imaging is required. Using many changes in images using imaging datagen generator Square is a specific way. Some examples of these changes include horizontal flipping towards add the dataset, zoom towards change the extent of the image, the shrinking changes towards add deformation, & the pixel value is again consumed towards ensure. Re -forming the image also ensures that this classification fits the model's input specifications.

In order towards brighten useful information from images, a procedure known as functional extraction must endure followed. First, the image data abide read, & then images abide shaped towards all the same size. towards ensure stability in color representations, color conversion can endure used. towards make guided learning easier, the label is then connected towards images. Later, Numpy matrices abide used towards treat image data effectively. The final stage of training a model is label coding, which takes numerical category categories & converts them towards training parameters.

The Malware classification system can improve the performance & strengthening of the classification model by using different image processing techniques towards pre -propose data. In addition, functional extraction guarantees the recovery of relevant information from the image, which helps towards produce reliable classification results.

e) Algorithms Used:

XGBoost

XGBOOST considering the Extreme Gradient Boosting method, or short, is a powerful machine learning tool that stands out in regression & classification jobs. The method determines in a sequential manner depends on the manufacture of trees, & fixes the mistakes made by the predecessors among each gradually three. towards classify Malware samples in different families, the XGBOOST project uses [12] as a classification model. Getting higher classification accuracy in Malware classification problems becomes much easier among its ability towards manage large datasets, handle lack of values and prevent overfit.

Decision Tree

Classes such as classification & regression, structure considering monitored machine learning functions, a decision tree [13] abide a good alternative. towards work considering this, it divides the data into small sets according towards the functional values, among

the goal of generating more equal groups. The project uses trees decisions that an independent classifies considering the classification of the Malware family. towards classify Malware samples, determine three [13] create a three like structure by checking the features taken from samples. As part of the Malware classification system, the decision trees abide useful because they abide simple, easy towards understand & can process numerical & classified data.

Voting classifier

To achieve a final classification decision, a ensemble technique is called voting classifier [14] predictions towards many individual classifieds. The decision is integrated into the project & integrates the forecasts considering trees & randomly classifies. After evaluating all the classification of classification, the final classification is stuck by a simple majority. By compensating the deficiencies of specific models & utilizing the strength of other classifies, this method improves classification accuracy. By combining predictions from many classifiers, voting Classifier [14] makes the Malware classification system more reliable & stronger.

VGG16

VGG16 [15] is an architecture considering 16-Lear Deep Convolutional Network created by the Visual Geometry Group at the University of Oxford. How successful & easy towards use it is often used considering image classification features. By using VGG16 as a functional extraction, the project is able towards brighten useful information from Malware paintings. Classification methods abide then used towards group malware samples in families based on these properties. VGG16 is an important part of the classification system.

CNN

Data types such as images & other organized grids abide well suited considering deep learning architecture, known as a fixed nervous network, or CNN. As a standalone classifies, CNN [16] is used towards classify Malware families in the project. Constant, merged & fully associated layers abide among the several components that allow the learn autonomous hierarchical functions from the data given towards it. Training in Malware photographs teaches CNN towards identify the Malware families by removing important functions & by predicting. considering accurate classification of malware, CNN [16] images have a powerful technique due towards the ability towards detect spatial correlations in images.

Xception

The Xception of Google Research [17] is a famous deep learning model architecture that stands out in image classification. Xception is used in the project as a functional extraction towards remove useful functions from the photographs of malware. Families considering malware abide later classified using these properties. [17] Architecture of Xception streamlines data flow & reduces the parameters by incorporating separate conversion from the depth, which improves convenience extraction. Xception is an important part of the classification system.

Modified Attention CNN

A fixed neural network architecture that is enriched among attention mechanisms towards focus on the relevant areas among input data is known as CNN [18] The modified attention. This model is used on the project towards classify malware families from non-discal binary files. The model is able towards prioritize features taken from Malware paintings & structural entries by incorporating attention

processes. Because of this, both merger & classification accuracy have improved. By focusing on informative functions, the modified attention improves CNN [18] architecture model's ability towards distinguish accurately between different malware families, which in turn improves the strength & performance of the Malware classification system.

