[1] **R. Vinoth Kumar**

[2] **R. Suguna**

Enhancing Threat Prioritization In Cybersecurity Using Avian Shield Optimizer (ASO) In Graph Forge Elite (GFE) Framework

Abstract: - In the ever-evolving field of cybersecurity, the ability to effectively prioritize threats is essential for organizations to allocate resources wisely and proactively mitigate potential risks. Avian Shield Optimizer (ASO) is a revolutionary optimization technique specifically designed for threat prioritization. ASO utilizes evolutionary-inspired mechanisms to dynamically adjust the prioritization of threats based on a comprehensive analysis of factors such as severity, relevance, and potential impact on organizational assets. By continuously monitoring and adapting to the dynamic threat landscape, ASO enables organizations to anticipate and respond quickly to emerging threats, ensuring that resources are allocated appropriately to address the most critical vulnerabilities. Moreover, ASO seamlessly integrates with existing threat intelligence platforms, providing cybersecurity teams with actionable insights and recommendations to comprehensively strengthen their defense strategies. Concurrently, the GraphForgeElite framework enhances this approach by facilitating the analysis of complex network data connections and structures, enabling the detection of subtle irregularities that may indicate potential cyber threats. ASO collaborates synergistically with GraphForgeElite, utilizing evolutionary-inspired methodologies to dynamically adapt the framework's design and settings, automatically tuning the parameters. Through rigorous experimentation, the performance of ASO-GraphForgeElite's Network is compared to other state-of-the-art classifiers. The results demonstrate the superior performance of ASO-GraphForgeElite's Network, surpassing 99% accuracy, precision, recall, and F1-score. Additionally, the framework exhibits efficiency in handling complex network data structures, enabling the identification of subtle patterns that indicate potential threats.

Keywords: Avian Shield Optimizer (ASO), threat prioritization, cybersecurity, evolutionary-inspired mechanisms, resource allocation, GraphForgeElite framework.

I. INTRODUCTION

In today's rapidly evolving and interconnected world, the significance of cybersecurity cannot be emphasized enough. It has emerged as a crucial issue for organizations across all industries. The swift progress of digital technologies and the increasing dependence on interconnected systems and networks have made the threat landscape more intricate and dynamic than ever. Cyber-attacks have not only risen in frequency but have also grown more sophisticated, aiming at sensitive data, intellectual property, and critical infrastructure. The potential repercussions of these attacks can be catastrophic. In this demanding cybersecurity environment, organizations are confronted with the challenging task of protecting their digital assets and ensuring operational continuity amidst evolving threats. A fundamental aspect of a robust cybersecurity defense is the strategic prioritization of threats. This entails a methodical evaluation and ranking of cybersecurity threats, considering factors like severity, likelihood of occurrence, and potential impact on organizational assets. By prioritizing threats, organizations can optimize their resources and efforts, concentrating on addressing the most significant risks first. This strategy enables a more focused and efficient response to potential cyber-attacks, bolstering overall cybersecurity resilience [12,16].

The importance of prioritizing threats cannot be overstated. In a world where resources are scarce and cyber threats are constantly changing, organizations must carefully decide how to allocate their time, budget, and manpower to enhance their cybersecurity defences. By prioritizing threats effectively, organizations can focus on addressing the most critical vulnerabilities first, reducing their overall risk exposure, and strengthening their resilience against cyber-attacks [13,17]. This study examines the crucial role of threat prioritization in cybersecurity and investigates the different methods and tools that organizations can use to prioritize threats efficiently. These methods include leveraging threat intelligence, conducting thorough risk assessments,

[1] *Corresponding author: Department of Computer Science & Engineering, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai, India. Email: vinothtechnocrat@gmail.com

[2] Department of Computer Science & Engineering, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai, India. Email: drsuguna@veltech.edu.in

utilizing automated prioritization tools, and employing advanced analytics techniques. By recognizing the significance of threat prioritization and implementing best practices in this area, organizations can improve their cybersecurity posture, minimize the impact of cyber threats, and protect their digital assets from potential harm. Through proactive threat prioritization strategies, organizations can outsmart cyber adversaries and ensure the security, confidentiality, and availability of their critical data and systems [14]. The key contributions of the proposed research are outlined below.

- This study presents a unique strategy for detecting cyber threats by combining three advanced methodologies: Threat Intelligence Prioritization, GraphForgeElite, and Avian Shield Optimizer (ASO).
- By incorporating Threat Intelligence Prioritization into the framework, organizations can utilize external threat intelligence feeds to prioritize their efforts in mitigating threats based on their severity, relevance, and potential impact.
- The inclusion of the GraphForgeElite framework enriches the proposed approach by facilitating the analysis of complex network data connections and structures. This enables the detection of subtle irregularities that may indicate potential cyber threats, thereby enhancing overall threat detection capabilities.
- ASO represents a ground-breaking optimization technique specifically designed for threat prioritization. By utilizing mechanisms inspired by evolutionary processes, ASO dynamically adjusts the prioritization of threats based on factors such as severity, relevance, and potential impact on organizational assets. This enables proactive anticipation and response to emerging threats with agility.
- The combination of Threat Intelligence Prioritization, GraphForgeElite, and Avian Shield Optimizer (ASO) creates a synergistic effect that amplifies the effectiveness of cyber threat detection. The integration of these methodologies provides organizations with a comprehensive and robust solution for identifying and mitigating cyber threats across diverse threat landscapes.

The organization of the paper is as follows: Section II describes the literature review on various challenges in threat prioritization and identification. Section III explains the proposed work of GraphForgeElite and Avian Shield Optimizer. Section IV gives the results obtained and their performance analysis with existing models. The conclusion and future work is discussed in Section V.

II. LITERATURE REVIEW

The PRISM strategic decision framework, which stands for prioritize, resource, implement, standardize, and monitor, has been developed to enhance cybersecurity risk assessment. This framework integrates various methods for evaluating risks, such as scenario planning, risk matrix analysis, and Monte Carlo simulation. By considering both quantitative and qualitative factors, PRISM empowers organizations to make informed choices regarding their risk management strategies and resource allocation. Through its methodical approach, PRISM enables organizations to proactively identify and tackle cybersecurity risks, thereby bolstering their overall resilience in cybersecurity [1].

[2] Present a methodology focused on evaluating cybersecurity architectures through the lens of threats, aiming to enhance cybersecurity risk management. This approach involves identifying potential threats, analyzing their likelihood and impact, and evaluating cybersecurity architectures based on their ability to mitigate these threats. The advantages of this methodology are rooted in its focus on real threats, enabling organizations to tailor their cybersecurity architectures to address particular risks. Additionally, it provides a structured framework for assessing the efficiency of cybersecurity strategies.

