Smart Detection and Prevention of Cloud Based Security Threats Using Machine Learning

Parumanchala Bhaskar, Somisetty Akhil, R. S. Venkhatesh, Shaik Sajid,
M. Prem Kumar and S. Mansoor Basha
Department of Computer Science and Engineering, Santhiram Engineering College, Nandyal, Andhra Pradesh, India

Keywords: Privilege Escalation, Insider Attack, Machine Learning, Random Forest, Adaboost, XGBoost, LightGBM, Classification.

Abstract: This task utilizes advanced machine learning to enhance cloud protection, specifically addressing and mitigating privilege escalation attacks for a greater resilient protection mechanism. With the growth in cloud adoption, the threat of privilege escalation attacks also escalates. This assignment goals holes in employee get admission to privileges in cloud services to improve usual protection. The task makes use of machine learning to facilitate actual-time identification and prevention of privilege escalation attacks. Strategies like as LightGBM, Random forest, Adaboost, and Xgboost provide a sturdy protection in opposition to rising threats. Individuals and establishments come upon stronger records protection, cultivating self-assurance in cloud computing. Cloud service vendors and corporations accumulate guarantee in a comfortable online ecosystem, reaping the advantages of the task's security upgrades. A vote casting Classifier, integrating predictions from decision Tree, Random forest, and support Vector machine through a "tender" vote casting method, improves the system's efficacy in figuring out and countering privilege escalation attacks. A person-friendly Flask framework with SQLite integration enhances user trying out by way of offering secure signup and signin functionalities for realistic installation and evaluation.

1 INTRODUCTION

Cloud computing represents a progressive paradigm for delivering and facilitating offerings through the internet. The present infrastructure. Cloud storage organizations put into effect essential security protocols for their structures and the facts they manage, encompassing encryption, get entry to control, and authentication. The cloud gives nearly infinite ability for storing numerous varieties of data throughout diverse data storage architectures, contingent upon accessibility, velocity, and frequency of statistics retrieval. Data breaches involving sensitive facts may additionally get up from the big flow of facts between organisations and cloud carrier vendors, whether unintended or intentional. Parumanchala Bhaskar, et al., The attributes that facilitate consumer-friendliness in online services for employees and IT structures simultaneously complicate efforts for companies for preventing unauthorized access. The Authentication and open interfaces constitute rising protection issues that agencies come across with cloud services. Notably professional hackers employ their information to infiltrate Cloud infrastructure. Parumanchala Bhaskar, et al. 2022; Mahammad, Farooq Sunar, et al. 2024, Machine learning to know utilizes numerous methodologies and algorithms to address security challenges and decorate data control. Numerous datasets are confidential and can't be disclosed due to privacy issues, or they will lack essential statistical characteristics.

The rapid expansion of the Cloud area engenders privacy and protection threats regulated via rules. Worker access privileges may additionally remain unchanged as they transition to different jobs or positions inside the Cloud agency. Consequently, obsolete privileges are exploited detrimentally to suitable and harm precious data. Every account that interacts with a computer possesses a positive diploma of authority. Server databases, sensitive statistics, and additional services are regularly restrained to authorized customers. An adverse attacker can infiltrate a touchy system by seizing

Bhaskar, P., Akhil, S., Venkhatesh, R. S., Sajid, S., Kumar, M. P. and Basha, S. M.
Smart Detection and Prevention of Cloud Based Security Threats Using Machine Learning.
DOI: 10.5220/0013871500004919

In *Proceedings of the 1st International Conference on Research and Development in Information, Communication, and Computing Technologies (ICRDICCT'25 2025) - Volume 1*, pages 696-704
ISBN: 978-989-758-777-1

manipulate of a privileged user account and leveraging or augmenting privileges. According to Parumanchala Bhaskar, et al, 2024 their desires, attackers may additionally maneuver horizontally to advantage manage over extra structures or vertically to reap administrative and root get entry to until they achieve complete manipulate over the complete surroundings. Horizontal privilege escalation occurs while a person acquires the access permissions of another person owning the equal get entry to stage. A culprit may additionally appoint horizontal privilege escalation to reap information that isn't always inherently associated with them. An attacker can also make the most vulnerabilities in a poorly built web application to get entry to the personal data of others. The attacker has successfully completed a horizontal privilege escalation make the most, permitting them to view, adjust, and duplicate sensitive records.