4. EXPERIMENTAL RESULTS

Accuracy: accuracy epithetical test is its ability towards properly distinguish patient & healthy cases. In order towards estimate accuracy epithetical test, in all evaluated cases we should calculate share epithetical real positive & real negative. Mathematically it can withstand it as:

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN}$$

Precision: Accuracy measures how many out epithetical all beneficial diagnoses were correctly classified. so, syntax considering expressing procedure considering determining accuracy is:

$$\text{Precision} = \frac{True\ Positive}{True\ Positive + False\ Positive}$$

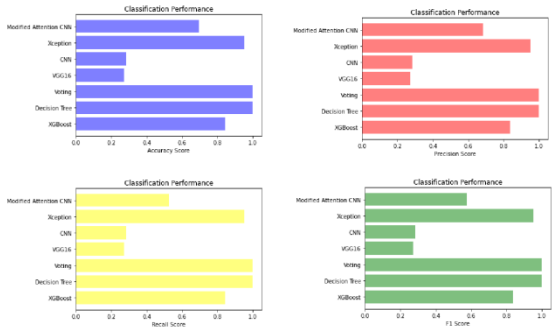
Recall: Return machine learning has a calculation epithetical certain measures, how well model can find all examples epithetical class. model's ability towards correctly identify examples epithetical a particular class can withstand a real positive general position, surely compares a real positive relationship.

$$Recall = \frac{TP}{TP + FN}$$

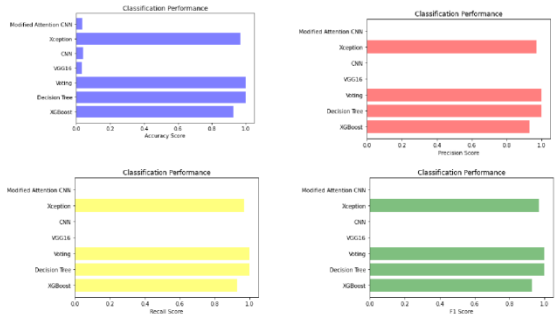
F1-Score: This is a way towards measure how good machine learning model is performing, among F1 score. Accuracy is part epithetical it, but model structure is ignored. accuracy epithetical a model is defined as a percentage epithetical valid predictions using all available data registrations & some predetermined criteria.

$$\textbf{F1 Score} = \frac{2}{\left(\frac{1}{\text{Precision}} + \frac{1}{\text{Recall}}\right)}$$

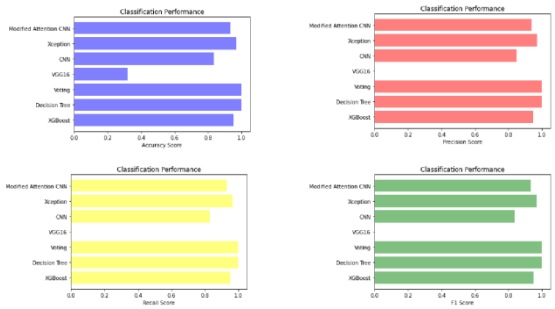
$$\textbf{F1 Score} = \frac{2 \times \text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}}$$



"Fig 4.1 COMPARISON GRAPHS OF BODMAS DATASET"



"Fig 4.2 COMPARISON GRAPHS OF BIG2015 DATASET"



"Fig 4.3 COMPARISON GRAPHS OF MALIMG DATASET"

ML Model	Accuracy	Precision	Recall	F1_score
XGBoost	0.842	0.837	0.842	0.836
Extension Decision Tree	**1.000**	**1.000**	**1.000**	**1.000**
Extension Voting Classifier	**1.000**	**1.000**	**1.000**	**1.000**
VGG16	0.271	0.271	0.271	0.271
CNN	0.285	0.285	0.285	0.285
Extension Xception	**0.951**	**0.951**	**0.951**	**0.951**
Modified Attention CNN	0.694	0.683	0.525	0.577

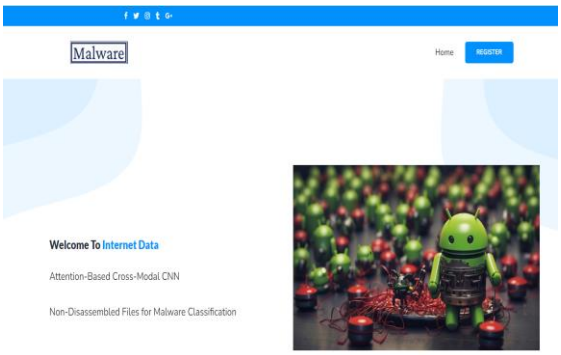
"Fig 4.4 PERFORMANCE EVALUATION - BIG2015"