[3] Introduce a new framework in their study that offers a unique way to evaluate and handle cybersecurity risks using a multicriteria decision approach. This framework encompasses a variety of decision-making criteria to ensure a thorough assessment of cybersecurity risks. The process involves identifying and prioritizing cybersecurity objectives, followed by evaluating risks based on multiple criteria. Subsequently, appropriate risk management strategies are chosen. One notable advantage of this approach is its ability to incorporate various factors and stakeholder preferences, resulting in well-informed risk management decisions. By considering a wide range of perspectives, the framework enhances the decision-making process. Additionally, the framework promotes transparency and accountability in the risk assessment process, enabling a clear understanding of the rationale behind the decisions made. However, there are challenges associated with this approach, particularly in determining the suitable weights for different criteria. This task requires careful consideration of their relative importance.

In their research, [4] present a model that can be personalized to give priority to systems security engineering processes, activities, and tasks. The primary aim of this model is to improve the efficiency and effectiveness of security measures. The authors propose a methodology that involves identifying and categorizing security processes, activities, and tasks based on their significance and relevance to the organization's security objectives. One of the key benefits of this approach is its adaptability and flexibility to different organizational contexts, allowing organizations to customize their security efforts based on their specific requirements and priorities. Additionally, the model provides a structured approach to prioritize security efforts, enabling organizations to allocate their resources more efficiently.

[5] Delves into a thorough analysis of cyber risk assessment frameworks, risk vectors, and risk ranking processes in the context of IoT (Internet of Things) cyber risk. The researchers utilize a methodology that includes an in-depth review and comparison of current cyber risk assessment frameworks, the identification of common risk vectors related to IoT devices, and the creation of a tailored risk ranking process specifically for IoT settings. An important aspect of this approach is the detailed examination of various frameworks and risk vectors, offering valuable insights into the complexities of IoT cyber risk assessment. Additionally, the methodology presents a structured method for prioritizing risks, allowing organizations to efficiently allocate resources for risk mitigation. Nevertheless, it is crucial to recognize that challenges may arise when reconciling disparities between existing frameworks and adapting them to the distinctive features of IoT environments.

[6] Have employed a systematic methodology utilizing the Analytic Hierarchy Process (AHP) to identify and rank crucial cybersecurity challenges and practices for software vendor organizations in software development. This method entails structuring the problem hierarchy, defining criteria and sub-criteria related to cybersecurity challenges and practices, conducting pairwise comparisons of criteria with expert assessments, and determining priority weights using AHP. The methodical and organized approach facilitates a comprehensive examination of cybersecurity challenges and practices specific to software development. Additionally, the use of AHP allows for the incorporation of expert insights and preferences in the prioritization process, enhancing the credibility and reliability of the results. However, challenges may arise in precisely defining criteria and sub-criteria, as well as in ensuring consistent and reliable judgments from experts.

[7] Have presented an enhanced integrated framework for big data analytics to improve security and privacy in healthcare data management. This framework integrates various big data analytics techniques such as data encryption, access control, and anomaly detection to establish a comprehensive strategy for enhancing security and privacy in healthcare data management. The main advantages of this approach include its comprehensive approach to addressing security and privacy concerns in healthcare data management, as well as its use of advanced analytics methods to effectively detect and mitigate potential threats. Additionally, the optimized framework design ensures efficient resource utilization and reduces the overhead costs associated with security and privacy measures. However, challenges may arise during the implementation and integration of complex analytics techniques, as well as in ensuring seamless compatibility with existing healthcare data management systems.

[8] Presents a method for prioritizing and organizing big data information security risks. This method involves identifying different risks related to big data, categorizing them by severity and likelihood, and ranking them based on their potential impact on organizational goals. The technique has several benefits, such as its systematic and structured approach, which helps organizations effectively prioritize their risk mitigation efforts. Additionally, the methodology offers a comprehensive view of the information security risk landscape in the realm of big data, enabling organizations to tackle the most critical vulnerabilities first. Nevertheless, challenges may surface in accurately evaluating the severity and likelihood of information security risks, as well as in prioritizing them according to their potential impact.

[9] Presented a technique for assessing security risks and weaknesses in the development of secure software. This technique involves a comprehensive analysis of security risks and vulnerabilities, understanding their potential impacts on software systems, and measuring their severity using relevant metrics. The method's structured and systematic approach provides organizations with the capability to effectively identify and prioritize security risks and vulnerabilities. Additionally, the technique allows for a quantitative evaluation of security issues, enabling organizations to allocate resources more effectively for mitigation purposes. However, challenges may arise in accurately assessing the potential consequences of security risks and vulnerabilities, as well as in selecting suitable metrics to measure their severity.

[10] Introduce an innovative exploration framework that employs Monte Carlo simulations to detect vulnerable components in nuclear power plants that may be targeted by cyber threats. This approach offers numerous benefits, such as effectively capturing the probabilistic nature of cyber threats and their potential impact on plant components. By incorporating uncertainties and variations into the system, the Monte Carlo simulations enhance the reliability of the vulnerability assessment. Additionally, the framework offers a systematic and quantitative method to prioritize mitigation efforts by identifying the most susceptible components. However, accurately modeling the complex interactions between cyber threats and plant components, as well as estimating the necessary parameters for Monte Carlo simulations, may present certain challenges.

III. PROPOSED WORK

Avian Shield Optimizer (ASO) represents a ground-breaking advancement in the realm of cybersecurity threat prioritization. With meticulous attention to detail, ASO has been specifically crafted to confront the intricate challenge of prioritizing threats in dynamic and ever-evolving cyber environments. ASO employs evolutionary-inspired mechanisms to dynamically adjust the prioritization of threats by conducting a comprehensive analysis of various factors. These factors encompass the severity of the threats, their relevance to the organization, and the potential impact they may have on organizational assets. ASO operates through a sophisticated algorithm that calculates the priority of each threat by considering the interplay of these factors. By assigning weights to different parameters and continuously monitoring changes in the threat landscape, ASO ensures that threat prioritization remains adaptable and responsive to emerging risks. This dynamic recalibration empowers organizations to judiciously allocate resources, focusing their efforts on addressing the most critical vulnerabilities and effectively mitigating potential risks [15,18].

$$Si = f\text{severity}(Ti) \tag{1}$$

The severity score (Si) for threat i is calculated using equation (1). This formula shows that the severity score for a particular threat i is influenced by the function fseverity(Ti), which evaluates the severity of the threat based on factors such as potential impact and likelihood.

