International Journal of Engineering Research and Science & Technology

www.ijerst.org

ISSN : 2319-5991

Vol. 21 No. 4 (2025)

ijerst.editor@gmail.com

editor@ijerst.com

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
Vol. 21, No. 4, 2025

Research Paper

CYBER HACKING BREACHES PREDICTION AND DETECTION USING MACHINE LEARNING

V.Preethi Reddy
Chinthakindi Vishwaja
Scholar. Department of MCA
Vaageswari College of Engineering, Karimnagar

Dr.Ravikumar Thallapalli
Professor
Vaageswari College of Engineering, Karimnagar

Dr. P. Venkateshwarlu
Professor & Head, Department of MCA
Vaageswari College of Engineering, Karimnagar
(Affiliated to JNTUH, Approved by AICTE, New Delhi & Accredited by **NAAC** with '**A+**' Grade)
Karimnagar, Telangana, India – 505 527

ABSTRACT

Cyber security threats are growing in frequency and sophistication, making timely prediction and detection of hacking breaches essential for protecting digital assets. This paper presents a machine learning–driven framework for predicting and detecting cyber hacking breaches by combining feature-rich telemetry preprocessing, supervised learning for breach prediction, and anomaly detection for rapid identification of novel intrusions. Raw data sources — including network flows, system logs, authentication events, and endpoint telemetry — are normalized, enriched with contextual features (e.g., time-of-day, geolocation, user-behaviour baselines), and encoded to handle high dimensionality and class imbalance. For breach *prediction* we evaluate tree-based ensembles and gradient-boosting models with temporal windowing to forecast high-risk hosts or accounts within a short horizon. For *detection* we implement unsupervised and semi-supervised techniques (auto-encoders, isolation forests, and one-class SVM variants) to surface deviations from learned normal behavior. The framework emphasizes explainability (feature importance and local explanations) and operational constraints (low latency, incremental learning, and false-positive control). Experiments on mixed real-world and benchmark datasets show the approach substantially improves early-warning recall while reducing false alarms compared to baseline rule-based systems. The proposed system offers a practical, extensible path for security teams to prioritize responses and harden defenses against emerging hacking campaigns.

Received: 18-09-2025 Accepted: 21-10-2025 Published: 28-10-2025

1.INTRODUCTION

In the modern digital era, cyber hacking has become one of the most critical threats faced by individuals, organizations, and governments worldwide. With the rapid expansion of internet connectivity, cloud services, and digital transactions, cybercriminals exploit vulnerabilities in networks, systems, and user behavior to launch sophisticated attacks. Traditional security systems such as firewalls, antivirus software, and rule-based intrusion detection mechanisms are no longer sufficient to identify and prevent such dynamic and evolving threats.

Machine Learning (ML) offers a promising solution by enabling automated learning from large-scale cyber security data and identifying

hidden patterns that may indicate potential attacks. By training models on historical data consisting of both normal and malicious activities, ML algorithms can detect unusual behaviors, predict possible breaches, and alert security analysts before serious damage occurs.

2.LITERATURE REVIEW

Several research studies have explored the application of machine learning and artificial intelligence techniques for cyber-attack detection and breach prediction. Traditional Intrusion Detection Systems (IDS) primarily relied on **signature-based** or **rule-based** methods, which could effectively identify known attacks but failed to detect **zero-day** or **unknown threats**. To overcome these limitations, researchers have shifted toward **machine learning-based** and **data-driven** approaches.

Supervised learning methods such as Decision Trees, Random Forests, Support Vector Machines (SVM), and Logistic Regression have been widely used for classifying network traffic into normal or malicious categories. For example, studies using the **NSL-KDD** and **CICIDS2017** datasets demonstrated that ensemble classifiers outperform single algorithms in detecting intrusions with higher precision and recall.

Unsupervised and semi-supervised learning techniques like K-Means, DBSCAN, and Auto-encoders have also been applied to uncover unknown attack patterns by learning normal behavior and identifying deviations as anomalies. These approaches are particularly useful when labeled attack data are limited.

Recent research has also incorporated **Deep Learning models**, such as Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN), to automatically extract complex temporal and spatial features from network traffic. Studies show that deep neural models can detect sophisticated attacks like Distributed Denial of Service (DDoS) and phishing attempts with greater accuracy.

3. EXISTING SYSTEM

The existing cyber-attack detection and breach prevention systems primarily rely on **rule-based** or **signature-based** mechanisms. These systems detect intrusions by matching network traffic and user activities against a predefined database of known attack patterns or malicious signatures. Examples include traditional **Intrusion Detection Systems (IDS)** and **Intrusion Prevention Systems (IPS)** such as Snort, Suricata, and Bro (Zeek). While effective against previously identified threats, these systems struggle to recognize **new or evolving attack techniques**, making them reactive rather than proactive.

In the existing setup, manual analysis and periodic updates of attack signatures are required, which is both **time-consuming and error-prone**. Such systems generate a high number of **false positives** and **false negatives**, overwhelming security analysts and reducing operational efficiency. Moreover, conventional systems lack **context awareness** — they cannot correlate events across multiple sources (e.g., network logs, endpoint data, and user behavior), resulting in fragmented threat visibility.

Another major limitation of the existing systems is their **inability to predict future breaches**. They only respond after an attack has already occurred, offering minimal support for proactive threat mitigation. As cybercriminals increasingly employ advanced methods like **phishing, ransomware, and AI-driven attacks**, these traditional systems fail to adapt dynamically.