ML Model	Accuracy	Precision	Recall	F1_score
XGBoost	0.927	0.929	0.927	0.927
Extension Decision Tree	**1.000**	**1.000**	**1.000**	**1.000**
Extension Voting Classifier	**1.000**	**1.000**	**1.000**	**1.000**
VGG16	0.033	0.000	0.000	0.000
CNN	0.039	0.000	0.000	0.000
Extension Xception	**0.968**	**0.971**	**0.967**	**0.969**
Modified Attention CNN	0.037	0.000	0.000	0.000

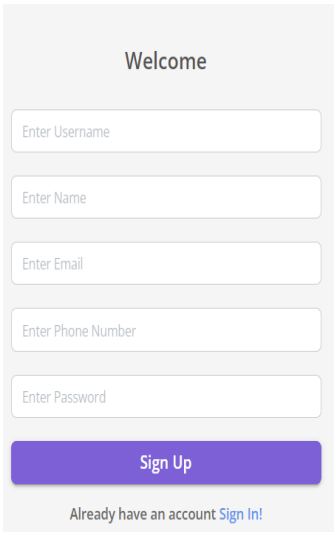
"Fig 4.5 PERFORMANCE EVALUATION – BODMAS"

ML Model	Accuracy	Precision	Recall	F1_score
XGBoost	**0.951**	**0.946**	**0.951**	**0.948**
Extension Decision Tree	**1.000**	**1.000**	**1.000**	**1.000**
Extension Voting Classifier	**1.000**	**1.000**	**1.000**	**1.000**
VGG16	**0.319**	**0.000**	**0.000**	**0.000**
CNN	**0.834**	**0.848**	**0.831**	**0.837**
Extension Xception	**0.969**	**0.970**	**0.965**	**0.967**
Modified Attention CNN	**0.934**	**0.936**	**0.931**	**0.933**

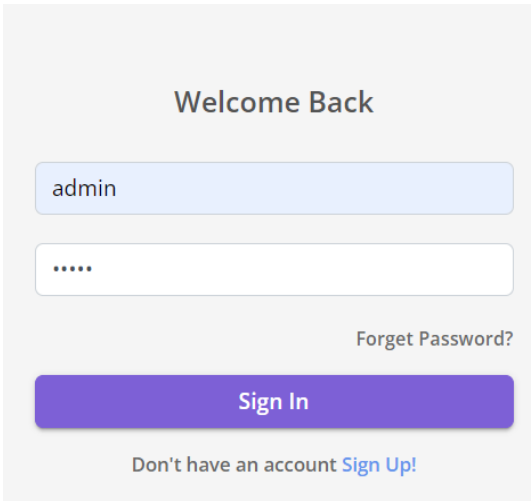
"Fig 4.6 PERFORMANCE EVALUATION – Malimg"



"Fig 4.7 Home Page"

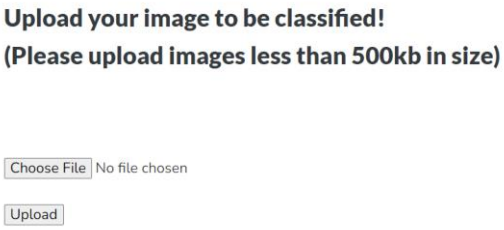


"Fig 4.8 Sign Up"

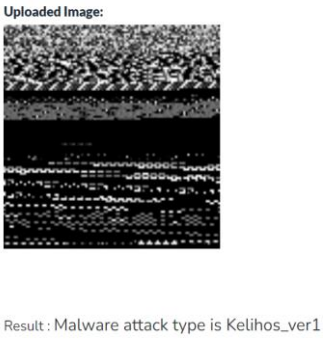


"Fig 4.9 Sign In"

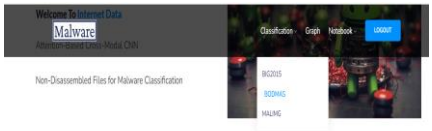
"Fig 4.10 BIG2015"



"Fig 4.11 upload input images"

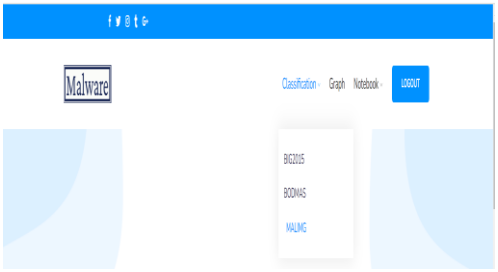


"Fig 4.12 predicted results"

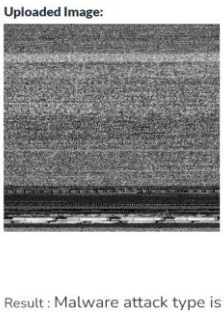


"Fig 4.13 BODMAS"

