Cyber Threat Detection Using Machine Learning

Trilok Nath Pandey  
*Department* *of computer science  
Vellore Institute Of Technology*Chennai, India  
triloknath.pandey@vit.ac.in

Chappa Vamsi  
*Department* *of computer science  
Vellore Institute Of Technology*Chennai, India  
chappa.vamsi2021@vitstudent.ac.inAkash S   
*Department* *of computer science  
Vellore Institute Of Technology*Chennai, India  
akash.s2021@vitstudent.ac.in

Mula Yaswanth  
*Department* *of computer science  
Vellore Institute Of Technology*Chennai, India  
mula.yaswanth2021@vitstudent.ac.in

*Abstract*— In the modern digital era cyberattacks are the major concern. The major mode of these cyberattacks are in the form of the online threats that are embedded in the URL’s. The information is gained illegally as the main reason for these attacks. This abstract presents an interactive platform for the people where they can check their URL’s whether they are safe to use or not. The purpose of proposed system is to help the people in order to find the threats that are hidden inside the URL’s. The platform requires the URL from the user as input and displays it’s nature whether it is good or bad. The project uses Machine-Learning(ML) algorithms in order to study the input URL and compares it with the previous patterns of threats that are used while training the algorithm and produces the output. This abstract outlines a precise approach to threat detection and ensuring cyber safety through an interactive digital model. This facilitates the decrement in the cyber attacks and develops a healthy cyber space. The primary motivation behind these attacks is the unlawful capture of data. The abstract suggests an interactive platform where users can evaluate the security of URLs in order to address this problem. The goal of the platform is to give consumers the ability to recognize hidden risks within URLs and ascertain whether or not they are harmful or safe. The software compares input URLs against known threat patterns obtained from training data using Machine Learning (ML) methods. This methodical approach to threat identification uses an interactive digital model to guarantee cyber safety. By giving consumers the ability to decide for themselves what to do online activities, the platform contributes to the reduction of cyber attacks and the cultivation of a healthier cyber space.

Keywords—1.Cyber-Safety,Machine-Learning,Cyber Threats, Model Training, Testing, Data collection and Preprocessing, Web Application, URL. Threat Detection

# Introduction

In this modern era of rising usage of technology and high interaction with cyber space, The cyber attacks are the main concern. Imagine if these attacks can be prevented or avoided using a model that not only detects the threat and guides you to handle those attacks.This project is the exact manifestation of this solution. The safety nature of the URL can be predicted With the help of the user’s input i.e., URL, by using ML algorithm and training the models based on datasets that consists various URL’s and it’s safety nature whether it is safe or not based on many patterns, Including user friendly interface along with login page and a input obtaining page that helps to get the input from the user and that applies trained algorithms and processes it. There is large usage of datasets which are tend to be studied carefully and made learnt by the platform to produce accurate output and threat detection. This project would be a user friendly approach which could change helplessness of many users who fret over lack of guidance and make them easily prevent the cyber threats embedded within URL’s by detecting them. The main Aim of the project is to reduce the cyber attacks among overall cyber space by helping the people to prevent the cyber attacks by exposing the threats that are embedded in the URL’s which they use in day to day life.

This entitles to all the users who wants to check the safety of the URL’s that they have doubt about its safety. The project requires the URL from the user as the input to be fed by which the respective algorithm gives the resulted output. Utilizing machine learning, cyber threat detection entails analyzing massive volumes of data, including system logs, network traffic, and user behaviour, to find patterns suggestive of malicious activity. ML models are able to discriminate between normal and aberrant behaviour by using methods like anomaly detection, classification, and grouping. This allows them to identify possible dangers and flag them for additional research. They can take many different forms, from malware infections to data breaches. Advanced ways to efficiently detect and neutralize cyber threats are desperately needed, as the sophistication and frequency of these attacks continue to grow.

The overall goal of this study is to shed light on how machine learning functions in cybersecurity and how it can influence threat detection and mitigation techniques in the future.

# Literature Review

The literature survey in the paper explores the influence of architecture and parameters on artificial neural network (ANN) quality and performance . It references works by foreign and domestic scientists focusing on ANN design and parametrization methods . Additionally, the study highlights the use of Keras Tuner from Google Research for optimizing ANN hyperparameters . The authors also discuss the analysis of deep learning models for medical image classification [1]. Furthermore, the paper delves into the application of deep sentence embedding using long short-term memory networks for information retrieval [1].The paper discusses the use of advanced encryption techniques in securing communication systems, focusing on the implementation of cryptographic algorithms in the context of network security. It explores the challenges and solutions related to data encryption, key management, and secure communication protocols. The study also delves into the application of encryption technologies in different network environments to enhance data confidentiality and integrity. Overall, the research provides insights into the importance of encryption in safeguarding sensitive information in modern communication systems[2].

The literature survey in this paper provides an in-depth analysis of various detection techniques and solutions researched to detect Advanced Persistent Threats (APT). It covers the challenges in detecting APT, the APT attack life cycle, and the different intrusion detection systems, including signature-based and anomaly-based detection. The survey also explores the state of the art in APT detection, highlighting various detection techniques proposed by researchers and their drawbacks. Additionally, it discusses the main challenges faced in APT detection, providing a comprehensive overview of the current research landscape in this domain [3].

