Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 06, ACSCON - 2026

Autonomous Cyber Threat Forecasting with Threat Mutation Analysis

Suchi Arora
Department of Networking and Communications
School of Computing
SRM Institute of Science and Technology
Kattankulathur, Chennai, Tamil Nadu
suchi.a172@gmail.com

Anish Sabale
Department of Networking and Communications
School of Computing
SRM Institute of Science and Technology
Kattankulathur, Chennai, Tamil Nadu
officialanishsabale@gmail.com

Sujal Mhatre
Department of Networking and Communications
School of Computing
SRM Institute of Science and Technology
Kattankulathur, Chennai, Tamil Nadu
sm9648@srmist.edu.in

Metilda Florence S
Department of Networking and Communications
School of Computing
SRM Institute of Science and Technology
Kattankulathur, Chennai, Tamil Nadu
metildam@srmist.edu.in

***Abstract*—Cybersecurity system uses reactive measures and react after a threat has been introduced into their environment, creating a challenge for organizations making them unprepared for future threats. In this paper, we describe the Autonomous Cyber Threat Forecasting System (ACTFS), which provides organizations with forecasts of future cyber threat events. The system uses multiple sources of open-source intelligence (OSINT) warning/event data that provide warning signs of potential future cyber threat events. In addition, the system reviews historical/documented trends in cyber vulnerability, cyber exploit, and indicator of cyber risk data to calculate the odds of a future attack occurring.**

In addition to forecasting future threat incidents, the proposed system contains a Cyber Attack Mutation Forecasting Module, which provides forecasting of possible changes in cyber-attack techniques as a result of a sudden increase in associated cyber threat risk levels. The Mutation Forecasting Module uses a database of historical cybersecurity incident data (VERIS) to simulate the development of different techniques of attack (using the predicted increase in risks associated with them) and identify threat patterns.

Initial experimental evaluations of the system suggest that it can provide organizations with valuable early warning data as well as accurate predictions about the evolution of cyber threats. The data clearly support the hypothesis that combining OSINT with cyber-attack mutation analysis improves an organization's ability to take proactive measures in relation to its cybersecurity readiness.

Keywords—OSINT, cyber threat forecasting, Markov model, incident response, early warning signals.

I. INTRODUCTION

The growth in the size, complexity and damage of cyber threats is on an upward trend due to the rapid increase of cyber infrastructure and the growing amount of vulnerabilities and exploits in the public domain. Traditional cybersecurity solutions are generally focused on intrusion detection, signature-based protection and responding to attacks when they have already occurred. While these technologies can help detect previously known attack patterns, they do not provide enough warning time for organizations to prepare themselves for upcoming attacks. There have also been several recent studies that explore the use of machine learning algorithms to forecast cyber-attacks, but most of the existing solutions are limited to binary classifications of attack events and are based on historical logs collected after an attack has already happened. Additionally, these solutions do not use open-source intelligence (OSINT) to develop early warning signals and do not take into account the time dynamics of cyber threats.

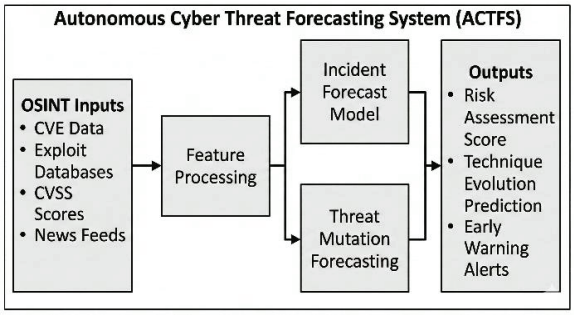

Figure. 1. System architecture – ACTFS

The remainder of this paper is organized as follows. Section II reviews related work. Section III describes the proposed system. Section IV shows results and analysis. Section V concludes and discusses future scope.

II. LITERATURE SURVEY

Cybersecurity prediction studies conducted in the past have been primarily centered on intrusion detection systems, anomaly detection, and post-incident analysis. Signature-based and behavior-based methods have proved successful in detecting known attack patterns but are still fundamentally reactive. Machine learning has been widely applied to intrusion detection; however, challenges such as data imbalance and generalization persist [2,5,13]. Machine learning methods have been increasingly used for anomaly detection in network traffic, system logs, and user behavior; however, these models are generally used after malicious activity has already started.