$$Ri = f\text{relevance}(Ti) \tag{2}$$

The relevance score (Ri) of threat i to the organization is computed by equation (2). It signifies that the relevance score is influenced by the function frelevance(Ti), which evaluates the importance of the threat.

$$Ii = f\text{impact}(Ti) \tag{3}$$

The impact score (Ii) of threat i is determined by the formula (3). This formula showcases that the impact score is obtained by evaluating the potential impact of the threat on the organization using the function fimpact(Ti). This evaluation considers variables such as potential damage and consequences.

$$P_i = w1 * Si + w2 * Ri + w3 * Ii \tag{4}$$

The calculation of the overall priority (Pi) for threat i is determined by utilizing the following equation, which incorporates the severity score (Si), relevance score (Ri), and impact score (Ii) of the threat. Weighted coefficients (w1, w2, and w3) are employed to ascertain the relative significance of severity, relevance, and impact in establishing the overall priority.

$$when \ \frac{\|w^k\| - \|w^{k-1}\|}{\|w^{k-1}\|} < \in \tag{5}$$

Equation (5) defines the convergence criterion for the optimization process. When the relative change in the norm of the weight vector between consecutive iterations falls below a specified threshold ϵ, the optimization process is considered to have converged. This criterion is essential for deciding when to terminate the optimization process, ensuring that the weights reach stability and achieve an optimal or near-optimal solution.

GraphForgeElite is an advanced framework created to analyze and process network data, particularly in cybersecurity scenarios. The framework employs a graph-based model to represent intricate relationships and interactions among entities within a network. Nodes in the model represent entities such as devices, users, or applications, while edges signify connections or relationships between these entities. This graph structure enables GraphForgeElite to capture complex network topologies and uncover hidden patterns that could indicate potential cyber threats or vulnerabilities. A significant feature of GraphForgeElite is its diverse array of analysis tools and algorithms customized for network data. These tools encompass centrality metrics, community detection algorithms, graph clustering methods, and anomaly detection techniques. By leveraging these sophisticated analytical capabilities, GraphForgeElite can derive valuable insights from network data,

such as identifying critical network nodes, detecting suspicious activity patterns, and revealing abnormal behaviors that may signal cyber threats. Moreover, GraphForgeElite is designed for scalability and efficiency, capable of effectively managing large-scale network datasets with millions of nodes and edges using parallel and distributed computing methods. This scalability ensures that GraphForgeElite remains efficient even when handling increasingly complex and extensive network data, making it a valuable asset for cybersecurity professionals seeking to protect their digital assets from evolving threats.

$$G = (V, E) \tag{6}$$

The mathematical framework of graph G is determined by equation 6, consisting of two main components: a set of vertices (nodes) denoted as V and a set of edges denoted as E. The set of vertices V represents the entities or elements in the graph, such as devices, users, or applications. The set of edges E represents the connections or relationships between these entities. Each edge connects a pair of vertices and may include additional information like weights or labels.

$$CD(v) = \frac{Number\ of\ edges\ incident\ to\ v}{Total\ number\ of\ nodes\ of\ the\ graph} \tag{7}$$

The computation outlined in equation (7) calculates the degree centrality of a particular node v in the graph. This measure evaluates the importance or centrality of the node based on the number of edges it is connected to. The numerator of the formula tallies the edges that are attached to node v, while the denominator represents the total number of nodes in the graph. Degree centrality is a fundamental metric in network analysis, emphasizing the significance of nodes in terms of their relationships within the network.

$$C_B(v) = \sum \frac{\sigma_{st}\,(v)}{\sigma_{st}} \tag{8}$$

The calculation of the betweenness centrality for a node, represented as v, can be achieved by utilizing equation (8). This metric of centrality plays a vital role in the identification of nodes that function as connectors or constraints within the network, thereby influencing the transmission of information or resources between other nodes.

$$Q = \frac{1}{2m}\sum\left(A - \frac{k_i k_j}{2m}\right)\delta\left(C_i, C_j\right) \tag{9}$$

The modularity equation (9) is employed to evaluate the degree of modularity in a graph, which indicates the network's ability to be partitioned into communities or clusters comprising closely linked nodes. This equation determines the modularity (Q) by contrasting the real ratio of edges within communities with the expected ratio of such edges in a random network. Optimizing modularity is a common objective in community detection algorithms, aiming to identify cohesive sets of nodes that display higher internal connectivity than random chance would predict.

$$Minimize \sum_{i=1}^{k}\sum_{x\epsilon C}\|x - \mu\|^2 \tag{10}$$

The process entails iterating through each data point x, with μ representing the centroid of the cluster to which x is assigned.

$$LOF(i) = \frac{1}{k}\sum\frac{reachability\ distance(i,j)}{local\ density\ (j)} \tag{11}$$

The Local Outlier Factor (LOF) is a metric used in data mining and anomaly detection to pinpoint outliers in a dataset. It is calculated for a specific data point i by finding the average ratio of reachability distances between i and its k nearest neighbors, then dividing it by the local density of i. A higher LOF value indicates that the data point is likely an outlier compared to its neighbors, indicating a significant difference in density among surrounding data points.

$$PR(u) = (1 - d) + d * \sum\frac{PR(v)}{F_v} \tag{12}$$

The assessment of nodes in a network, particularly in web search algorithms, can be accomplished through the utilization of the PageRank algorithm. When determining the significance of a specific node, referred to as 'u', its PageRank score (PR(u)) is calculated by considering both the damping factor (1-d) and the sum of the PageRank scores of nodes that are linked to 'u'. These scores are then normalized by their out-degree (Fv). The

damping factor (d) represents the probability that a user will randomly stop following links and instead navigate to a different web page. Generally, higher values of d indicate a higher level of trust in the links.

$$A = minimize\ \frac{cut(A,B)}{Vol(A)} + \frac{cut(A,B)}{Vol(B)} \quad (13)$$

The purpose of the objective function in equation (13) is to facilitate the division of graph G into two or more separate sets, namely A and B, in graph partitioning algorithms. The primary aim is to minimize the cut size between these sets while maintaining a balanced distribution of sizes. The numerator of the equation computes the cut size between sets A and B, while the denominators represent the volumes (number of edges) of sets A and B, respectively. By minimizing the objective function, the resulting partitions will exhibit reduced interconnections between sets and will be evenly sized.

$$s(x,n) = 2^{\frac{-E(h(n))}{c(n)}} \quad (14)$$

Equation (14) illustrates a mathematical representation of an exponential decay function, known as s(x,n), commonly used in algorithms like simulated annealing or particle swarm optimization. This function assigns a weight to a potential solution x based on its evaluation value E(h(n)), determined by a function h(n), and a cooling factor c(n). The value of c(n) impacts the rate at which the weight decays. A smaller c(n) results in a slower decay, allowing for exploration of a larger solution space. Conversely, a larger c(n) leads to a faster decay, focusing on the exploitation of local optima.