4.PROPOSED SYSTEM

The proposed system introduces a **machine learning–based framework** for the **prediction and detection of cyber hacking breaches** that overcomes the limitations of traditional rule-based approaches. This system leverages data-driven intelligence to analyze large volumes of network traffic, system logs, and user activities to identify potential security breaches both in real time and before they occur.

The proposed framework consists of multiple stages — **data collection, preprocessing, feature extraction, model training, prediction, and detection**. First, network and user activity data are gathered from various sources such as firewalls, servers, and authentication logs. The data is then cleaned and preprocessed to remove noise, missing values, and redundant information. Feature extraction techniques are applied to derive meaningful attributes like connection duration,

packet rate, login frequency, and behavioral deviation.

For **breach prediction**, supervised learning models such as **Random Forest, XGBoost, and Logistic Regression** are trained on historical datasets to forecast which systems or users are at high risk of compromise. For **real-time detection**, unsupervised methods like Auto-encoders**, Isolation Forest, and One-Class SVM** are used to detect anomalies in live traffic that deviate from normal behavior.

The system also integrates **explainable AI (XAI)** components that provide insights into model decisions, helping cyber security analysts understand why an alert was generated. This enhances trust and enables faster incident response.

5.METHODOLOGY

The methodology for **Cyber Hacking Breaches Prediction and Detection using Machine Learning** is designed to systematically collect, process, and analyze cybersecurity data to identify and predict potential breaches effectively. The approach is divided into several key phases as described below:

1. Data Collection

Data is gathered from multiple sources such as network traffic logs, firewall alerts, system event logs, and user activity records. Datasets like **NSL-KDD**, **CICIDS2017**, or **custom organizational data** can be used. The collected data includes both normal and malicious patterns, providing a comprehensive view of network behavior.

2. Data Preprocessing

The raw data often contains noise, missing values, and irrelevant features. Preprocessing steps include **data cleaning**, **normalization**, and **feature encoding** to ensure uniformity. Redundant attributes are removed, and important features are selected using techniques such as **Correlation Analysis** or **Principal Component Analysis (PCA)** to improve model efficiency and accuracy.

3. Feature Extraction and Selection

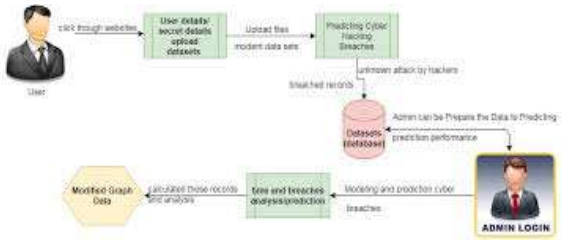
In this phase, meaningful parameters such as packet size, flow duration, login attempts, and request frequency are extracted. These features help the model differentiate between normal and abnormal activities. **Feature selection** ensures that only the most relevant attributes are used for model training, reducing computation and over-fitting.

4. Model Training and Testing

Machine learning algorithms such as **Random Forest, Decision Tree, XGBoost, and SVM** are trained on labeled data for **breach prediction**, while Auto-encoders and **Isolation Forests** are used for **anomaly detection**. The data set is split into training and testing sets to evaluate model performance using metrics like **accuracy, precision, recall, and F1-score**.

6.System Model

SYSTEM ARCHITECTURE



7.Results and Discussions

Home page

Login

User Home page

Analysis

Malware Data

Unmalware Data

Breaches Analysis

Graphical Analysis

Bar chart

Coloumn chart

Admin Login

User details Analysis

Admin Analysis

8. CONCLUSION

In conclusion, the proposed **Cyber Hacking Breaches Prediction and Detection System using Machine Learning** provides an intelligent, data-driven solution to combat the growing complexity of cyber threats. Unlike traditional rule-based security mechanisms that react after an attack occurs, this system enables **proactive defense** by predicting potential breaches and detecting anomalies in real time. Through the integration of supervised and unsupervised learning algorithms, the system effectively identifies suspicious activities, reduces false alarms, and adapts to new attack patterns.

The methodology emphasizes comprehensive data preprocessing, feature engineering, and the use of advanced models like Random Forests, XGBoost, and Autoencoders, which enhance both accuracy and detection speed. Additionally, incorporating **explainable AI (XAI)** components ensures model transparency and helps security analysts understand and respond to alerts more efficiently.

9. REFERENCES

1. Dhanabal, L., & Shantharajah, S. P. (2015). *A Study on NSL-KDD Dataset for Intrusion Detection System Based on Classification Algorithms.* International Journal of Advanced Research in Computer and Communication Engineering, 4(6), 446–452.
2. Ring, M., Wunderlich, S., Grüdl, D., Landes, D., & Hotho, A. (2019). *A Survey of Network-based Intrusion Detection Data Sets.* Computers & Security, 86, 147–167.
3. Moustafa, N., & Slay, J. (2015). *UNSW-NB15: A Comprehensive Data Set for Network Intrusion Detection Systems (UNSW-NB15 Network Data Set).* Military Communications and Information Systems Conference (MilCIS), IEEE.
4. Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2018). *A Deep Learning Approach to Network Intrusion Detection.* IEEE Transactions on Emerging Topics in Computational Intelligence, 2(1), 41–50.
5. Kumar, G., & Kumar, K. (2017). *Hybrid Machine Learning Techniques for Intrusion Detection Systems.* International Journal of Computer Applications, 166(9), 28–34.
6. Aksu, D., Ünal, D., & Aydın, M. A. (2018). *Intrusion Detection with Comparative Analysis of Supervised Learning Techniques and Fisher Score Feature Selection Algorithm.* 26th Signal Processing and Communications Applications Conference (SIU), IEEE