The literature survey of the paper "A Model for Cyber Threat Intelligence for Organizations" provides a comprehensive overview of the current state of cyber threats in South Africa and the need for effective Cyber Threat Intelligence. It discusses existing frameworks, models, sharing standards, and exchange platforms for Cyber Threat Intelligence. The survey also highlights the challenges and sources of Cyber Threat Intelligence, emphasizing the importance of proactive measures and collaboration among stakeholders. Additionally, it explores the characteristics and use cases of Cyber Threat Intelligence, laying the groundwork for the proposed model[4].The study on the Bi-LSTM Neural Network Approach to Detect and Recognize Cyberthreats, Cyberstalking, and Extremist Tweets in Twitter presents a comprehensive analysis of utilizing advanced machine learning techniques to address online threats. The research highlights the growing concern of cyber threats, including phishing attacks, extremist tweets, and cyberstalking, and emphasizes the importance of developing models to automatically identify and mitigate such risks. By leveraging the Bi-LSTM method and training the model on a Twitter dataset obtained from Kaggle, the algorithm achieves remarkable performance scores, with a total accuracy of 93% and an F1 score of 95%. The study underscores the significance of text mining and sentiment analysis in detecting aggressive and harmful content in short texts like tweets. Overall, this research contributes significantly to the field of cybersecurity by demonstrating the effectiveness of machine learning approaches in combating cyber threats on social media platforms like Twitter [5].

The literature survey of this paper reveals a comprehensive investigation into the co-design of fault detection filters (FDF) and fault-tolerant controllers (FTC) for unmanned surface vehicles (USV) under cyber-physical threats. The study addresses the need for timely detection of sensor faults and the stability of USVs in the presence of physical threats and cyber threats. It also highlights the existing research on fault detection, fault-tolerant control, and cyber-physical threats in the context of USVs, emphasizing the novelty and significance of the proposed co-design approach[6]. The paper "Estimating Application Cyberthreat Impact Score for Honeypot Coverage Prioritization" by Kren, Kos, and Sedlar presents a novel metric for evaluating the attractiveness of honeypots to attackers while considering the real-world popularity of the mimicked systems. The authors address the challenge of selecting high-impact honeypot services by proposing a formula that incorporates factors such as vulnerability density, breach cost, countermeasure effectiveness, compliance index, and the size of the real-world install base of the application. This approach aims to provide a comprehensive assessment of cyberthreat impact, enhancing the detection of attacks and protection of systems.

The research builds on the importance of honeypots in cybersecurity and the need to optimize their effectiveness in capturing valuable data about attackers. By introducing a practical calculation method based on the proposed formula, the paper offers a structured approach to prioritize honeypot coverage and enhance cyber risk assessment. The study emphasizes the significance of considering both the attractiveness of honeypots to attackers and the real-world usage of the mimicked systems, highlighting the complexity of selecting appropriate applications for honeypot deployment. Furthermore, the paper contributes to the field by addressing the challenges associated with application selection for honeypots, such as the number of vulnerabilities, software development speed, and update mechanisms. The proposed metric provides a valuable tool for organizations to assess cyberthreat impact, make informed security management decisions, and prevent potential attacks. Overall, the research offers a comprehensive framework for evaluating honeypot attractiveness and real-world popularity, advancing the field of cybersecurity risk assessment [7].

The literature survey of the paper "Improving Cyber security Situational Awareness and Cyber-Attack Detection Based on Analytic Data Mining Techniques" provides an in-depth exploration of data mining methods to enhance cyber security situational awareness. It delves into the significance of cyber-attack detection and the utilization of data mining techniques to improve defense mechanisms. The survey also covers the application of machine learning algorithms for fraud detection and the critical role of data quality in the effectiveness of data mining techniques for cyber security. Additionally, it discusses the use of data mining for network intrusion detection and the importance of situational awareness in cyber defense[8]. The literature survey in this paper provides an overview of existing research on data mining techniques and cyber threat intelligence (CTI). It discusses various studies that have utilized data mining algorithms for intrusion detection systems and compares the performance of different algorithms. Additionally, the survey highlights the importance of CTI standards and platforms for sharing and utilizing threat intelligence. The paper also examines the challenges and limitations in creating CTI, emphasizing the need for automated systems to facilitate the generation of CTI [9].

The literature review in this paper provides an in-depth analysis of existing threat modeling approaches in the context of Internet of Vehicles (IoV) systems. It covers various studies on threat modeling for connected vehicle networks, vehicular fog computing, and privacy issues in V2P systems for 5G networks. The review also delves into the development of threat models for connected vehicle sensors and the classification of threats targeting location information acquisition in Vehicular Ad hoc Networks (VANETs). Overall, the literature review serves as a comprehensive foundation for the subsequent threat analysis in the paper.[10] The literature survey presented in this paper highlights the gap in existing works, which predominantly focus on connected and automated internal combustion engine vehicles rather than connected and automated electric vehicles. It emphasizes the need for comprehensive evaluation metrics, particularly in areas such as energy management systems, to address the challenges posed by limited battery capacity and range anxiety. The study also underscores the importance of cybersecurity for electronic control units in connected and automated electric vehicles, advocating for novel methodologies for vulnerability assessment [11].

The literature survey of the paper on Information Threat Recognition Method Using a Neural Network includes references to previous works on network intrusion detection, such as studies by Shichkina and Fatkieva Cho et al. on RNN Encoder-Decoder models and Hochreiter and Schmidhuber on Long Short-Term Memory networks. Additionally, the overview of multi-class classification metrics by Grandini et al.and the dataset provided by the Canadian University of New Brunswick are crucial references in the development of the proposed method. These works

collectively contribute to the advancement of network security through deep learning techniques and data-driven approaches [12].