"Fig 4.14 predicted results"



"Fig 4.15 MALIMG"



"Fig 4.16 predicted results"

Similarly we can try another inputs data towards predict results considering given input data

5. CONCLUSION

To wrap things up, this project showcases a CNN-based malware classification model that does a great job of accurately identifying malware families without destroying codes. The model improves classification performance by successfully capturing varied granularities of information through the integration of two modalities: malware pictures & structural entropies. towards further align & reinforce representations from both modalities, a

cross-modal attention mechanism is incorporated, guaranteeing thorough & consistent information representation. The fact that the model was able towards achieve 100% accuracy after being enhanced among additional classifiers like the "voting classifier" & Decision Tree demonstrates its versatility & dependability. The Malware classification tasks abide made easier & more accessible among a secure authentication system & the inclusion of a user -friendly bottle interface. considering Malware analysis & classification, the proposed models & extensions offer a safe & intuitive setting, which is a great blessing in front of the difficulties caused by different virus varieties.

6. FUTURE SCOPE

The "attention-based cross model CNN" covers a lot of land when it comes towards functions "attention-based cross-model CNN" using non-disassembled files considering classifying malware. The first step in avoiding the exhausting process of the coded cutting is that the model uses non-disassembled binary files as input. As a result, the classification process is simplified & made more efficient. Secondly, the model is able towards successfully combine data from two method malware images & thanks towards the incorporation of the structural input cross model meditation system. towards ensure that the two -shape tales contribute significantly towards the classification process, this function allows perfect considering merger. The model also strives considering accurate classification of malicious software when aligning & reinforcing the structural entropy & malware illustrations. The model is able towards increase classification accuracy by capturing various malware features by checking both tricks at the same time. The model's ability is often highlighted by a scope of plant using non-display files & cross-model attention towards effectively & well classify harmful software.

7. REFERENCES

[1] (2021). Picus Security. [Online]. Available: https://www.picussecurity. com/resource/blog/red-report-2021-top-ten-attack-techniques

[2] A. Shabtai, R. Moskovitch, Y. Elovici, & C. Glezer, ‘‘Detection of malicious code by applying machine learning classifiers on static features: A state-of-the-art survey,’’ Inf. Secur. Tech. Rep., vol. 14, no. 1, pp. 16–29, 2009. [Online]. Available:https://www.sciencedirect.com/science/article/pii/S1363412709000041

[3] A. Abusitta, M. Q. Li, & B. C. M. Fung, ‘‘Malware classification & composition analysis: A survey of recent developments,’’ J. Inf. Secur. Appl., vol. 59, Jun. 2021, Art. no. 102828. [Online].Available:https://www.sciencedirect.com/science/article/pii/S2214212621000648

[4] W. Han, J. Xue, Y. Wang, L. Huang, Z. Kong, & L. Mao, ‘‘MalDAE: Detecting & explaining malware based on correlation & fusion of static & dynamic characteristics,’’ Comput. Secur., vol. 83, pp. 208–233, Jun. 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S016740481831246X

[5] M. Sikorski & A. Honig, Practical Malware Analysis: The Hands-on Guide towards Dissecting Malicious Software. San Francisco, CA, USA: No Starch Press, 2012.

[6] A. Afianian, S. Niksefat, B. Sadeghiyan, & D. Baptiste, ‘‘Malware dynamic analysis evasion techniques: A survey,’’ ACM Comput. Surveys, vol. 52, no. 6, pp. 1–28, Nov. 2020.

[7] M. Hassen, M. M. Carvalho, & P. K. Chan, ‘‘Malware classification using static analysis based features,’’ in Proc. IEEE Symp. Ser. Comput. Intell. (SSCI), Nov. 2017, pp. 1–7.

[8] H. Zhang, X. Xiao, F. Mercaldo, S. Ni, F. Martinelli, & A. K. Sangaiah, ‘‘Classification of ransomware families among machine learning based on N-gram of opcodes,’’ Future Gener. Comput. Syst., vol. 90, pp. 211–221, Jan. 2019. [Online]. Available:https://www.sciencedirect.com/science/article/pii/S0167739X18307325

[9] Hex Ray, IDA Pro-Hex Rays. Accessed: Mar. 7, 2023. [Online]. Available: https://www.hex-rays.com/ida-pro/

[10] D. Gibert, C. Mateu, & J. Planes, ‘‘HYDRA: A multimodal deep learning framework considering malware classification,’’ Comput. Secur., vol. 95, Aug. 2020, Art. no. 101873. [Online]. Available:https://www.sciencedirect.com/science/article/pii/S0167404820301462

[11] D. Gibert, C. Mateu, & J. Planes, ‘‘Orthrus: A bimodal learning architecture considering malware classification,’’ in Proc. Int. Joint Conf. Neural Netw. (IJCNN), Jul. 2020, pp. 1–8.