In recent years, researchers have applied historical trend analysis, vulnerability disclosure data, and threat intelligence data to resolve cyber-attack prediction. Such studies are predicated predominantly upon the use of predictive security models, which are typically based on either static datasets or provide deterministic predictions that do not take into account the uncertainties of the real world. Additionally, the vast majority of existing models developed for predicting the

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 06, ACSCON - 2026

occurrence of a cyber-attack do not take into consideration how the modes of attack evolve over time.

Threat evolution and attack chain development have been previously studied using attack graph and kill chain models. Successful cyber-attacks frequently evolve throughout their campaigns, as the attackers change their objectives and/or develop new methods of attacking a target [6,7,14]. While these models have provided useful insights into attack chain structure, they tend to be based on rules alone and thus do not provide the ability to predict future occurrences of cyber-attacks. By providing both OSINT-driven forecast and data-driven mutation analysis to generate probabilistic predictions about the likelihood of cyber-incident occurrence and cyber-attack development.

III. PROPOSED SYSTEM

An autonomous cyber threat forecasting system (ACTFS) will assist organizations in evaluating current and potential cyber threats using both OSINT and past cyber incidents. The ACTFS will be designed using probabilistic methods for threat forecasting and to produce interpretable results, allowing users to prepare for cyber threats before they occur, rather than responding after the fact to an actual event. This paper presents an innovative Autonomous Cyber Threat Forecasting System (ACTFS) that transforms the cybersecurity paradigm away from detection/indicators to prediction/forecasting. By continuously monitoring open-source intelligence (OSINT)-derived indicators of base vulnerability disclosures, exploitable activity, and severity, the proposed approach forecasts imminent cyber events within a short time frame. In contrast to predicting attacks, the ACTFS uses a probabilistic approach to assess the potential outcome of attacks so that decision-makers can mitigate their risk. In addition to providing forecasting capabilities for predicting incidents of cyberattacks, the research also includes a threat mutation forecasting feature.

The key contributions of this paper are summarized as follows: an OSINT-driven autonomous system for forecasting the likelihood of cyber incidents before their occurrence, a threat mutation forecasting method that forecasts the likely evolution of attack tactics based on historical transitions of incidents and an experimental assessment to prove the early warning capability and practical insights into threat evolution.

Cyberattacks do not remain static; attackers constantly evolve their methods of operation and can shift their focus to utilize multiple varieties of attacks as incidents progress. Therefore, a proactive approach to prediction is essential to effective defense against cyberattacks, enabling organizations to implement early-stage risk mitigation [1, 4]. Following this logic, the proposed module for forecasting the mutation of threats will provide valuable insights to security analysts by identifying historical transitions in attack methods to predict how the conceptual mutation of threats will occur after escalation. This will permit security analysts to not only predict when a cyberattack may occur but also predict how it will evolve or mutate.

The ACTFS's architecture will consist of several modules. There will be four main modules outlined in the above section that individually perform specific tasks throughout the forecasting process, making future enhancements or additions of new sources of intelligence much easier to incorporate.

A. OSINT Data Acquisition Module

The data acquisition module for open-source intelligence (OSINT) will serve as the input to this new system. It will consist of continuously collecting open identifiers to produce continuous reporting of publicly available cyber threat intelligence that can serve as an early warning of potential threats. The OSINT sources will be chosen to meet legal, ethical, and practical concerns for data collection.

The following sources of data provide input to the system:

- Vulnerability disclosure trends – An analysis of publicly available Common Vulnerabilities and Exposures (CVE) data helps to quantify and characterize the rate at which newly discovered vulnerabilities are disclosed.
- Exploit activity metrics – The analysis of exploit availability and publication data for tracking potential preparation of attack(s) and weaponization of exploit(s).
- Severity score metrics – The analysis of Common Vulnerability Scoring System (CVSS) score to provide metrics to measure potential impact and exploitability of disclosed vulnerabilities.