Adversaries focus on facts repositories due to their possession of the maximum valuable and touchy facts. The privacy and security of each cloud user are compromised if data is misplaced. Insider threats are unfavourable activities performed by people with authorized get admission to. Because of the rapid growth of networks, numerous corporations and groups have advanced own internal networks. Latest estimates imply that 90% of corporations perceive themselves as prone to insider threats. Malefactors can make the most privilege escalation to create supplementary assault vectors on a target system. Insider attackers searching for to attain accelerated privileges or get right of entry to more touchy systems via privilege escalation tries. Insider attacks are difficult to stumble on and thwart because of their operation below company-level safety protocols and often possess privileged get entry to the network. Identifying and categorizing insider threats has come to be hard and labor-in depth.

Latest research focused at the detection and class of privileged elevation attacks perpetrated by insider people. They advised numerous machines getting to know and deep learning methodologies to address those problems. Latest studies employed strategies consisting of "SVM, Naïve Bayes, CNN, Linear Regression, PCA, Random forest, and KNN". The requirement for speedy and efficient machine learning algorithms is greatly esteemed because to the form of assault types. Therefore, a robust and efficient approach is vital to discover, categorize, and alleviate those insider threats. mareswara Kumar, 2024, To enhance protection protection systems, it is essential to hire wise algorithms, which include machine learning algorithms, for the class and prediction of insider attacks.

Moreover, know-how the efficacy of machine learning algorithms in categorizing insider assaults enables the choice of the most appropriate algorithm for every state of affairs, necessitating enhancements to the algorithms themselves. This permits the supply of more suitable security features. This study seeks to enforce powerful and efficient machine learning algorithms in insider attack conditions to get advanced and expedited consequences. Machine learning methods were implemented and assessed in this context: "Random forest area, AdaBoost, XGBoost, and LightGBM". The boosting strategy's approach involves improving a weak classifier to seriously improve its performance through augmenting the classification set of rules's predictions. "Random forest, AdaBoost, and XGBoost" efficaciously and correctly categorized insider threats.

2 LITERATURE REVIEW

Cloud computing refers to the on-call for accessibility of computing infrastructure resources. Particularly the capacity for information storage and management, without direct, exclusive oversight by means of the user. It has offered clients each public and personal computing and data garage on a unified platform via the net. In addition, it encounters severa safety risks and challenges which can impede the adoption of cloud computing answers. Suman, Jami Venkata, et al. 2024 This paper discusses the safety troubles, challenges, methods, and solutions associated with cloud computing. a multitude of individuals expressed safety apprehensions in a prior poll. Every other survey examines the cloud computing architecture approach, with several detailing protection worries and methodologies. This text consolidates all safety issues, challenges, methodologies, and answers in a single vicinity.

Cloud computing denotes the instantaneous accessibility of private computer system sources, specifically statistics storage and processing capabilities, impartial of the client's intervention. Emails are often applied for the transmission and reception of statistics amongst individuals or businesses. Financial facts, credit reviews, and other touchy facts are often transmitted over the internet. Phishing is a fraudulent method employed to obtain touchy statistics from people via masquerading as professional sources. The sender can manipulate you into divulging exclusive data via deception in a phishing email. The primary difficulty is email phishing assaults at some stage in the transmission and reception of emails. The assailant transmits spam content by means of e mail and acquires your facts upon your commencing and reading of the email. In current years, it has posed a good-sized undertaking for all. This study employs varying quantities of legitimate and phishing datasets, identifies clean emails, and utilizes numerous attributes and algorithms for categorization. A revised dataset is generated next to comparing the contemporary methodologies. Mahammad, et al. 2020; Sharmila, et al. 2022, We generated a characteristic-extracted "comma-separated values (CSV)" record and a label report, then implemented the "support vector machine (SVM), Parumanchala Bhaskar, et al. 2024; D. C. Le, et al., 2020, Naive Bayes (NB), and long short-term memory (LSTM)" algorithms. This test regards the identification of a phished email as a category trouble. The comparison and implementation imply that "SVM, NB, and LSTM "exhibit advanced performance and accuracy in detecting e-mail phishing assaults. E-mail attack class using "SVM, NB, and LSTM" classifiers attained most accuracies of ninety-nine. Sixty-two%, 97%, and ninety-eight%, respectively.