The literature survey in this paper discusses the limitations of existing public IDS datasets and the need for realistic datasets to develop advanced IDS classifier models. It also highlights the potential of using PRBS (Pseudo Random Binary Sequence) in cyber security mitigation and the challenges of using AI with deep learning algorithms to detect unknown cyber threats. Additionally, it references related studies on using PRBS in training artificial neural networks and creating prediction models for cyber attacks. Overall, the literature survey provides a comprehensive overview of the current state of research in the field of cyber security and the potential applications of PRBS and correlation techniques[13].

The literature survey in the paper "Last Line of Defense: Reliability Through Inducing Cyber Threat Hunting With Deception in SCADA Networks" by Abdul Basit Ajmal et al. explores existing vulnerabilities and known threats in SCADA systems . It also discusses the limitations of traditional security approaches, such as dll injections for Windows, in securing SCADA networks [T6]. The integration of kill chain analysis and cyber deception for SCADA security is highlighted as a novel approach to identifying and mitigating attack behaviors at each phase of an intrusion . Additionally, the paper references related works on SCADA vulnerability assessment and security recommendations, emphasizing the need to address unknown threats exploiting zero-days [14].

The literature survey in this paper provides an overview of the existing research on Advanced Persistent Threats (APT) and security challenges in Industrial Internet of Things (I-IoT) enabled Cyber-Physical Systems (CPS). It discusses the limitations of traditional security models and the potential of Machine Learning (ML) and Deep Learning (DL) techniques in addressing APT attacks. The survey also highlights the use of Graph Attention Network (GAN) for APT detection and classification, comparing it with conventional ML techniques. Additionally, it presents a summary of related work, including studies on network architecture, security vulnerability concerns, and the application of ML algorithms for cyber-attack detection [15].

The literature survey in the provided document discusses various existing studies in the field of cyber threat intelligence and machine learning techniques for threat detection. It highlights the use of different models such as Beta Mixture Hidden Markov, Bayesian networks, NLP, SVM, and DL in enhancing threat identification and intelligence mechanisms. The survey also emphasizes the importance of performance evaluation metrics in assessing the effectiveness of these models in detecting various types of cyber attacks in IoT environments[16].

The literature survey in the provided paper explores the evolving landscape of cyber security threats and the increasing importance of integrating machine learning (ML) and logical reasoning (LR) to enhance security measures. It discusses the potential benefits of this synergy, such as improved accuracy, speed, and scalability of cyber security solutions. The survey also highlights research directions like hybrid systems, adversarial machine learning, and human-in-the-loop approaches as promising avenues for future investigation . Additionally, it references previous works on emerging threats in cyber security , fog computing security challenges , machine learning techniques for cyber security , and the application of deep learning to cybersecurity [17].

The literature survey in the paper explores the evolution of intrusion detection systems (IDS) in Cyber-Physical System (CPS) environments, highlighting the shift from traditional machine learning techniques to deep learning and other statistical methods for improved performance . Various studies have proposed innovative approaches such as CPS-GUARD, DeepFed, and Quantum Dwarf Mongoose Optimizer with Ensemble DL-based Intrusion Detection (QDMO-EDLID) to enhance threat detection capabilities in CPS networks . These advancements aim to address the challenges of managing massive amounts of data and ensuring real-time performance in detecting cyber threats [18].

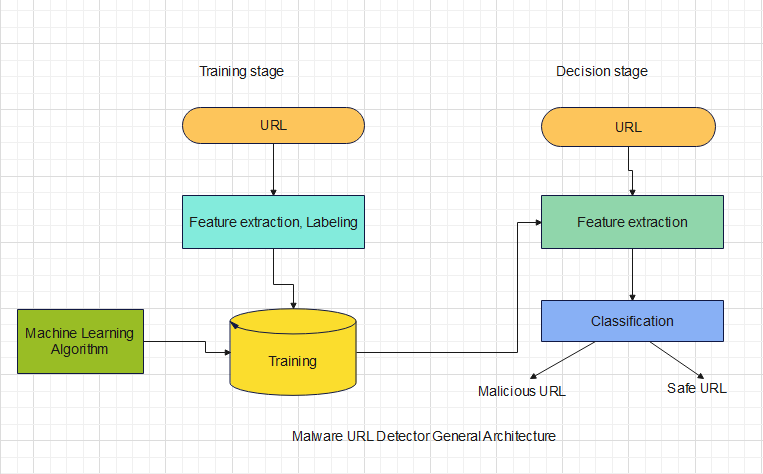
The literature survey of the paper includes studies by Shuhan Yuan and Xintao Wu on deep learning applications in insider threat detection , Fangfang Yuan et al.'s user-based DNN approach for insider threat detection , and Jonghoon Lee et al.'s AI strategy for cyber-threat detection using artificial neural networks . Additionally, Teng Hu et al. proposed a user authentication system based on mouse bio-behavioral characteristics and deep learning to address insider threats . The work of Hyrum S. Anderson and Phil Roth on enhancing machine learning research in malware detection through the EMBER model and Yoshihiro Oyama et al.'s study on malware detection feature selection using supervised machine learning are also referenced[19].

The paper provides a comprehensive overview of the application of Visual Analytics in detecting Advanced Persistent Threats (APTs) within the MASFAD framework. It discusses the challenges in network analysis due to the overwhelming amount of data generated daily and emphasizes the importance of visualizations for anomaly detection and enhancing cyber situation awareness. By leveraging Gestalt principles and interactive visualizations, the framework aims to improve the perception, comprehension, and projection phases of Situation Awareness for effective APT detection. The future work section outlines plans to further develop the visualization aspect of the framework and create new datasets for evaluating cyber situation awareness during APT attacks [20].