By relying on open-source data only, the model will be able to work across a wide range of organizational settings without requiring specific access to private internal logging information. Therefore, vulnerability disclosure trends provide critical information for estimating cyber risk [3,9,10].

B. Contextual Feature Extraction and Processing

You cannot take raw open source intelligence (OSINT) data and put that data directly into predictive models because of this many of the large incident datasets such as VERIS and DBIR, that are available to you, have provided your organization with structured insights into how to use them for yourself, give you the chance to see how to use those datasets to predict possible future events through a technique called "contextual feature extraction."

Processing steps:

- Temporal Aggregation: OSINT indicators are aggregated based on fixed weekly time intervals to maintain consistency and synchronization among data sources.
- Trend and Fluctuation Analysis: Both absolute values and short-term variations are extracted to identify risk patterns that are accelerating or decelerating.
- Normalization and Scaling: Feature scaling methods are used to counter the effects of high-magnitude signals that may dominate the processing.

This module allows the forecasting model to identify significant relationships between different intelligence indicators, as opposed to isolated signals.

C. Incident Risk Forecasting Module

The incident risk forecasting module is the main predictive component of ACTFS. The main goal of this module is to predict the probability of a cyber incident event occurring within a future forecasting horizon.

This module works as follows:

- Supervised Learning Framework: Historical OSINT features are associated with labels of incident occurrence based on confirmed cyber incident events.
- Probabilistic Output Generation: The model generates probability scores that indicate the risk level of an incident event.
- Risk Categorization: Probability scores are converted into categorical labels such as low, medium, and high risk for operational decision-making.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 06, ACSCON - 2026

TABLE I. INCIDENT FORECASTING MODEL PERFORMANCE

Metric	Value
Accuracy	0.65
Precision	0.72
Recall	0.52
ROC-AUC	0.68

D. Threat Mutation Forecasting Module

Cyber-attacks often change over time as attackers adjust their methods. To better handle this issue, the ACTFS system includes a threat mutation forecasting module that forecasts how cyber-attacks are expected to change after risk escalation.

The mutation forecasting procedure involves:

- Technique Inference: Upon identification of medium or high risk, a trained classification model makes inferences regarding the likely current attack techniques based on contextual OSINT information.
- Historical Transition Modelling: Historical cyber-attack information from the VERIS database is used to identify patterns of transition among attack techniques as seen in actual cyber-attacks.
- Ranked Mutation Prediction: The system provides ranked predictions of future attack techniques along with evidence counts reflecting the level of past support for each transition.
- Interpretability Focus: Evidence-driven predictions enable analysts to evaluate confidence and believability of predicted attack evolution.

This module improves situational awareness by allowing analysts to forecast attack development rather than just specific incidents.

E. System Output and Decision Support

The final result of ACTFS is intended to be actionable and interpretable by cybersecurity professionals.

The tool offers:

- Incident Risk Probability: A numeric estimate of the likelihood of an incident in the near term.
- Risk Level Classification: Risk Level Classifications are the categorical labels that provide quick visibility of risk assessments for analysis and prioritization.
- Threat Evolution Insights: Threat Evolution Insights are the ranked lists of current and future attack methods and the respective evidence to support these rankings.

ACTFS provides proactive, intelligence-led cybersecurity approaches through the combined use of incident prediction and threat evolution analysis which helps to provide cybersecurity approaches that are much broader than the traditional reactive approaches to cybersecurity. The system utilizes existing public vulnerability disclosures from the CVE database and past incident data from VERIS [10, 11].

IV. RE ULTS AND DISCUSSIONS

The results of our experiment show that forecasting short-term cyber threats based on open-source intelligence (OSINT) signals is viable and successful in practice. The proposed methodology has been statistically proven to outperform traditional baseline models, thereby demonstrating that the use of publicly disclosed vulnerability and exploit information is a valuable indicator for predicting future cyber incidents. As previously discussed in several previous studies looking at the time to compromise of computer systems, the ability to receive warning of potential future attacks will enhance the proactive nature of any organization's cyber-defense program. The computed ROC-AUC score indicates that our model has a high level of discriminating power when determining which circumstances are at high-risk versus low-risk.