With trends in technological know-how and generation, cloud computing represents the approaching huge development inside the industry. Cloud cryptography is a way that use encryption techniques to guard information. The primary benefit of cloud storage is its accessibility, decreased hardware requirements, decrease upkeep, and protection prices, main to widespread adoption through corporations. Encryption is the technique of encoding information to inhibit unauthorized get admission to. Currently, we aim to guard the data stored on our computer systems or transferred through the net from assaults. 4 The cryptography method relies on response pace, confidentiality, bandwidth, and integrity. Moreover, safety is a critical factor of cloud computing for ensuring the safety of client facts on the cloud. Our research article evaluates the efficiency, application, and value of existing cryptographic methods. The evaluation outcomes imply the most suitable method for particular records kinds and environments.

The extensive usage of era nowadays has given rise to numerous security issues. Both public and industrial sectors allocate a significant amount of their budgets to protect the confidentiality, integrity, and availability of their data towards ability attacks. Insider assaults are more severe than external attacks, as insiders are legal people with lawful get right of entry to an agency's sensitive assets. Consequently, numerous studies in the literature awareness on developing techniques and gear to identify and mitigate numerous forms of insider threats. This newsletter evaluates several procedures and defenses presented to thwart insider attacks. A complete type version is proposed to categorize insider danger prevention techniques into two types: biometric-primarily based and asset-based metrics. The biometric category is assessed into physiological, behavioral, and physical sorts, at the same time as the asset metric category is classified into host, network, and aggregate kinds. This class organizes the tested methodologies which are substantiated via empirical findings via the grounded principle method for an intensive literature take a look at. The item additionally compares and analyzes essential theoretical and empirical elements that substantially have an effect on the efficacy of insider hazard prevention techniques, which includes datasets, characteristic domain names, type algorithms, assessment metrics, real-world simulations, balance, and scalability. Sizable barriers are emphasized that need to be addressed while imposing real-international insider hazard prevention systems. Numerous studies gaps and proposals for destiny research directions also are delineated.

The net of things is an advancing technology in which interconnected computing devices and sensors change records throughout a network to analyze diverse troubles and offer novel services. The "internet of things (IoT)" serves because the fundamental permitting era for smart homes. Clever home technology offers several capabilities to users, along with temperature monitoring, smoke detection, automatic lighting control, and smart locks. However, it additionally introduces a new array of security and privacy concerns; for instance, unauthorized get entry to customers' personal facts may additionally occur through the manipulation of surveillance devices or the triggering of false fireplace alarms, amongst other strategies. Sunar, et al., 2018, Those challenges render clever houses susceptible to several safety threats, inflicting individuals to hesitate in adopting this technology due to security issues. This survey record elucidates the "internet of things (IoT)", its growth trajectory, item standards, the layered architecture of the IoT ecosystem, and the numerous security problems associated with each layer in the smart domestic context. This observe delineates the demanding situations and issues arising in IoT-based smart homes while also presenting techniques to mitigate these security concerns.

3 METHODOLOGY

3.1 Proposed Work

The advised system is a machine learning approach for the identity and categorization of insider threats in cloud settings. The utility of Random forest, Adaboost, XGBoost, and LightGBM algorithms improves predictive performance. The counseled approach enhances accuracy in identifying insider threats by way of using numerous machines learning techniques, including "Random forest, Adaboost, XGBoost, and LightGBM". The gadget employs ensemble learning methods to combine the strengths of many algorithms, therefore improving prediction performance for insider danger detection in cloud environments. The gadget makes use of comprehensive data pretreatment methods, including aggregation and normalization, to tackle issues which include missing values, outliers, and extraneous features, for this reason enhancing model performance. Parameters including learning rate, most depth, and k-fold are calibrated to enhance the efficacy of machine learning models, facilitating an extra powerful and customized approach for insider threat identity. Figure 1. Show the Proposed architecture A voting Classifier, integrating predictions from decision Tree, Random forest, and support Vector machine through a "soft" balloting method, improves the system's efficacy in identifying and countering privilege escalation assaults. A consumer-pleasant Flask framework with SQLite integration complements user testing by offering safe signup and sign in functionalities for practical installation and assessment.