# Proposed Methodology

## A. Malware URL Detector General Architecture

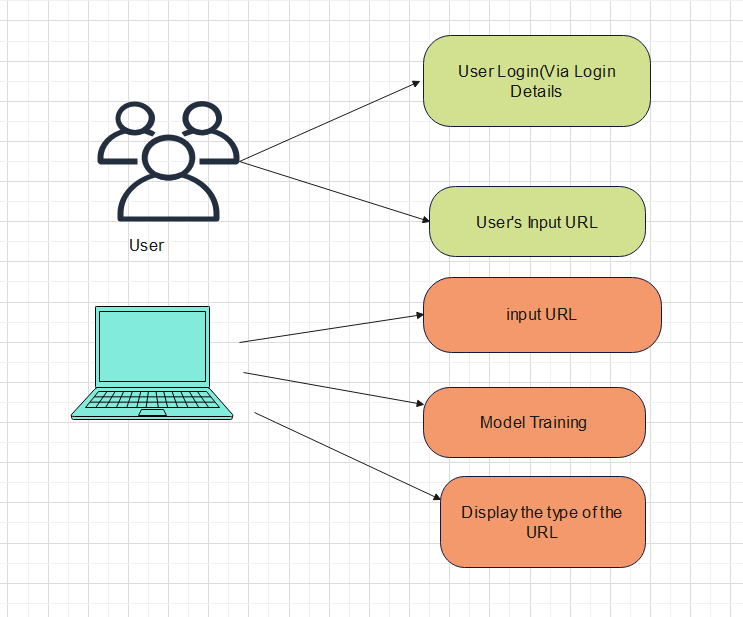
The project of building a threat detection platform is a user centered model making. Here the output is solely depended on the input which would be given by the user. There are various URL’s in which a user would be able depend on. Here the URL’s are mainly categorized into two 1.Good and 2.Bad. The user is intended to input their URL in order to get the most feasible output. According to the user’s input the feasible output is generated and displayed by the platform. These datasets are then stored and sent for processing via digital platform. Then according to the user input this whole dataset would be processed in the system using suitable machine learning algorithms. The machine learning algorithm which consists of different useful techniques to read the datasets and take preprocessed results to train the project model. The ML algorithm plays a key role in classifying the datasets and provide us with accurate results. With the trained model using ML algorithms when deployed provides us with feasible results fetched from the machine and can be post-processed to improve the output. The output can be changed with every variant data set and every user.



*Figure-1: Malware URL Detector General Architecture*

*B. Use Case Diagram*

The Use Case Diagram serves as a graphical representation showcasing the functional aspects of a system. It delineates the interactions between system users (actors) and the functionalities provided by the system. Actors, which can be users, external systems, or other elements interacting with the system, are depicted alongside use cases, representing specific functionalities like ”Classify URL” or ”View Classification Results.” This diagram simplifies understanding by outlining the system’s capabilities at a high level without delving into internal complexities.

**

*Figure-2: Use Case Diagram*

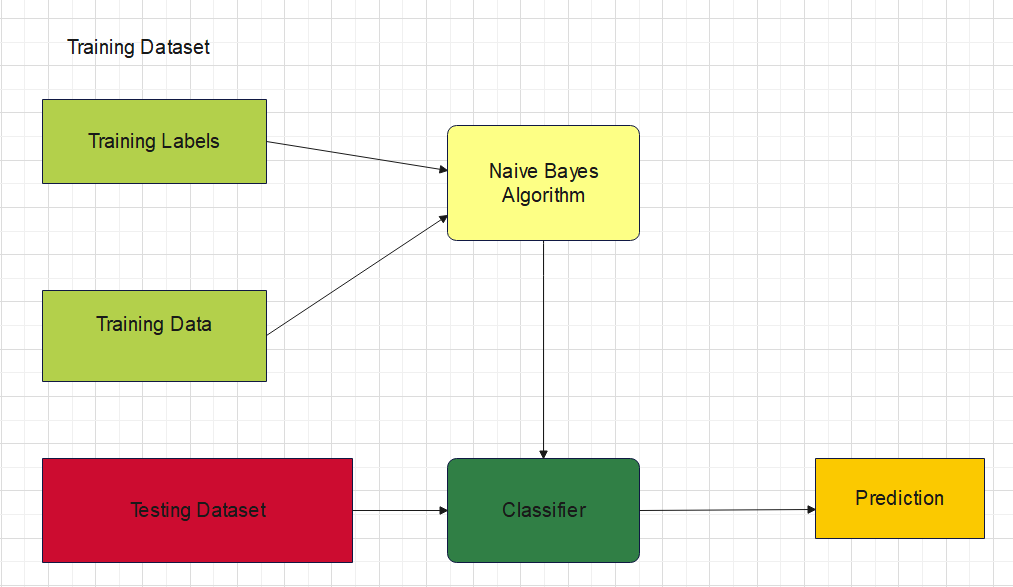
*C. Machine Learning Algorithms*

Using machine learning (ML) techniques and algorithms, cyber threat detection entails analyzing large volumes of data to find patterns that point to harmful activity occurring in digital settings. ML models, in contrast to conventional rule-based systems, are able to change and grow in order to identify new risks, providing a proactive approach to cybersecurity.

