AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
Peer Reviewed, Referred & Indexed Journal
E-ISSN:3069-0102
VOL.6, NO. 2(1) (2026)

Defense Strategies for Epidemic Cyber Security Threats: Modeling and Analysis by Using a Machine Learning Approach

Mrs. K.BHARATHI, M. Tech-Assistant Professor, Department of MCA, Bapatla Engineering College Bapatla, Andhra Pradesh

Mr. NUTHALAPATI SUMANTH, (Reg No : Y25MC23055), Ms. SERUMANTHAPURI CHINNI, (Reg No : Y25MC23074)
Ms. TIRUMALASETTI VIGNESWARI, (Reg No: Y25MC23092), Ms. DUNNA SMILY, (Reg No : Y25MC23018),
Department of MCA, Bapatla Engineering College, Bapatla, Andhra Pradesh, India

Abstract—Cyber security threats are getting worse because of how connected everything is, because of cloud computing and Internet-based services. These threats include things like malware, worms, ransomware and botnets that spread quickly across networks, just like how diseases spread. These attacks can cause a lot of damage to systems, compromise sensitive information and disrupt how organisations work. The old ways of protecting against these threats are not working well. So we need ways to defend against these threats that can adapt and learn. This research is about creating defence strategies for cybersecurity threats using machine learning. We are looking at how cyber attacks spread and how we can use that information to predict and stop them. By looking at patterns of how attacks happen and how vulnerable networks are, we can train computers to find abnormal activity and predict when a big cyber threat might happen. Our approach combines machine learning with models of how cyber attacks spread to improve how we detect and respond to threats. We use machine learning techniques to look at a lot of network traffic data and security logs. This helps us tell the difference between malicious activity more accurately. We also use analytics to anticipate what attacks might look like in the future and recommend how to defend against them. We also looked at how different defence strategies work, like detecting threats early, isolating parts of the network using automated response systems and changing security policies. We used metrics like how accurate our detection is, how many false positives we get how long it takes to respond, and how efficient the system is. Our experiments show that using machine learning makes a difference in how well cyber defence systems can detect and stop cyber threats in real time. What we found out can help us create better cyber defence systems that can handle fast-spreading cyber attacks. By using machine learning and looking at how cyber attacks spread, we can create a scalable way to manage cybersecurity threats. This research shows how important it is to use data-driven security solutions to make networks more resilient and protect digital systems from new cyber threats. Cybersecurity threats are a problem and we need to use cybersecurity threat management to protect against them. Cybersecurity threats are getting worse. We need to do something about them.

Keywords: Cyber Security, Epidemic Threats, Machine Learning, Malware Propagation, Network Security, Anomaly Detection, Cyber Defence Strategies.

I. INTRODUCTION

The Internet and computers have changed a lot because of digital technologies, cloud computing and the fact that many networks are connected. These changes have made it easier for people to talk to each other share data. Make systems work better. However they have also created problems for cyber security. One of the problems is that cyber threats can spread quickly like diseases. These threats, such as malware, worms, ransomware and botnet attacks can infect systems in a short time.

Cyber attacks that spread like diseases take advantage of weaknesses in networks and software. They can move from one device to another, causing cyber problems. When a system is infected, it can send code to other connected systems, making the problem bigger. These attacks can cause a lot of damage, disrupt important services and put sensitive data at risk. Traditional cybersecurity methods, like systems that look for known threats and firewalls that follow rules, often struggle to find threats and complex attack patterns. So there is a growing need for smarter defence systems that can find and stop these threats in real time.

In recent years, machine learning has become a powerful tool for improving cybersecurity. Machine learning helps computers learn from data, find patterns that are not obvious and make good guesses about potential threats. By looking at a lot of network traffic data, system logs and user behaviour, machine learning algorithms can find anomalies. Identify bad activities more efficiently than traditional methods. These techniques can adapt to changing cyber threats without needing constant updates.