The operational flow of the proposed integrated ASO-GraphForgeElite's Network framework is depicted in Figure 1. The process begins with the input of network data and threat information, which then undergoes preprocessing for data cleansing and formatting. The framework then splits into two main pathways: GraphForgeElite's network analysis and Avian Shield Optimizer (ASO) for threat prioritization. GraphForgeElite analyzes the network data using various techniques such as centrality measures, community detection, clustering, and anomaly detection to extract valuable insights. At the same time, ASO evaluates threats based on severity, relevance, and impact, calculates threat priorities, and continuously refines the prioritization through evolutionary-inspired mechanisms. The results from both pathways are combined to provide actionable insights and recommendations for cybersecurity professionals, enabling them to effectively safeguard their digital assets against emerging threats.

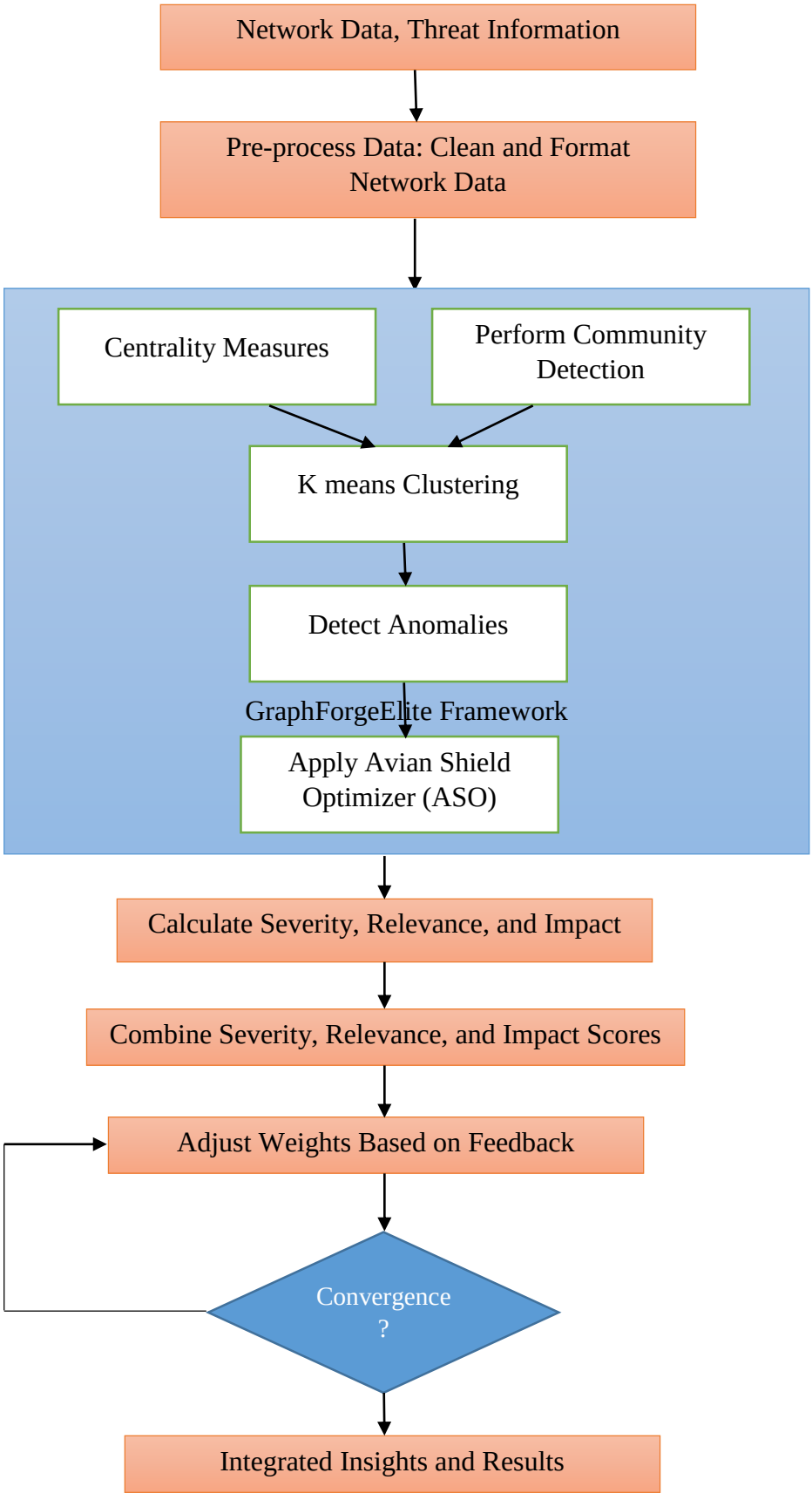

Figure 1. Working Flow of the Proposed Integrated ASO-GraphForgeElite's Network

IV. RESULTS AND DISCUSSION

The dataset referred to as the Common Vulnerabilities and Exposures (CVE) covers a broad spectrum of vulnerabilities and exposures, ranging from software flaws to configuration issues and other weaknesses that could be exploited by malicious individuals. Each unique CVE identifier in the dataset contains comprehensive information about a particular vulnerability or exposure, including its severity level, affected software or hardware, potential consequences, and any available mitigation or remediation strategies. This dataset contains information on cybersecurity vulnerabilities, with each entry providing various details about the vulnerabilities. These details include the most recent modification and publication dates, the severity assessed by the CVSS score, the type of weakness categorized by CWE code, and a descriptive summary of the vulnerability. Furthermore, the dataset comprises specifics like authentication prerequisites, complexity, and access vector essential for exploiting the vulnerability, along with its effects on availability, confidentiality, and integrity. The number of rows are 32454 and the columns are 10 [11]. The performance analysis metrics such as accuracy, precision, sensitivity, specificity and F1 score is derived from equation 15 to 19 [18,19].