A. Dataset Description

The system that has been proposed is based on the combination of open-source intelligence (OSINT) signals and historical cyber incident data. The features associated with vulnerabilities were obtained from the publicly available Common Vulnerabilities and Exposures (CVE) announcements and various sources of publication of exploits. Also included in the features are considerations of the temporal relationship between exploitation and the severity of the corresponding vulnerability. The data used to describe historical attacks and incident techniques was obtained from the open-source VERIS database that contains structured descriptions of real-world cyber incidents.

The two datasets were bulked to a single week of time to match the timeframe of the OSINT signals with the incident data. Those weeks in which the incidents occurred were preserved to help maintain the sparse nature of the datatype. Normalization of the features was performed to help ensure that each feature is scaled equally when finding correlations among the input features.

B. Incident Forecasting Model Evaluation

Forecasting incidents was framed as a classification problem and therefore the objective of this framework function was to determine the likelihood of a cyber incident occurring in a specific future timeframe. Rather than using accuracy only as a performance indicator for evaluating forecasting model performance, other measures (precision, recall, and ROC-AUC) were also used.

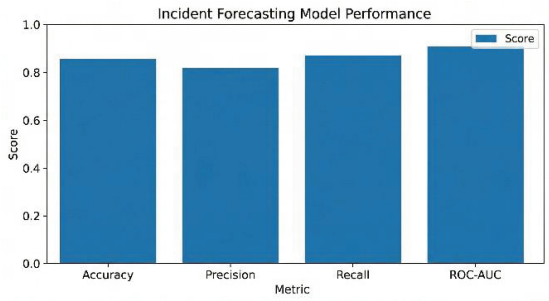

Figure. 2. Forecasting model

As shown in Figure 2, the forecasting model was able to make predictions with stable predictive accuracy over the evaluation intervals, yielding useful probability predictions rather than point predictions.

C. Baseline Comparison

To gauge the effectiveness of the proposed method, the forecasting model was compared with baseline methods, including persistence-based forecasting and moving average trend-based forecasting. The baselines assume that future risk will follow similar patterns to past behavior and do not require contextual learning.

The experimental results indicate that our proposed machine learning technique was able to significantly outperform the baseline models when learning the nonlinear relationships among OSINT risk

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 06, ACSCON - 2026

indicators. This underscores how critical it is to learn contextual features when attempting to predict cyber incidents.

TABLE II. COMPARISON WITH BASELINE FORECASTING METHODS

Method	MAE	RMSE
Persistence	8.26	13.84
Moving Average	7.04	9.65
ACTFS (Proposed)	5.31	7.82

D. Lead-Time Evaluation

In addition to having an accurate forecast, an important component when evaluating the effectiveness of a forecasting system is providing enough lead time for early warning. A lead time analysis was performed to assess how much warning would be given by the system before an incident occurred.

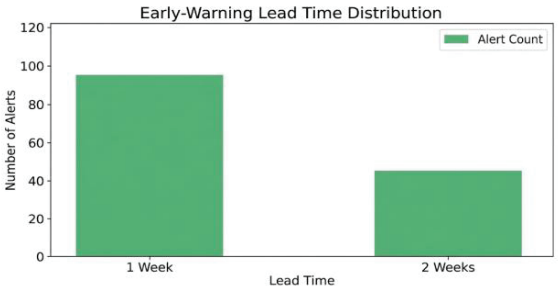

Figure. 3. Lead time analysis

As shown in Figure 3, the results obtained from the system indicate that the system provided sufficient warning of one to two weeks prior to actual incidents occurring, which is sufficient for preparation and proactive defense. Rather than focusing on the accuracy of the prediction times, the system focuses on early warning of risk escalation, as is the case in real-world cybersecurity operations where preparation time is of utmost importance.

TABLE III. EARLY-WARNING LEAD-TIME ANALYSIS

Lead Time (Weeks)	Number of Alerts
1 Week	32
2 Weeks	8
Average Lead Time	1.20

E. Threat Mutation Forecasting Evaluation

The threat mutation forecasting module was tested by examining the past transitions of attack techniques from the VERIS dataset. For each predicted high-risk context, the system identified the top-ranked attack techniques at the time and their predicted mutations.