Another important idea in security is using epidemic modelling to understand how cyber threats spread. Epidemic models, which were first used to study the spread of diseases, can be used to simulate the spread of cyber attacks. Models like Susceptible-Infected-Susceptible and Susceptible-Infected-Recovered have been used to analyse how malware spreads and how different defence strategies can control the problem. By combining epidemic modelling with machine learning, researchers can develop more proactive cyber defence systems.

This study focuses on using machine learning to model and analyze cyber security threats that spread like diseases. The goal is to find patterns of cyber attack spread, analyse network weaknesses and implement machine learning based detection

systems to prevent cyber problems. The proposed approach combines machine learning algorithms with epidemic propagation models to enhance the detection, prediction and mitigation of cyber threats.

This study also looks at the effectiveness of defence strategies, such as finding threats early, monitoring for anomalies, automated response systems and adaptive security policies. The combination of machine learning and epidemic modelling provides a framework that can improve the resilience of computer networks against rapidly spreading cyber threats.

Overall, this research helps develop scalable cyber defence systems that can effectively address the challenges posed by cybersecurity threats that spread like diseases. By using machine learning techniques and epidemic-based analysis, the proposed framework aims to enhance the ability of organisations and network administrators to detect, predict and mitigate cyberattacks before they cause damage. Cybersecurity threats are a problem and cybersecurity is important to prevent these threats. Cybersecurity threats can spread quickly. Cybersecurity systems need to be able to detect and stop them.

II. LITERATURE SURVEY

The internet and computer networks are growing fast, and this has led to a big increase in cyber threats that spread like diseases. Cyber threats are a problem, and researchers are working hard to understand them and find ways to stop them. They are using models that are similar to the ones used to study the spread of diseases to understand how cyber threats spread. They are also using machine learning techniques to design defence strategies against cyber threats.

This section is about the studies that have been done on cyber threats, how malware spreads and how machine learning can be used to defend against cyberattacks.

Some researchers used models that were originally designed to study the spread of diseases to understand how malware spreads across computer networks. These models, like the Susceptible-Infected model, divide computer networks into different groups to show how malware spreads. The Susceptible-Infected-Recovered model is widely used because it can show how malware spreads and help predict cyber attacks.

Some researchers have made these models better to show how cyber threats behave in networks. For example, they have used models like the SI, SIS and SEIRS models to study how malware spreads and to test defence strategies. These models can show how malware spreads across networks and help researchers find ways to stop it. They have also come up with models like the SIIDR model to study self-spreading malware and big cyber attacks like WannaCry. These new models are more accurate than the ones.

Recently, researchers have been working on predicting cyber threats using math and random modelling techniques. For instance, they have come up with a way to predict the spread of cyber threats using the Susceptible-Infected Recovered model with random parameters. This new model helps estimate how fast malware spreads and predicts cyber attacks accurately. This helps detect and stop cyber threats early.

Cyber threats are getting more complex, so machine learning is becoming a part of cybersecurity. Machine learning helps systems learn from data, find patterns and identify unusual behaviour in networks. These techniques are widely used to detect malware, find intruders and gather threat intelligence. Studies show that machine learning algorithms like classification, clustering and anomaly detection are much better at finding activities than traditional security systems.

Researchers have also been working on combining machine learning with models that study the spread of diseases to predict how malware spreads in networks. One study came up with a model that uses Graph Convolutional Networks and representation learning to study the relationships between nodes in a network. This model can show the structure of the network. Predict how infected nodes will behave, which helps predict the spread of malware more accurately. The results show that machine learning models can find infection paths and help prevent big cyber attacks.

In addition to machine learning techniques, researchers have been using scientific machine learning approaches that combine differential equations with neural networks to study the spread of malware. These hybrid models are more accurate. Can be interpreted easily. Studies using data from past cyber attacks, like the Code Red worm outbreak, show that hybrid machine learning models can reduce prediction errors and provide insights into how malware spreads.