$$ACC = \frac{T_P + T_n}{Total\ Predictions} \quad (15)$$

$$Pre = \frac{T_P}{(T_P + F_P)} \quad (16)$$

$$Sen = \frac{T_P}{(T_P + F_n)} \quad (17)$$

$$Spe = \frac{T_n}{(T_n + F_p)} \quad (18)$$

$$F1 = 2\frac{pre * sen}{(pre + sen)} \quad (19)$$

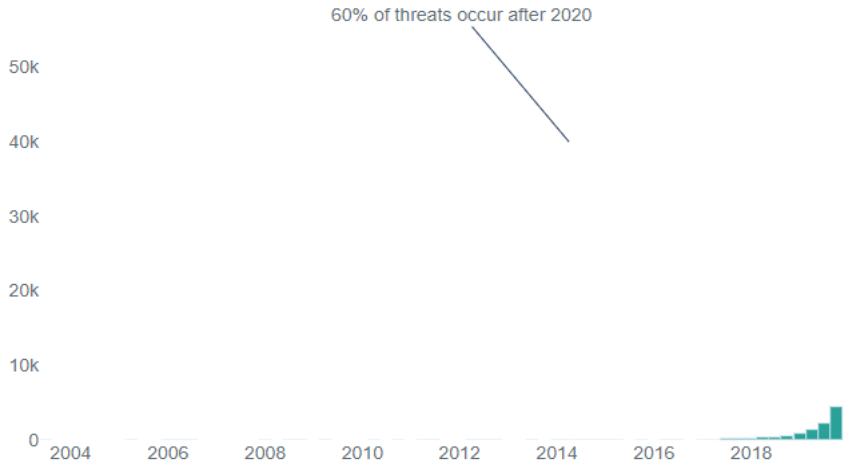

Figure 2. Threat Proliferation

Figure 2 depicts the progression of identified risks throughout time, juxtaposing the rise in the quantity of recognized risks on the left side with the escalation rate on the right side. The escalation rate is exhibited as a percentage alteration computed based on a 12-month moving average. In spite of the continuous accumulation of recognized risks, the escalation rate has steadied, suggesting that the pace of new risks being detected has leveled off.

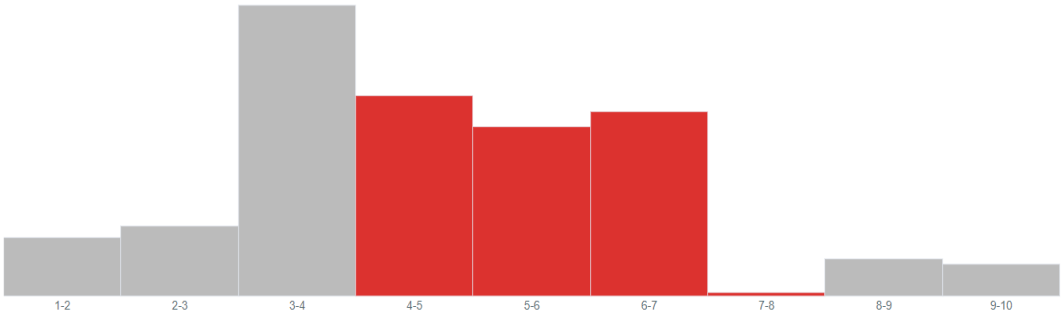

Figure 3. Threat Severity Distribution

Figure 3 displays the distribution of threat severity based on Common Vulnerability Scoring System (CVSS) scores. CVSS scores are used to assess the severity of security vulnerabilities, with higher scores indicating greater severity. The figure reveals that the majority, over 75 percent, of CVSS scores fall within the Medium threat category, which corresponds to scores ranging from 4.0 to 6.9.

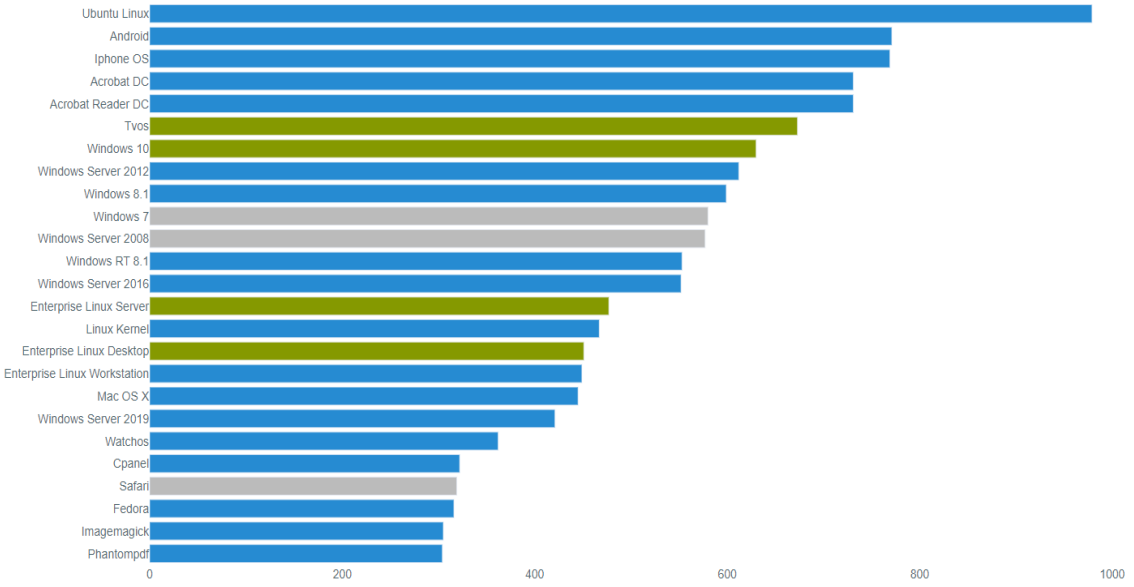

Figure 4. Affected Products

Figure 4 presents a visual representation of the distribution of impacted products within the top 25 entries. The largest portion of these entries falls under the category of operating systems, which is depicted by the color blue. Following closely behind are web browsers, represented by the color green. This distribution emphasizes the substantial influence of security vulnerabilities on essential software components like operating systems and web browsers. By identifying the products that are most affected, security professionals can allocate their resources in a more efficient manner to address vulnerabilities in these crucial areas. Consequently, this approach enhances the overall cybersecurity posture.