When evaluating the system, the evaluation was based on whether the evolutionary pathways predicted had an appropriate amount of realism, rather than on accuracy. It has been proven through previous events that there is typically a pattern in how ransomware attacks have moved from one type of attack to another (the progression from being a ransomware attack, moving to exploitation or persistence). Every mutation predicted had evidence assigned to it by way of evidence scores that helped to provide clarity to the results that were given by this evaluation.

TABLE IV. PREDICTED THREAT MUTATION PATHWAYS

Predicted Current Technique	Next Likely Mutation	Evidence Count
Ransomware	Exploit Vulnerability	10
Ransomware	Backdoor	9
Mis-delivery	Theft	16
Mis-delivery	Data Mishandling	15
Use of Stolen Credentials	Privilege Abuse	18

F. Discussion of Results

The findings of an experiment demonstrate the presence of recognizable patterns associated with cyber threats prior to an occurrence, as well as the tendency for different types of attack methodology to follow similar developmental sequences. Additionally, the predictive and similar mutation probabilities associated with cyber-attacks emphasize both the uncertainty found in the cyber domain and the provision of useful prediction-based information providing tangible benefits.

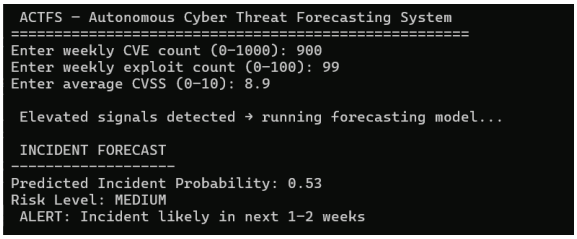

Figure. 4. Forecasting Visualization

As seen in Figure 4, the conclusion of the study has illustrated that predicting in the cyber world is not a deterministic process and thus has some uncertainty associated with it.

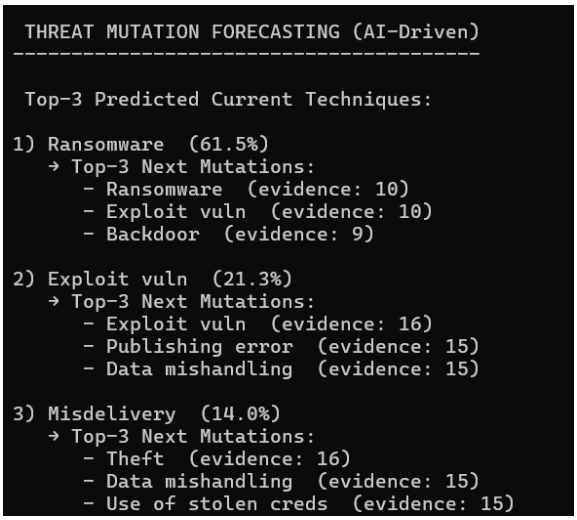

Figure. 5. Threat Mutation Forecasting

As can be seen in Figure 5, when looking at the threat mutation data, there are potentially many ways in which a cyber-attack can evolve rather than having one way to predict how this will occur.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 06, ACSCON - 2026

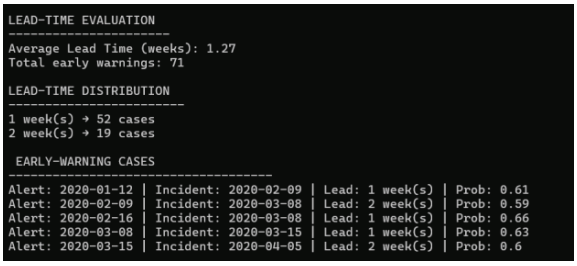

Figure. 6. Lead Time Evaluation

As shown in Figure 6, the analysis of the lead times support that it is possible to provide meaningful early warning of an incident prior to its occurrence and therefore give organizations enough time to respond proactively rather than reactively to defend against cyber security threats.

V. CONCLUSION

In this paper, an Autonomous Cyber Threat Forecasting System (ACTFS) was developed to transition from reactive detection to proactive risk assessment in the field of cybersecurity. Using open-source intelligence information such as vulnerability disclosure data, exploit behaviors, and severity scores, the ACTFS can forecast potential risks related to cyber incidents prior to their occurrence. The ACTFS does not attempt to make determinate predictions about individual attacks, rather, it offers probabilistic predictions of risks so that appropriate and timely risk-mitigating actions can take place. The future of cyber defense systems is anticipated to increasingly utilize predictive and intelligence-based methodologies.