Another important area of research is using intelligence and deep learning to improve cyber defence mechanisms. Modern cybersecurity systems use AI techniques to detect threats, classify malware and analyse behaviour. These systems analyse a lot of network data. Automatically find unusual patterns that indicate cyber attacks. However, machine learning-based cybersecurity systems still face challenges like attacks, lack of transparency and the need for high-quality training data.

Overall, the research shows that studying the spread of diseases and machine learning are tools for understanding and stopping cyber threats. While models that study the spread of diseases provide a framework for analysing malware, machine learning techniques improve threat detection and prediction. However, most studies focus on either modelling the spread of malware or detecting threats separately. Therefore, there is a

need for frameworks that combine both approaches to develop effective and adaptive cyber defence strategies. The proposed research addresses this gap by studying cyber threats and analysing defence mechanisms using machine learning techniques to improve the detection, prediction and prevention of cyber attacks.

Cyber threats and machine learning are the focus of this research. Cyber threats are a problem, and machine learning is a crucial part of the solution. By combining cyber threats and machine learning, researchers can develop effective defence strategies against cyber attacks. Cyber threats will continue to evolve, so it is essential to stay of them by using machine learning and other techniques to predict and prevent cyber attacks. Cyber threats and machine learning are closely related. Understanding this link is key to developing effective cyber defence mechanisms.

III. ALGORITHM

The proposed algorithm focuses on detecting and mitigating epidemic cybersecurity threats using a machine learning based predictive framework. The system analyses network traffic patterns, identifies abnormal activities, and generates defensive responses to prevent large-scale cyber attacks such as malware propagation, botnets, and distributed denial-of service (DDoS) attacks.

A. ML-Based Epidemic Cyber Threat Detection and Defence

Input: Network dataset D containing traffic logs, system events, and user activity data.

Output: Detection of epidemic cyber threats and generation of defence strategies.

Step 1: Data Collection: Cybersecurity data is collected from multiple sources, including:

- Network traffic logs
- Firewall logs
- Intrusion Detection System (IDS) alerts
- System event logs
- User activity records

The collected dataset can be represented as:

$$D = \{N,S,U\} \quad (1)$$

where N represents network traffic data, S represents system log data, and U represents user activity data.

Step 2: Data Preprocessing: The collected data is pre processed to improve its quality and consistency.

- Remove duplicate and incomplete records
- Normalise network traffic data
- Handle missing values using statistical techniques
- Convert raw log files into structured datasets

Step 3: Feature Extraction: Important cybersecurity features are extracted from the dataset, such as:

- Packet transmission rate
- Source and destination IP addresses
- Network protocol types
- Number of failed login attempts
- Traffic flow behaviour
- Malware signature indicators

The extracted features are represented as:

$$F = \{f_1,f_2,f_3,\ldots,f_n\} \quad (2)$$

where f_i represents network security attributes.

Step 4: Threat Modelling: The spread of cyber attacks is modelled using an epidemic propagation model. In this model, systems in the network are categorised as:

- Susceptible (S): Systems vulnerable to attacks
- Infected (I): Compromised systems
- Recovered (R): Secured systems after mitigation

This model helps analyse how cyber threats propagate through a network.

Step 5: Machine Learning-Based Threat Detection: Machine learning algorithms such as Decision Tree, Random Forest, Support Vector Machine (SVM) and Neural Networks are applied to analyse extracted features.

$$Y = f(F) \quad (3)$$

where F represents the feature vector and Y represents the predicted threat classification.

Step 6: Threat Classification: Detected threats are classified into categories such as:

- Malware propagation attacks
- Botnet attacks
- Distributed Denial of Service (DDoS) attacks
- Phishing or intrusion attempts

Step 7: Defence Strategy Generation: Once a threat is detected, the system performs defence actions:

- Block malicious IP addresses
- Isolate infected systems from the network
- Update firewall and intrusion prevention rules
- Generate alerts for cybersecurity administrators

Step 8: Performance Evaluation: The effectiveness of the proposed system is evaluated using standard metrics.