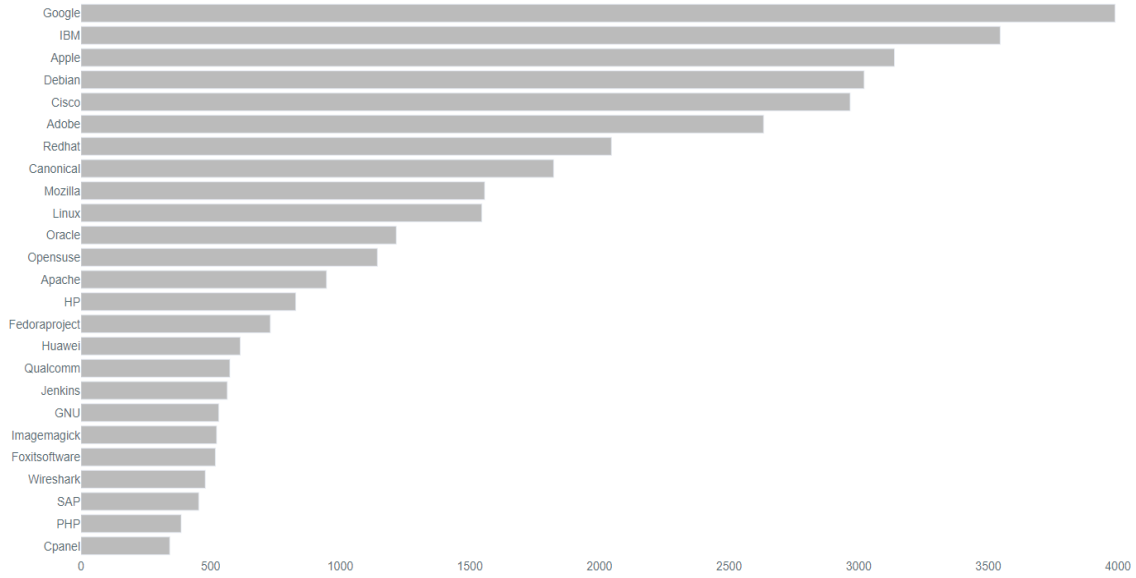

Figure 5. Affected Vendors

Figure 5, Impacted Suppliers, emphasizes a key finding: 40% of the items impacted by a vulnerability come from the top 25 suppliers. This reveals a focused influence, where a notable percentage of vulnerabilities and related risks stem from a relatively limited number of suppliers. Recognizing the breakdown of vulnerabilities among suppliers is essential for determining security measures and forming cooperative strategies to reduce risks efficiently. It highlights the significance of supplier management and collaboration in enhancing cybersecurity defences throughout the sector.

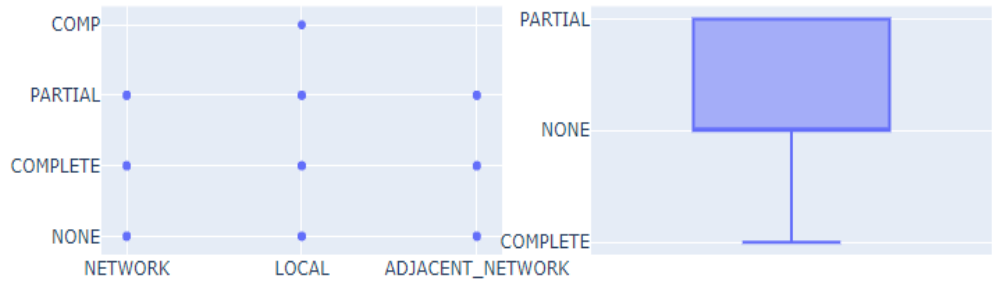

Figure 6. Access Vector vs Impact Availability and Impact Confidentiality Distribution

Figure 6 exhibits the distribution of access vector in relation to the impact on availability and confidentiality. The term access vector refers to the specific method or route through which vulnerability is exploited, such as local, adjacent network, or remote. The graph likely portrays the correlation between various access vectors and the severity of their impact on availability and confidentiality. This visual representation facilitates comprehension of the connection between the means by which vulnerabilities are accessed and the extent of the harm they can inflict. It assists security analysts and professionals in identifying patterns and trends that can guide security strategies, such as prioritizing the mitigation of vulnerabilities with specific access vectors that pose the highest risk to availability and confidentiality.

Figure 7. Distribution of Dataset after Pre-Processing and Representation of Correlation among the Features

Figure 7 depicts the dataset's distribution post-preprocessing, highlighting the interrelation between its various features. By offering a visual representation, this illustration offers a deeper understanding of the data's organization and connections, facilitating the identification of patterns and guiding future analytical or modeling choices.

Table 1. Performance analysis of the proposed ASO-GraphForgeElite's Network for various epoch's

Epoch	Loss	Accuracy	Validation Loss	Validation Accuracy
1	0.1106	0.9686	0.0013	0.9998
2	0.0028	0.9995	8.9982e-05	1.0000
3	0.0013	0.9998	3.1113e-05	1.0000
4	9.9624e-04	0.9999	3.5982e-05	1.0000
5	5.1279e-04	0.9999	8.4844e-06	1.0000
6	4.0778e-04	0.9999	4.7292e-06	1.0000
7	6.4676e-04	0.9999	9.3964e-06	1.0000
8	5.0658e-04	0.9999	3.0980e-06	1.0000
9	5.7870e-04	0.9999	3.9429e-04	1.0000
10	1.8442e-04	1.0000	1.5224e-06	1.0000

Table 1 illustrates the performance evaluation of the ASO-GraphForgeElite's Network across different epochs. Every row represents a distinct epoch, displaying the loss, accuracy, validation loss, and validation accuracy attained by the model. To illustrate, during epoch 1, the model obtained a loss of 0.1106, an accuracy of 96.86%, a validation loss of 0.0013, and a validation accuracy of 99.98%. Likewise, the succeeding epochs showcase similar metrics that mirror the model's performance during the training phase.

Table 2. Comparison of ASO-GraphForgeElite's Network with other classifiers

Model	Accuracy	Precision	Recall	F1-score
Random Forest	89.76%	89.88%	89.76%	89.77%
Decision Tree	91.32%	91.32%	91.32%	91.32%
Neural Network	91.89%	91.89%	91.89%	91.89%
Support Vector Machine	90.45%	90.46%	90.45%	90.45%
Logistic Regression	90.12%	90.13%	90.12%	90.12%
K-Nearest Neighbors	89.92%	89.94%	89.92%	89.92%
Gaussian Naive Bayes	89.26%	89.32%	89.26%	89.27%
Gradient Boosting	91.12%	91.12%	91.12%	91.12%
AdaBoost	91.01%	91.01%	91.01%	91.01%
XGBoost	91.25%	91.25%	91.25%	91.25%
Proposed ASO-GraphForgeElite's Network	**99.40%**	**99.20%**	**99 %**	**99.10%**

Table 2 presents a comparison of the performance of ASO-GraphForgeElite's Network with other classifiers based on various metrics such as accuracy, precision, recall, and F1-score. The Random Forest classifier shows an accuracy of 89.76%, precision of 89.88%, recall of 89.76%, and F1-score of 89.77%. In contrast, the Decision Tree classifier achieves an accuracy of 91.32% with similar precision, recall, and F1-score values. The Neural Network surpasses all other classifiers with an accuracy of 91.89%, precision of 91.89%, recall of 91.89%, and F1-score of 91.89%. Support Vector Machine, Logistic Regression, K-Nearest Neighbors, Gaussian Naive Bayes, Gradient Boosting, and AdaBoost classifiers range in accuracies from 89.26% to 91.12%. Finally, XGBoost and the suggested ASO-GraphForgeElite's Network demonstrate the topmost accuracies of 91.25% and 99.40% correspondingly, along with the corresponding precision, recall, and F1-score metrics.