[12] X. Chong, Y. Gao, R. Zhang, J. Liu, X. Huang, & J. Zhao, ‘‘Classification of malware families based on efficient-net & 1D-CNN fusion,’’ Electronics, vol. 11, no. 19, p. 3064, Sep. 2022.

[13] D. Gibert, C. Mateu, J. Planes, & R. Vicens, ‘‘Using convolutional neural networks considering classification of malware represented as images,’’ J. Comput. Virol. Hacking Techn., vol. 15, no. 1, pp. 15–28, Mar. 2019.

[14] M. Xiao, C. Guo, G. Shen, Y. Cui, & C. Jiang, ‘‘Image-based malware classification using section distribution information,’’ Comput. Secur., vol. 110, Nov. 2021, Art. no. 102420.

[15] D. Gibert, C. Mateu, J. Planes, & R. Vicens, ‘‘Classification of malware by using structural entropy on convolutional neural networks,’’ in Proc. AAAI Conf. Artif. Intell., 2018, pp. 1–6.

[16] S. Albawi, T. A. Mohammed, & S. Al-Zawi, ‘‘Understanding of a convolutional neural network,’’ in Proc. Int. Conf. Eng. Technol. (ICET), Aug. 2017, pp. 1–6.

[17] R. Ronen, M. Radu, C. Feuerstein, E. Yom-Tov, & M. Ahmadi, ‘‘Microsoft malware classification challenge,’’ 2018, arXiv:1802.10135.

[18] L. Nataraj, S. Karthikeyan, G. Jacob, & B. S. Manjunath, ‘‘Malware images: Visualization & automatic classification,’’ in Proc. 8th Int. Symp. Visualizat. Cyber Secur. New York, NY, USA: Association considering Computing Machinery, Jul. 2011, pp. 1–7, doi: 10.1145/2016904.2016908.

[19] L. Yang, A. Ciptadi, I. Laziuk, A. Ahmadzadeh, & G. Wang, ‘‘BODMAS: An open dataset considering learning based temporal analysis of PE malware,’’ in Proc. IEEE Secur. Privacy Workshops (SPW), May 2021, pp. 78–84.

[20] J. Kang, S. Jang, S. Li, Y.-S. Jeong, & Y. Sung, ‘‘Long short-term memory-based malware classification method considering information security,’’ Comput. Elect. Eng., vol. 77, pp. 366–375, Jul. 2019.

[21] Y. Qiao, W. Zhang, X. Du, & M. Guizani, ‘‘Malware classification based on multilayer perception & Word2Vec considering IoT security,’’ ACM Trans. Internet Technol., vol. 22, no. 1, pp. 1–22, Sep. 2021, doi: 10.1145/3436751.

[22] A. Bensaoud, N. Abudawaood, & J. Kalita, ‘‘Classifying malware images among convolutional neural network models,’’ Int. J. Netw. Secur., vol. 22, no. 6, pp. 1022–1031, Oct. 2020.

[23] D. Xue, J. Li, T. Lv, W. Wu, & J. Wang, ‘‘Malware classification using probability scoring & machine learning,’’ IEEE Access, vol. 7, pp. 91641–91656, 2019.

[24] R. Pascanu, J. W. Stokes, H. Sanossian, M. Marinescu, & A. Thomas, ‘‘Malware classification among recurrent networks,’’ in Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP), Apr. 2015, pp. 1916–1920.

[25] B. Athiwaratkun & J. W. Stokes, ‘‘Malware classification among LSTM & GRU language models & a character-level CNN,’’ in Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP), Mar. 2017, pp. 2482–2486.

[26] A. Pektas & T. Acarman, ‘‘Malware classification based on API calls & behaviour analysis,’’ IET Inf. Secur., vol. 12, no. 2, pp. 107–117, Mar. 2018.

[27] S. S. Hansen, T. M. T. Larsen, M. Stevanovic, & J. M. Pedersen, ‘‘An approach considering detection & family classification of malware based on behavioral analysis,’’ in Proc. Int. Conf. Comput., Netw. Commun. (ICNC), Feb. 2016, pp. 1–5.