Accuracy

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \quad (4)$$

Precision

$$Precision = \frac{TP}{TP + FP} \quad (5)$$

Recall

$$Recall = \frac{TP}{TP + FN} \quad (6)$$

F1 Score

$$F1 = 2 \times \frac{Precision \times Recall}{Precision + Recall} \quad (7)$$

where *TP*, *TN*, *FP*, and *FN* represent true positives, true negatives, false positives, and false negatives, respectively.

The proposed algorithm helps detect epidemic cyber threats at an early stage and provides automated defence mechanisms to strengthen the network security.

IV. METHODOLOGY

The proposed methodology focuses on developing a machine learning-based framework for detecting and controlling epidemic cybersecurity threats in network environments. Epidemic cyber threats such as malware propagation, botnets, worms, and distributed denial-of-service (DDoS) attacks can spread rapidly across interconnected systems. Therefore, an intelligent defence strategy is required to detect these threats at an early stage and prevent large-scale damage. The methodology integrates network data analysis, machine learning models, epidemic threat modelling, and automated defence mechanisms to improve cybersecurity protection.

A. Data Collection

The first step involves collecting cybersecurity data from various network sources. These data sources provide valuable information about network behaviour and potential security threats.

- Network traffic logs
- Firewall logs
- Intrusion Detection System (IDS) alerts
- System event logs
- User activity records

The collected dataset is represented as:

$$D = \{N, S, U\} \quad (8)$$

where *N* represents network traffic data, *S* represents system log data, and *U* represents user activity data.

B. Data Preprocessing

Raw network data often contains noise and missing values. Therefore, Preprocessing is required to improve data quality.

- Remove duplicate or incomplete records
- Handle missing values using statistical methods
- Normalise network traffic features
- Convert raw log files into structured datasets

C. Feature Extraction

Feature extraction identifies important attributes that describe network behaviour. These features help machine learning models detect abnormal activities.

$$F = \{f_1, f_2, f_3, \ldots, f_n\} \quad (9)$$

where f_i represents security-related attributes such as packet rate, protocol type, source and destination IP address, connection duration, and login attempts.

D. Epidemic Threat Modeling

To analyse how cyber threats propagate in a network, an epidemic propagation model is used. In this model, network nodes are categorised into three states:

- Susceptible (S): Systems vulnerable to attacks
- Infected (I): Systems compromised by cyber threats
- Recovered (R): Systems secured after mitigation

This model helps understand the spread of cyber attacks within a network.

E. Machine Learning-Based Threat Detection

Machine learning algorithms such as Decision Trees, Random Forest, Support Vector Machines (SVM), and Neural Networks are applied to analyse the extracted features and detect cyber threats.

$$Y = f(F) \quad (10)$$

where *F* represents the feature vector and *Y* represents the predicted classification of network activity.

F. Threat Classification

Detected threats are classified into categories such as:

- Malware propagation attacks

- Botnet attacks
- Distributed Denial of Service (DDoS) attacks
- Phishing or unauthorised intrusion attempts

G. Defense Strategy Implementation

Once a threat is detected, the system initiates defence mechanisms such as:

- Blocking malicious IP addresses
- Isolating infected systems from the network
- Updating firewall and security rules
- Generating alerts for cybersecurity administrators

H. Performance Evaluation

The performance of the proposed system is evaluated using standard metrics.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{11}$$

$$Precision = \frac{TP}{TP + FP} \tag{12}$$

$$Recall = \frac{TP}{TP + FN} \tag{13}$$

$$F1 = 2 \times \frac{Precision \times Recall}{Precision + Recall} \tag{14}$$

where *TP*, *TN*, *FP*, and *FN* represent true positives, true negatives, false positives, and false negatives, respectively.

The proposed methodology enables early detection of epidemic cyber threats and supports automated defence strategies to enhance the security and resilience of network systems.