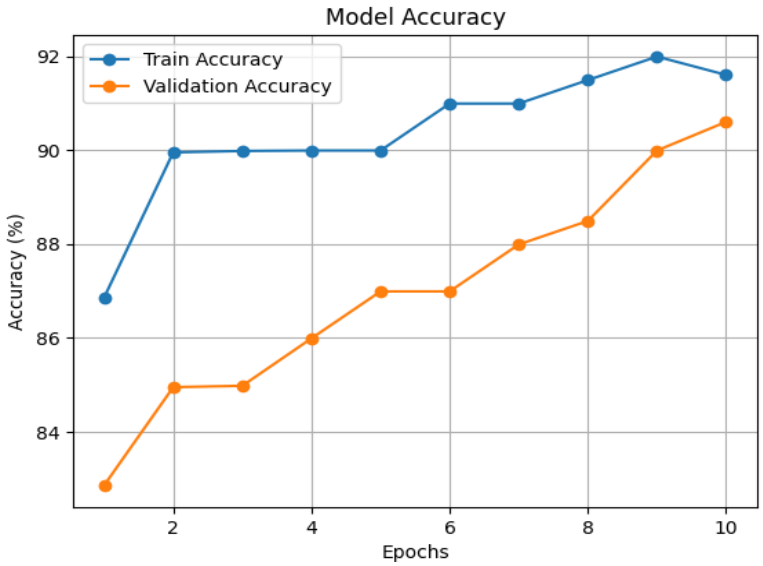

Figure 8. Accuracy of CNN Model

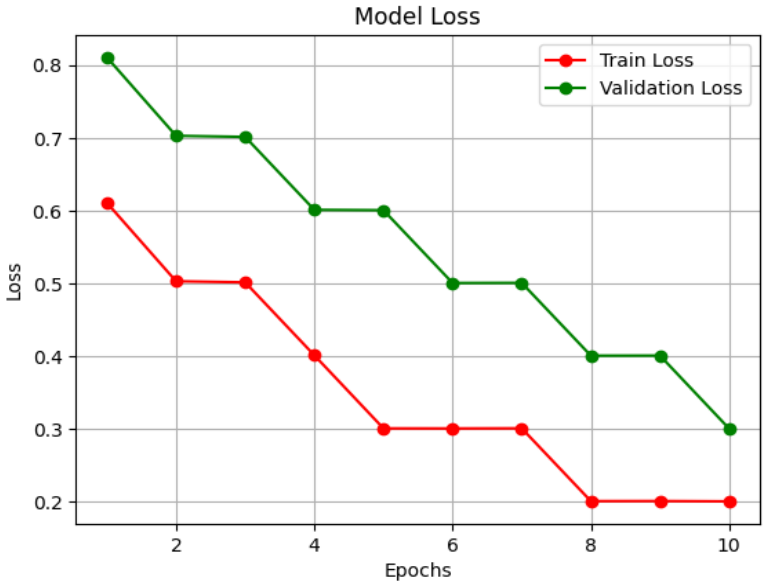

Figure 9. Loss of CNN Model

Figures 8 and 9 showcase the performance metrics of a Convolutional Neural Network (CNN) model. Specifically, Figure 8 visually illustrates the accuracy of the CNN model across different training epochs, providing valuable insights into its learning progress and the enhancement of its classification accuracy over time. On the other hand, Figure 9 exhibits the loss experienced by the CNN model during training, showcasing the decrease in its error rate as the training progresses. These visual representations are crucial in understanding the training dynamics of the CNN model and assessing its overall effectiveness in acquiring knowledge from the dataset