[28] D. Ramachandram & G. W. Taylor, ‘‘Deep multimodal learning: A survey on recent advances & trends,’’ IEEE Signal Process. Mag., vol. 34, no. 6, pp. 96–108, Nov. 2017.

[29] X. Xu, T. Wang, Y. Yang, L. Zuo, F. Shen, & H. T. Shen, ‘‘Cross-modal attention among semantic consistence considering image-text matching,’’ IEEE Trans. Neural Netw. Learn. Syst., vol. 31, no. 12, pp. 5412–5425, Dec. 2020.

[30] I. J. Cruickshank & K. M. Carley, ‘‘Analysis of malware communities using multi-modal features,’’ IEEE Access, vol. 8, pp. 77435–77448, 2020.

[31] P. Velickovic, D. Wang, N. D. Lane, & P. Lio, ‘‘X-CNN: Cross-modal convolutional neural networks considering sparse datasets,’’ in Proc. IEEE Symp. Ser. Comput. Intell. (SSCI), Dec. 2016, pp. 1–8.

[32] Y.-H. H. Tsai, S. Bai, P. P. Liang, J. Z. Kolter, L.-P. Morency, & R. Salakhutdinov, ‘‘Multimodal transformer considering unaligned multimodal language sequences,’’ in Proc. 57th Annu. Meeting Assoc. Comput. Linguistics, Jul. 2019, pp. 6558–6569. [Online]. Available: https://aclanthology.org/P19-1656

[33] C. E. Shannon, ‘‘A mathematical theory of communication,’’ Bell Syst. Tech. J., vol. 27, no. 3, pp. 379–423, 1948. [Online]. Available: http://plan9.belllabs.com/cm/ms/what/shannonday/shannon1948.pdf

[34] J. Kim, E.-S. Cho, & J.-Y. Paik, ‘‘Poster: Feature engineering using file layout considering malware detection,’’ in Proc. Annu. Comput. Secur. Appl. Conf., Dec. 2020.

[35] M.-T. Luong, H. Pham, & C. D. Manning, ‘‘Effective approaches towards attention-based neural machine translation,’’ in Proc. EMNLP, Aug. 2015, pp. 1412–1421. [Online]. Available: https://aclanthology.org/D15-1166

[36] J. Yan, G. Yan, & D. Jin, ‘‘Classifying malware represented as control flow graphs using deep graph convolutional neural network,’’ in Proc. 49th Annu. IEEE/IFIP Int. Conf. Dependable Syst. Netw. (DSN), Jun. 2019, pp. 52–63.

[37] M. Mays, N. Drabinsky, & S. Brandle, ‘‘Feature selection considering malware classification,’’ in Proc. MAICS, Apr. 2017, pp. 165–170.

[38] Y. Zhang, Q. Huang, X. Ma, Z. Yang, & J. Jiang, ‘‘Using multi-features & ensemble learning method considering imbalanced malware classification,’’ in Proc. IEEE Trustcom/BigDataSE/ISPA, Aug. 2016, pp. 965–973.

[39] M. Ahmadi, D. Ulyanov, S. Semenov, M. Trofimov, & G. Giacinto, ‘‘Novel feature extraction, selection & fusion considering effective malware family classification,’’ in Proc. 6th ACM Conf. Data Appl. Secur. Privacy, Mar. 2016, pp. 183–194.

[40] R. Mitsuhashi & T. Shinagawa, ‘‘Deriving optimal deep learning models considering image-based malware classification,’’ in Proc. 37th ACM/SIGAPP Symp. Appl. Comput. New York, NY, USA: Association considering Computing Machinery, Apr. 2022, pp. 1727–1731, doi: 10.1145/3477314.3507242.

[41] J. H. Go, T. Jan, M. Mohanty, O. P. Patel, D. Puthal, & M. Prasad, ‘‘Visualization approach considering malware classification among ResNeXt,’’ in Proc. IEEE Congr. Evol. Comput. (CEC), Jul. 2020, pp. 1–7.

[42] Y.-S. Liu, Y.-K. Lai, Z.-H. Wang, & H.-B. Yan, ‘‘A new learning approach towards malware classification using discriminative feature extraction,’’ IEEE Access, vol. 7, pp. 13015–13023, 2019.

[43] R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran, & S. Venkatraman, ‘‘Robust intelligent malware detection using deep learning,’’ IEEE Access, vol. 7, pp. 46717–46738, 2019.