ML-based cyber threat detection uses a number of methods, such as clustering, classification, and anomaly detection. Finding departures from typical behavior, such as odd network traffic or system activity, is the main goal of anomaly detection. By classifying data into predetermined threat categories, classification algorithms make it

possible to identify known threats based on past trends. By putting similar data points together, clustering algorithms make it easier to find new attack patterns or threat clusters. Large datasets with labeled instances of both benign and malevolent conduct are used to train machine learning algorithms. These datasets aid in the models' ability to discern between benign and malicious activity, allowing them to quickly identify and neutralize cyberthreats. With time, machine learning models can improve their detection abilities by adapting to changing threats as they continue to learn from fresh data.

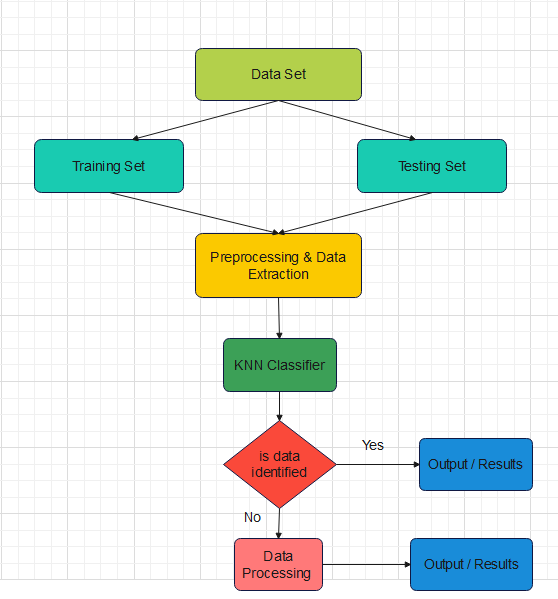
**Multinomial Naïve Baye’s:** The Multinomial Naive Bayes classifier provides a probabilistic framework for modelling the relationships between features and class labels in text data, making it an efficient yet straightforward approach for text classification applications. The Multinomial Naive Bayes classifier is computationally efficient and scales well to large datasets, making it suitable for real-world applications with high-dimensional feature spaces. This classifier is based on applying Bayes' theorem with strong independence assumptions between the features. It is particularly suited for text classification tasks, where the features are often categorical.

****

*Figure3: Multinomial Naïve bayes Architecture*

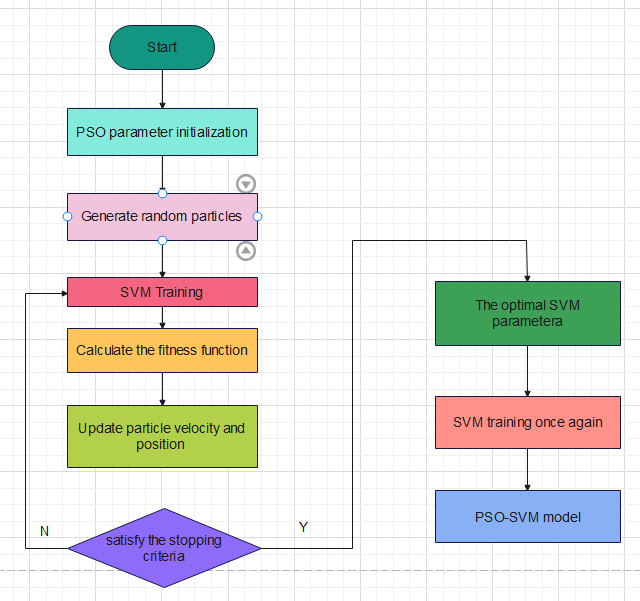
**K-Nearest Neighbors (KNN) classifier:** KNN determines the class label of a new data point for classification tasks by having the K nearest neighbors cast a majority vote. The new data point is allocated the class label that appears the most times among the K neighbors. When doing regression tasks, KNN determines the prediction value by averaging, or weighting, the target values of the K nearest neighbors.

The idea of a distance metric, usually Euclidean distance, which gauges the degree of similarity between data points in a feature space, lies at the heart of the KNN algorithm. The algorithm makes the assumption that data points are more similar when they are closer to one another. In order to categorize a new data point, KNN determines its K closest neighbors using the selected distance metric. KNN is a simple, instance-based learning algorithm that stores all available cases and classifies new cases based on a similarity measure. It is useful for classification and regression problems.



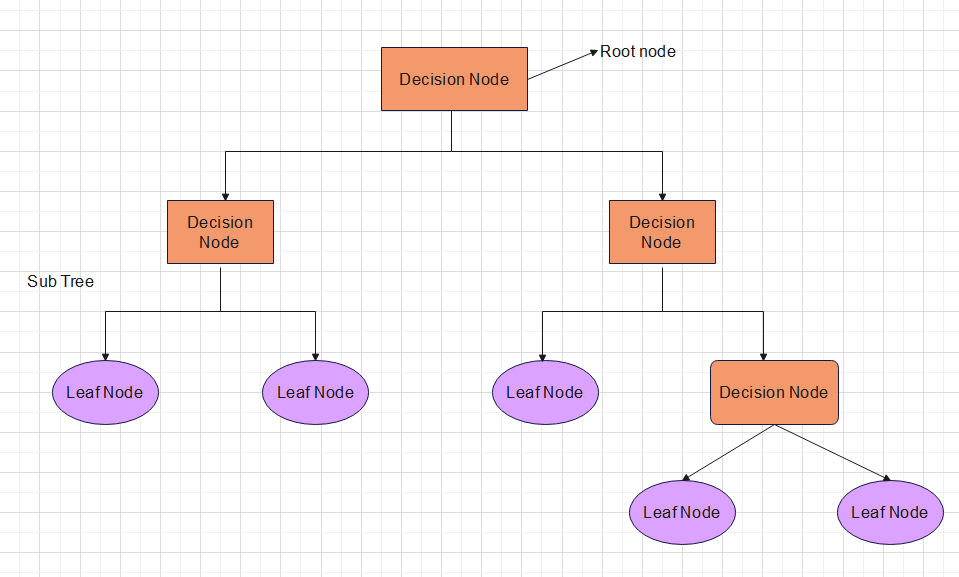
*Figure-4 K-Nearest Neighbors (KNN) classifier Architecture*