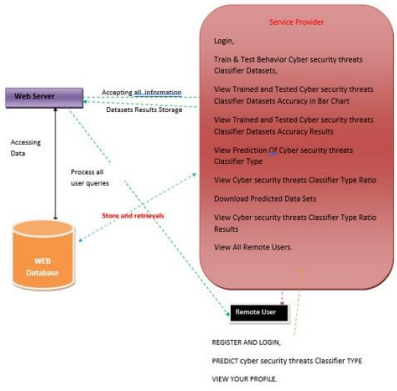

Fig. 1. Architecture Overview

V. RESULT ANALYSIS

This section presents the experimental evaluation of the proposed A machine learning-based framework for detecting and mitigating epidemics and cybersecurity threats in network environments. The objective of the analysis is to evaluate the effectiveness of the proposed defence strategy in identifying cyber threats such as malware propagation, botnets, worms, and distributed denial-of-service (DDoS) attacks.

A network security dataset containing network traffic logs, firewall logs, system event logs, and intrusion detection system (IDS) alerts was used for the experiment. The dataset includes features such as packet transmission rate, connection duration, protocol types, source and destination IP addresses, and login attempt statistics. The dataset was divided into training data (80%) and testing data (20%) to train and evaluate the machine learning models.

A. Model Performance Evaluation

Machine learning algorithms such as Decision Trees, Random Forest, Support Vector Machines (SVM) and Neural Networks are used to analyse network behaviour and detect epidemic cyber threats. These models learn patterns from historical network data and classify network traffic as either normal or malicious.

The performance of the proposed system is evaluated using standard metrics including accuracy, precision, recall, and F1-score.

B. Accuracy Analysis

Accuracy measures the proportion of correctly classified network activities among all observed events.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{15}$$

where *TP* represents true positives, *TN* represents true negatives, *FP* represents false positives, and *FN* represents false negatives.

C. Precision and Recall Analysis

Precision and recall are used to evaluate the reliability of the cyber threat detection system.

$$Precision = \frac{TP}{TP + FP} \tag{16}$$

$$Recall = \frac{TP}{TP + FN} \tag{17}$$

Precision indicates how many predicted threats are actually malicious, while recall measures the ability of the system to detect all existing cyber threats.

D. F1 Score Evaluation

The F1-score combines precision and recall into a single metric to measure the overall performance of the detection model.

$$F1 = 2 \times \frac{Precision \times Recall}{Precision + Recall} \quad (18)$$

E. Epidemic Threat Propagation Analysis

The propagation of cyberattacks in the network is analysed using an epidemic threat model. In this model, network nodes are categorised into three states:

- Susceptible (S): Systems vulnerable to cyber attacks
- Infected (I): Systems compromised by malware or attacks
- Recovered (R): Systems secured after mitigation

The analysis shows that early detection and quick response significantly reduce the number of infected systems in the network.

F. Defense Strategy Effectiveness

Once a threat is detected, the system automatically activates defence strategies such as blocking malicious IP addresses, isolating infected systems, updating firewall rules, and generating alerts for the network administrators. These actions reduce the spread of epidemic cyber threats and improve network security.

G. Overall System Performance

The experimental results demonstrate that the proposed machine learning-based defence framework effectively detects epidemic cybersecurity threats and improves overall network protection. The integration of machine learning detection with automated defence mechanisms enhances threat response time and reduces malware propagation.

Overall, the proposed system provides an efficient solution for protecting modern network infrastructures from rapidly spreading cyberattacks.

Visualization and Output:

Fig. 2. wed page

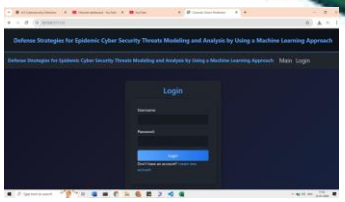

Fig. 3. login page

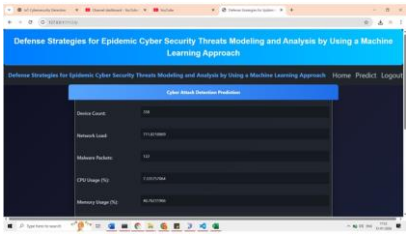

Fig. 4. Prediced value

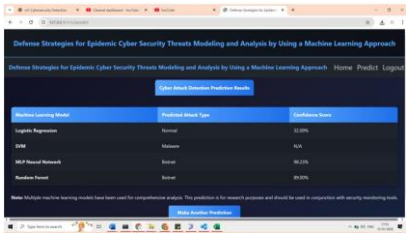

Fig. 5. Predicedion

VI. CONCLUSION

In this work, we use one of the intelligent techniques based on an artificial neural network to investigate the mathematical model that simulates Pony Stealer (malware attack) in the connection that has been developed. The mathematical model is compartmental since asymptomatic devices, as well as Exposed Susceptible, Susceptible, Infectious, and Recovered, have all been regarded as separate systems linked by a single server. Some infections can propagate through asymptomatic devices without causing symptoms. These viruses are identified through infectious devices. This extra type of device is crucial to include in cybersecurity models since many cyber attacks are intended to control the device system in an anonymous manner in order to collect personal data [68]. Such real-world processes are regulated by a set of ordinary differential equations. Deep neural learning-based machine learning techniques [69] have been applied to solve the system of ordinary differential equations underlying the epidemic model. In the ANN approach, we use one hidden layer for sample points of each equation in Matlab, and using the RK-4 approach, a reference solution is generated, which is later analysed using the Levenberg-Marquardt algorithm's training, testing, and validation procedures. Since the approximate solutions and analytical answers correspond with the lowest absolute errors

when compared to state-of-the-art techniques, the detailed graphical analysis shows that the suggested method is accurate and effective. Additionally, performance indicator values are getting closer to zero, demonstrating awless outcome modelling.

REFERENCES

[1] F. Song, Y. Lei, S. Chen, L. Fan, and Y. Liu, "Advanced evasion attacks and mitigations on practical ML-based phishing website classifiers," Int. J. Intell. Syst., vol. 36, no. 9, pp. 5210–5240, Sep. 2021.

[2] B. Sabir, M. A. Babar, and R. Gaire, "An evasion attack against ML-based phishing URL detectors," Tech. Rep., 2020.

[3] H. Shirazi, B. Bezawada, I. Ray, and C. Anderson, "Adversarial sampling attacks against phishing detection," in Proc. IFIP Annu. Conf. Data Appl. Secur. Cham, Switzerland: Springer, Jul. 2019, pp. 83–101.

[4] S. Anupam and A. K. Kar, "Phishing website detection using support vector machines and nature-inspired optimization algorithms," Telecommun. Syst., vol. 76, no. 1, pp. 17–32, Jan. 2021.

[5] A. K. Jain and B. B. Gupta, "Towards detection of phishing websites on client-side using machine learning based approach," Telecommun. Syst., vol. 68, no. 4, pp. 687–700, Aug. 2018.

[6] S. Chen, M. Xue, L. Fan, S. Hao, L. Xu, H. Zhu, and B. Li, "Automated poisoning attacks and defenses in malware detection systems: An adversarial machine learning approach," Comput. Secur., vol. 73, pp. 326–344, Mar. 2018.

[7] I. Vayansky and S. Kumar, "Phishingchallenges and solutions," Comput. Fraud Secur., vol. 2018, no. 1, pp. 15–20, Jan. 2018.

[8] Z. Abaid, M. A. Kaafar, and S. Jha, "Quantifying the impact of adversarial evasion attacks on machine learning based Android malware classifiers," in Proc. IEEE 16th Int. Symp. Netw. Comput. Appl. (NCA), Oct. 2017, pp. 1–10.

[9] I. Corona, B. Biggio, M. Contini, L. Piras, R. Corda, M. Mereu, G. Mureddu, D. Ariu, and F. Roli, "DeltaPhish: Detecting phishing webpages in compromised websites," in Proc. Eur. Symp. Res. Comput. Secur. Cham, Switzerland: Springer, Sep. 2017, pp. 370–388.