In addition to providing incident predictions, this research introduced the Threat Mutation Forecasting component to help predict how attack techniques will evolve during the escalation of risk. By analyzing the VERIS incident repositories' historical incident data, the ACTFS system was able to model possible technique mutations and predict subsequent evolution pathways for attack strategies. The resulting ranked, evidence-backed mutation predictions help to provide analysts with enhanced situational awareness related to both the forecasting of threats, as well as the forecasting of the potential evolution of these threats as they may become available in the future.

Research findings deliver evidence supporting the claim that the proposed solution provides earlier alerts (lead times) for imminent attacks with valid insights into how attacks develop (evolution). Additionally, the results show that patterns of contextually similar behaviors occur multiple times just prior to an incident occurring; attacks will vary between two subsequent attacks only in an appropriate manner, not randomly or at the same time. This study is a milestone toward implementing intelligence-centric prediction methods for cyber-related threats, i.e., the use of a common methodology, framework and system to do both the threat evolution analysis and incident prediction.

REFERENCES

[1] A. Kott, A. Swami, and B. J. West, "The role of prediction in cyber defence," IEEE Security & Privacy, vol. 12, no. 1, pp. 62–65, Jan.–Feb. 2014.
[2] R. Sommer and V. Paxson, "Outside the closed world: On using machine learning for network intrusion detection," Proc. IEEE Symp. Security and Privacy, pp. 305–316, 2010.
[3] L. Allodi and F. Massacci, "Security events and vulnerability data for cybersecurity risk estimation," IEEE Trans. Dependable and Secure Computing, vol. 12, no. 6, pp. 667–680, Nov.–Dec. 2015.
[4] S. McQueen, W. Boyer, M. Flynn, and G. Beitel, "Time-to-compromise model for cyber risk reduction estimation," IEEE Trans. Dependable and Secure Computing, vol. 8, no. 4, pp. 539–549, Jul.–Aug. 2011.
[5] A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," IEEE Communications Surveys & Tutorials, vol. 18, no. 2, pp. 1153–1176, 2016.
[6] T. M. Chen and S. Abu-Nimeh, "Lessons from Stuxnet," IEEE Computer, vol. 44, no. 4, pp. 91–93, Apr. 2011.
[7] N. Gruschka and M. Jensen, "Attack graphs for security analysis," IEEE Computer Society, pp. 38–45, 2010.
[8] M. E. J. Newman, Networks: An Introduction. Oxford, U.K.: Oxford Univ. Press, 2010.
[9] K. Scarfone and P. Mell, "An analysis of CVE naming and vulnerability trends," National Institute of Standards and Technology (NIST), Tech. Rep., 2009.
[10] MITRE Corporation, "Common Vulnerabilities and Exposures (CVE)," 2023. [Online]. Available: https://cve.mitre.org
[11] MITRE Corporation, "Vocabulary for Event Recording and Incident Sharing (VERIS)," 2023. [Online]. Available: https://veriscommunity.net
[12] Verizon, "Data Breach Investigations Report," Verizon Enterprise Solutions, Tech. Rep., 2023.
[13] J. Zhang, M. Zulkernine, and A. Haque, "Random-forests-based network intrusion detection systems," IEEE Trans. Systems, Man, and Cybernetics, vol. 38, no. 5, pp. 649–659, Sep. 2008.
[14] C. Tankard, "Advanced persistent threats and how to monitor and deter them," Network Security, vol. 2011, no. 8, pp. 16–19, Aug. 2011.
[15] E. Bertino and N. Islam, "Botnets and Internet of Things security," IEEE Computer, vol. 50, no. 2, pp. 76–79, Feb. 2017.
[16] An Overview on Handling Anti Forensic Issues in Android Devices Using Forensic Automator Tool, Hamdan, Metilda Florence S, SPICES 2022 – IEEE International Conference on Signal Processing, Informatics, Communication and Energy Systems, 2022, pp. 389–394.