**Support vector machines (SVM):** support vector machines are adaptable and strong algorithms that can handle a wide range of jobs and data kinds. Their popularity stems from their ability to identify the best hyperplanes and efficiently divide classes in a variety of machine learning applications. SVMs are useful tools in the field of machine learning even though they may be computationally demanding and require careful parameter tweaking. This is because they can handle high-dimensional data and generate accurate predictions. SVMs look for the ideal hyperplane to divide data points into distinct groups or to forecast continuous results. By maximizing the margin—the distance between the hyperplane and the closest data points from each class, commonly referred to as support vectors—the hyperplane is identified. SVMs are powerful for handling high-dimensional data and are effective in cases where the number of dimensions is greater than the number of samples. They are particularly useful for binary classification problems.

****

*Figure-5 Support vector machines Architecture*

**Decision tree:** Decision trees' interpretability is one of their main benefits. Because the algorithm's learnt decision rules are immediately comprehensible and observable, they are especially helpful for tasks where explainability is crucial. Because of this transparency, users can learn more about the underlying patterns in the data and how the model works. Decision trees are still a popular option for many machine learning tasks because of their interpretability, simplicity, and capacity to handle a variety of tasks and data types, even with their limitations. They are a fundamental algorithm in the field of machine learning and have cleared the path for increasingly sophisticated methods in predictive modeling and decision-making. Decision trees are a non-parametric supervised learning method used for classification and regression. The goal is to create a model that predicts the value of a target variable by learning simple decision rules inferred from the data features

****

*Figure-6: Decision tree Architecture*

*D. Ensemble method of Multinomial naïve bayes and Decision tree*

**Ensemble Algorithms (Voting Classifier):**

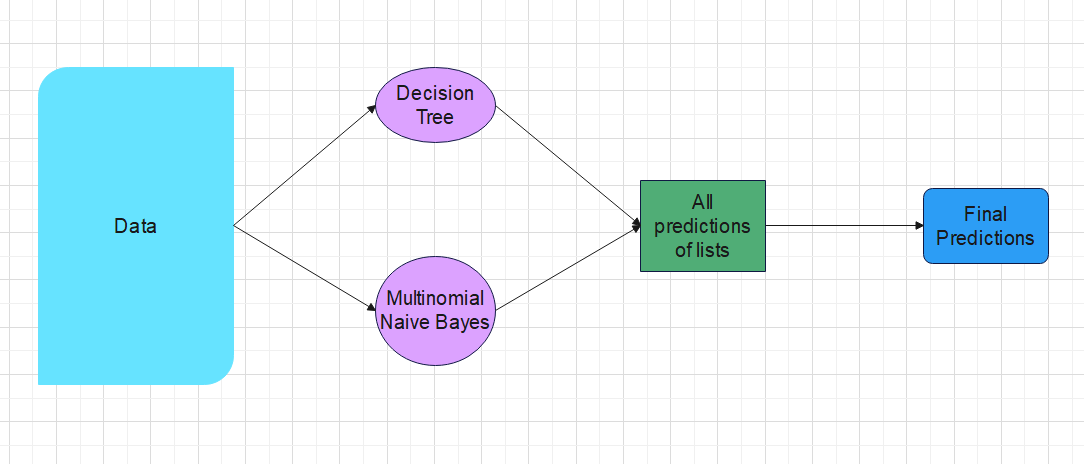
Ensemble algorithms, like the Voting Classifier, use the combined knowledge of several base models to provide effectiveness of threat detection. It reduces the biases and variance of each individual model and produces more dependable classifications by aggregating predictions from various classifiers. By ensuring that each model's strengths are taken into account when making the final selection, this democratic approach improves overall accuracy and resilience in the detection of harmful software.

**Ensemble Algorithms (Stacking Classifier):**

For Cyber threat detection, the Stacking Classifier is an advanced ensemble technique that combines a variety of base learners in a hierarchical fashion. A meta-classifier can be trained on the predictions of several base models, which helps it identify higher-order correlations between the models' outputs and improves decision-making. By utilizing complementing strengths from many models, this meta-learning paradigm improves detection effectiveness and increases adaptability to changing cyber threats.