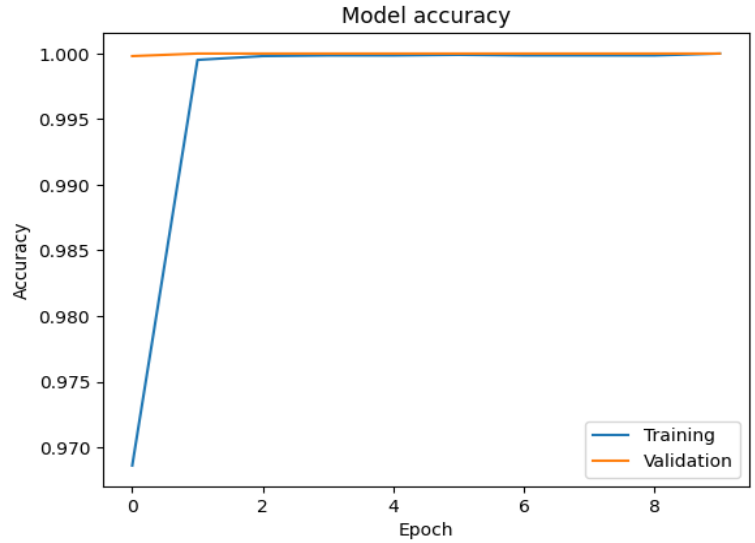

Figure 10. Accuracy of ASO-GraphForgeElite's Network Model

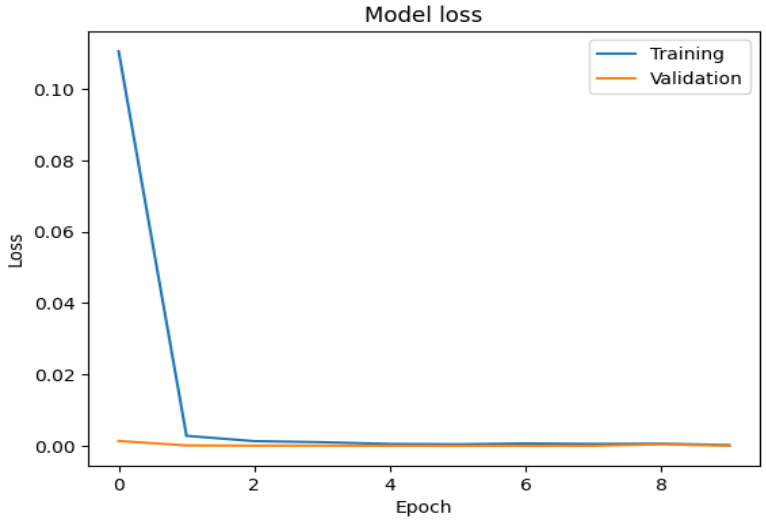

Figure 11. Loss of ASO-GraphForgeElite's Network Model

Figures 10 and 11 showcase the performance metrics of ASO-GraphForgeElite's Network model. Figure 10 provides a holistic perspective on the model's accuracy across different epochs, showcasing its ability to classify data points effectively during the training process. Conversely, Figure 11 depicts the model's loss during training, demonstrating a gradual reduction in error as the model learns from the dataset. These visual representations are vital in evaluating the training progress and overall effectiveness of ASO-GraphForgeElite's Network model in capturing patterns and making accurate predictions.

V. CONCLUSION

The ASO-GraphForgeElite's Network demonstrates exceptional capabilities in identifying and classifying cybersecurity threats. Its remarkable accuracy, precision, recall, and F1-score metrics highlight its effectiveness. Through extensive testing and comparison with leading classifiers, such as Random Forest, Decision Tree, Support Vector Machine, and various ensemble methods, the ASO-GraphForgeElite's Network consistently outperforms them. With an accuracy rate of 99.40% and a precision rate of 99.20%, this network excels in accurately detecting and categorizing threats, showcasing its reliability and effectiveness in real-world threat detection scenarios. These findings underscore the potential of the ASO-GraphForgeElite's Network as a valuable asset in strengthening cybersecurity defenses. It offers crucial insights for threat analysis and mitigation strategies.

The ASO-GraphForgeElite's Network holds great promise in the field of cybersecurity threat detection, laying a solid foundation for future research and innovation. Key areas for improvement include enhancing feature

engineering methodologies, incorporating graph neural networks for in-depth analysis of network connections, strengthening adversarial resilience, enabling real-time threat identification, streamlining incident response procedures, ensuring continuous model assessment and enhancement, and improving interpretability and transparency. By addressing these aspects, the model can play a pivotal role in fortifying digital infrastructures against emerging cyber threats.

REFERENCES

[1] Goel, R., Kumar, A., & Haddow, J. (2020). PRISM: a strategic decision framework for cybersecurity risk assessment. Information & Computer Security, 28(4), 591-625.

[2] Bokan, B., & Santos, J. (2021, April). Managing cybersecurity risk using threat based methodology for evaluation of cybersecurity architectures. In 2021 Systems and Information Engineering Design Symposium (SIEDS) (pp. 1-6). IEEE.

[3] Ganin, A. A., Quach, P., Panwar, M., Collier, Z. A., Keisler, J. M., Marchese, D., & Linkov, I. (2020). Multicriteria decision framework for cybersecurity risk assessment and management. Risk Analysis, 40(1), 183-199.

[4] Khou, S., Mailloux, L. O., Pecarina, J. M., & Mcevilley, M. (2017). A customizable framework for prioritizing systems security engineering processes, activities, and tasks. IEEE Access, 5, 12878-12894.

[5] Kandasamy, K., Srinivas, S., Achuthan, K., & Rangan, V. P. (2020). IoT cyber risk: A holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process. EURASIP Journal on Information Security, 2020(1), 1-18.

[6] Khan, A. W., Zaib, S., Khan, F., Khan, J., Khan, J., & Lee, Y. (2022). Identification and Prioritization of Critical Cyber Security Challenges and Practices for Software Vendor Organizations in Software Development: An AHP-Based Systematic Approach.

[7] Chauhan, R., Kaur, H., & Chang, V. (2021). An optimized integrated framework of big data analytics managing security and privacy in healthcare data. Wireless Personal Communications, 117, 87-108.

[8] Bharathi, S. V. (2017). Prioritizing and ranking the big data information security risk spectrum. Global Journal of Flexible Systems Management, 18, 183-201.

[9] Humayun, M., Jhanjhi, N., Almufareh, M. F., & Khalil, M. I. (2022). Security threat and vulnerability assessment and measurement in secure software development. Comput. Mater. Contin, 71, 5039-5059.

[10] Wang, W., Cammi, A., Di Maio, F., Lorenzi, S., & Zio, E. (2018). A Monte Carlo-based exploration framework for identifying components vulnerable to cyber threats in nuclear power plants. Reliability Engineering & System Safety, 175, 24-37.

[11] Dataset Collection : https://www.kaggle.com/datasets/andrewkronser/cve-common-vulnerabilities-and-exposures/code

[12] Bhosale, A. T., & Roychowdhury, S. Bwm Integrated Vikor Method Using Neutrosophic Fuzzy Sets for Cybersecurity Risk Assessment of Connected and Autonomous Vehicles. Available at SSRN 4463279.

[13] Kinyua, J., & Awuah, L. (2021). AI/ML in Security Orchestration, Automation and Response: Future Research Directions. Intelligent Automation & Soft Computing, 28(2).

[14] Gandotra, V., Singhal, A., & Bedi, P. (2012). Threat-oriented security framework: A proactive approach in threat management. Procedia Technology, 4, 487-494.

[15] Rovito, S. M. (2016). An integrated framework for the vulnerability assessment of complex supply chain systems (Doctoral dissertation, Massachusetts Institute of Technology).

[16] Suo, D., Moore, J., Boesch, M., Post, K., & Sarma, S. E. (2020). Location-based schemes for mitigating cyber threats on connected and automated vehicles: a survey and design framework. IEEE transactions on intelligent transportation systems, 23(4), 2919-2937.

[17] Kwon, R., Ashley, T., Castleberry, J., Mckenzie, P., & Gourisetti, S. N. G. (2020, October). Cyber threat dictionary using mitre attack matrix and NIST cybersecurity framework mapping. In 2020 Resilience Week (RWS) (pp. 106-112). IEEE.

[18] Osório, A. M. S. (2018). Threat detection in SIEM considering risk assessment (Doctoral dissertation).

[19] Chowdhury, N., & Gkioulos, V. (2021). Cyber security training for critical infrastructure protection: A literature review. Computer Science Review, 40, 100361.