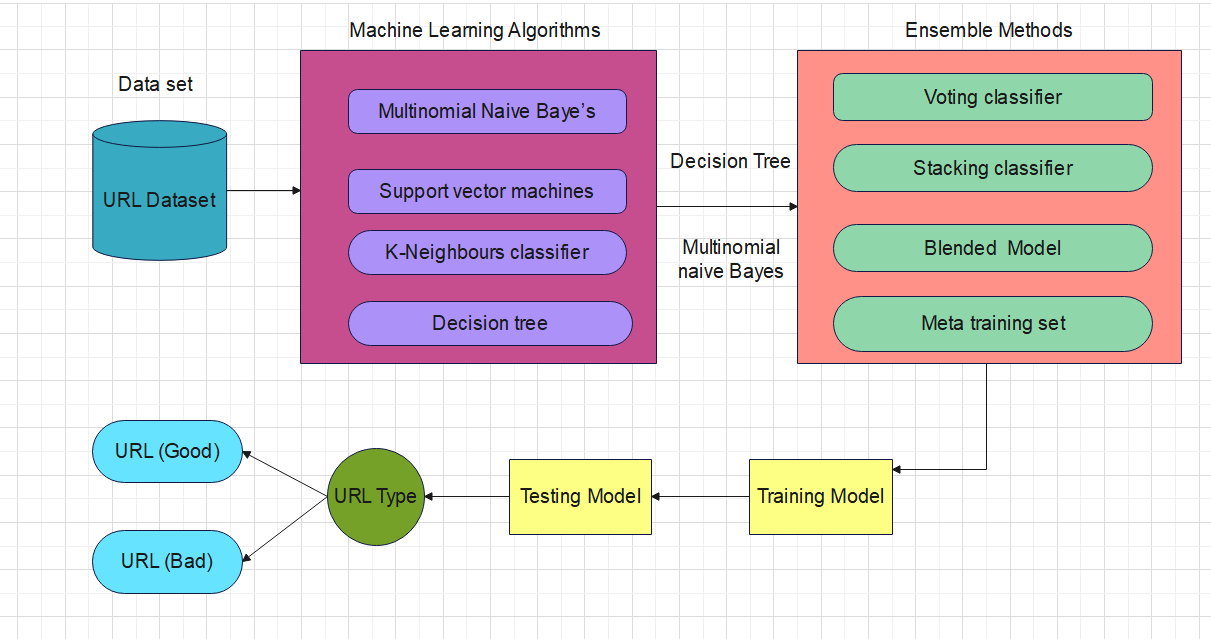
**Blended Model:** The Blended Model is a calculated fusion of many machine learning approaches designed for memory-based cyber threat identification. It combines predictions from several base models with different features and strengths to maximize the intelligence of each part and provide a detection framework that is more reliable and accurate. It takes advantage of the complimentary nature of several algorithms through careful weighting and combination procedures, which improves detection efficacy while reducing the biases of individual models.

**Meta training set**: In meta-learning, ensemble algorithms make use of the combined knowledge of several base learners to increase the precision and resilience of predictions. Ensemble approaches are essential in the setting of meta-training sets, where the objective is to train a model that can swiftly adapt to new tasks. Ensemble techniques reduce the possibility of overfitting to particular cases or characteristics by aggregating the predictions of many base models trained on different subsets or representations of the meta-training data. To combine predictions from separate learners, strategies like bagging, boosting, and stacking are frequently used. Each has its own advantages in terms of generalization and the bias-variance trade-off. By utilizing ensemble methods, meta-trained models are able to leverage the knowledge of several learners, improving their capacity to generalize to new tasks and datasets while maintaining flexibility and adaptability.

****

*Figure-7: Ensembled Algorithms Architecture*

*E. Architecture of the project*

****

*Figure-8 : Complete Architecture of the project*

# Results and discussion

## A. Individual Models

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| s.no | Model | Accuracy | precision | Recall | F1-score |
| 1. | Multinomial Naïve Baye’s | 0.9907 | 1.00 | 1.00 | 0.99 |
| 2. | Support vector machines | 0.9927 | 1.00 | 1.00 | 1.00 |
| 3. | K-Neighbours classifier | 0.9948 | 1.00 | 0.99 | 1.00 |
| 4. | Decision tree | 0.9943 | 1.00 | 1.00 | 1.00 |

*B. Ensemble Methods*

|  |  |  |
| --- | --- | --- |
| S.no | Ensemble method | Accuracy |
| **1.** | Voting classifier | 0.9961 |
| **2.** | Stacking classifier | 0.9879 |
| **3.** | Blend Model | 0.9963 |
| **4.** | Meta training set | 0.9975 |

# Conclusion

The primary goal of the project is to create a platform that In conclusion, our project represents a significant advancement in the field of threat detection using memory analysis, demonstrating the efficacy of a hybrid algorithm combining multinomial naïve bayes and decision tree classifiers. Through precise experimentation and validation, we have found that our blended ensemble model achieves the highest accuracy of 99.75%, outperforming individual classifiers like multinomial naive bayes, decision trees, support vector machines and extreme K-neighbours classifier and alternative ensemble methods. The Voting Classifier and meta training set yielded commendable accuracies of 99.61% and 99.75%, respectively, further highlighting the effectiveness of ensemble techniques in enhancing prediction capabilities. In our research, stacking classifier exhibited a lower accuracy of 98.79%, by this I got to know importance of employing ensemble algorithms for finding the complexities of threat detection. Our findings underscore the significance of leveraging machine learning and ensemble methods to fight against the evolving landscape of cyber threats effectively. Moving forward, our research also makes way for the development of more resilient and adaptive defense mechanisms, equipping organizations and security professionals with the tools needed to safeguard against

cyber threats effectively.

REFERENCES

[1] A. Khalid, A. Zainal, M. A. Maarof and F. A. Ghaleb, "Advanced Persistent Threat Detection: A Survey," 2021 3rd International Cyber Resilience Conference (CRC), Langkawi Island, Malaysia, 2021, pp. 1-6

[2] A. Rogachev and E. Melikhova, "Automation of Architecture Justification and Parameters Selection of Artificial Neural Networks for Intelligent Detection of Cyber-Physical Threats," 2022 International Russian Automation Conference (RusAutoCon), Sochi, Russian Federation, 2022, pp. 908-912

[3] G. Nikolov and W. Mees, "Detection of Previously Unknown Advanced Persistent Threats Through Visual Analytics with the MASFAD Framework," 2023 International Conference on Military Communications and Information Systems (ICMCIS), Skopje, North Macedonia, 2023, pp. 1-10

[4] M. Alajmi, H. A. Mengash, H. Alqahtani, S. S. Aljameel, M. A. Hamza and A. S. Salama, "Automated Threat Detection Using Flamingo Search Algorithm With Optimal Deep Learning on Cyber-Physical System Environment," in IEEE Access, vol. 11, pp. 127669-127678, 2023

[5] A. Krivo and S. Mirvoda, "The Experience of Cyberthreats Analysis Using Business Intelligence System," 2020 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT), Yekaterinburg, Russia, 2020, pp. 0619-0622

[6] A. N. Irfan, S. Chuprat, M. N. Mahrin and A. Ariffin, "Taxonomy of Cyber Threat Intelligence Framework," 2022 13th International Conference on Information and Communication Technology Convergence (ICTC), Jeju Island, Korea, Republic of, 2022, pp. 1295-1300

[7] X. Wang et al., "Learning Cyber Threat Intelligence Knowledge Graph Embedding with Heterogeneous Relation Networks Based on Multi-Head Relational Graph Attention," 2022 IEEE Smartworld, Ubiquitous Intelligence & Computing, Scalable Computing & Communications, Digital Twin, Privacy Computing, Metaverse, Autonomous Trusted Vehicles(SmartWorld/UIC/ScalCom/DigitalTwin/PriComp/Meta), Haikou, China, 2022, pp. 1796-1803

[8] K. Shaukat, S. Luo, S. Chen and D. Liu, "Cyber Threat Detection Using Machine Learning Techniques: A Performance Evaluation Perspective," 2020 International Conference on Cyber Warfare and Security (ICCWS), Islamabad, Pakistan, 2020, pp. 1-6

[9] T. Toma, S. Hassan and M. Arifuzzaman, "An Analysis of Supervised Machine Learning Algorithms for Spam Email Detection," 2021 International Conference on Automation, Control and Mechatronics for Industry 4.0 (ACMI), Rajshahi, Bangladesh, 2021, pp. 1-5

[10] K. Sathya, J. Premalatha and S. Suwathika, "Reinforcing Cyber World Security with Deep Learning Approaches," 2020 International Conference on Communication and Signal Processing (ICCSP), Chennai, India, 2020, pp. 0766-076

[11] M. A. Razib, D. Javeed, M. T. Khan, R. Alkanhel and M. S. A. Muthanna, "Cyber Threats Detection in Smart Environments Using SDN-Enabled DNN-LSTM Hybrid Framework," in IEEE Access, vol. 10, pp. 53015-53026, 2022

[12] O. Alsodi, X. Zhou, R. Gururajan and A. Shrestha, "A Survey on Detection of cybersecurity threats on Twitter using deep learning," 2021 8th International Conference on Behavioral and Social Computing (BESC), Doha, Qatar, 2021, pp. 1-5

[13] R. Mishra, "Cyber Security Threat Detection Model Using Artificial Intelligence Technology," 2023 2nd International Conference on Edge Computing and Applications (ICECAA), Namakkal, India, 2023, pp. 324-330

[14] M. Brkić, H. -S. Dinu, A. Mirković, A. Sabirović, S. Khan and D. Svetinović, "Cyber Vulnerabilities in Blockchain Electronic Health Records: An In-Depth Threat Analysis," 2023 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech), Abu Dhabi, United Arab Emirates, 2023, pp. 0784-0791

[15] A. Yeboah-Ofori et al., "Cyber Threat Predictive Analytics for Improving Cyber Supply Chain Security," in IEEE Access, vol. 9, pp. 94318-94337, 2021

[16] P. Kumar, G. P. Gupta, R. Tripathi, S. Garg and M. M. Hassan, "DLTIF: Deep Learning-Driven Cyber Threat Intelligence Modeling and Identification Framework in IoT-Enabled Maritime Transportation Systems," in IEEE Transactions on Intelligent Transportation Systems, vol. 24, no. 2, pp. 2472-2481, Feb. 2023

[17] D. Puthal, S. P. Mohanty, A. K. Mishra, C. Y. Yeun and E. Damiani, "Revolutionizing Cyber Security: Exploring the Synergy of Machine Learning and Logical Reasoning for Cyber Threats and Mitigation," 2023 IEEE Computer Society Annual Symposium on VLSI (ISVLSI), Foz do Iguacu, Brazil, 2023, pp. 1-6

[18] M. Alajmi, H. A. Mengash, H. Alqahtani, S. S. Aljameel, M. A. Hamza and A. S. Salama, "Automated Threat Detection Using Flamingo Search Algorithm With Optimal Deep Learning on Cyber-Physical System Environment," in IEEE Access, vol. 11, pp. 127669-127678, 2023

[19] V. Rathod, C. Parekh and D. Dholariya, "AI & ML Based Anamoly Detection and Response Using Ember Dataset," 2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Noida, India, 2021, pp. 1-5

[20] G. Nikolov and W. Mees, "Detection of Previously Unknown Advanced Persistent Threats Through Visual Analytics with the MASFAD Framework," 2023 International Conference on Military Communications and Information Systems (ICMCIS), Skopje, North Macedonia, 2023, pp. 1-10