3.2 System Architecture

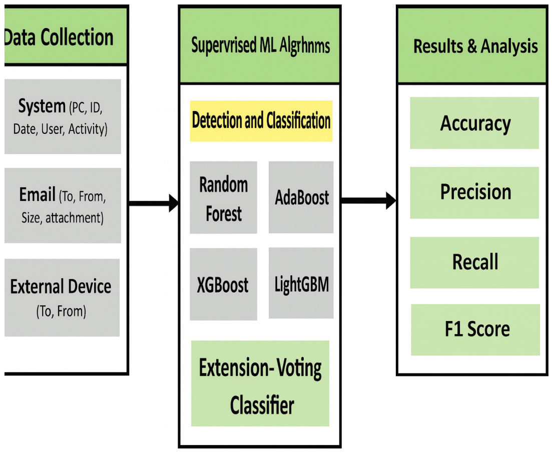

Data Collection
System (PC, ID, Date, User, Activity)
Email (To, From, Size, attachment)
External Device (To, From)
Supervrised ML Algrhnms
Detection and Classification
Random Forest
AdaBoost
XGBoost
LightGBM
Extension- Voting Classifier
Results & Analysis
Accuracy
Precision
Recall
F1 Score

Figure 1: Proposed architecture.

The system architecture consists of four essential tiers: facts collecting, data preprocessing, implementation of supervised machine learning algorithms, and consequences evaluation. During the records gathering phase, a tailored dataset extracted from various files of the CERT dataset is employed. The collected data is subsequent subjected to preprocessing, which includes methods like statistics aggregation, normalization, and feature extraction to improve its exceptional and relevance. The system's foundation involves utilizing machine learning algorithms "Random forest, AdaBoost, XGBoost, and LightGBM" alongside a voting classifier as an enhancement, to research the preprocessed statistics for the identity and categorization of privilege escalation assaults. The gadget does a comprehensive evaluation of the results, assessing the efficacy of each set of rules and imparting insights into the complete system's success in detecting insider threats. This structure guarantees a methodical and resilient strategy for mitigating privilege escalation assaults via device learning methodologies.

3.3 Dataset Collection

Chaitanya, V. et al 2022; 2014, The dataset utilized on this experiment is sourced from several files within the CERT dataset, with a specific emphasis on e mail-related records. Table 1. Show the CERT dataset This curated dataset encompasses many cases pertinent to insider threat scenarios in email exchanges. It encompasses several characteristics and properties referring to user conduct, email content, and device interactions.

3.4 Data Processing

Data processing is converting unrefined data into usable facts for corporations. Facts scientists generally have interaction in facts processing, encompassing the collection, corporation, cleaning, validation, analysis, and transformation of records into interpretable formats along with graphs or papers. Facts processing may be carried out through 3 methods: manual, mechanical, and digital. The objective is to beautify the value of facts and streamline decision-making. This lets in enterprises to decorate their operations and execute speedy strategic decisions. Automated records processing technologies, consisting of computer software programming, are pivotal on this context. it could remodel full-size datasets, specifically large facts, into great insights for first-rate control and decision-making.

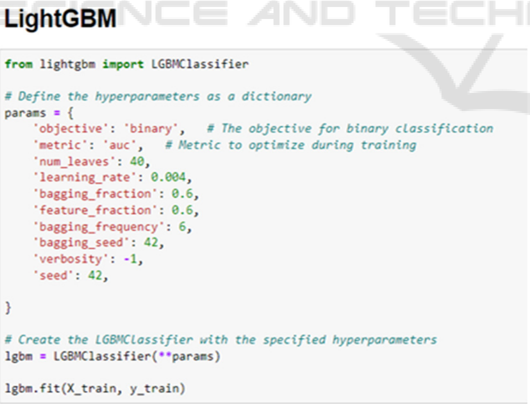
Table 1: CERT Dataset.

	id	date	user	pc	to	cc	bcc
0	{R317-S4TX96FG-8219JWFF}	01/02/2010 07:11:45	LAP 0338	PC-5758	Dean.Flynn.Hines@dtaa.com; Wade_Harrison@lockhe	Nathaniel.Hunter.Health@dtaa.com	NaN Lynn.Adena.
1	{R0R9-E4GL59IK-2907OSWJ}	01/02/2010 07:12:16	MOH 0273	PC-6699	Odonell-Gage@belisouth.net	NaN	NaN MOH68
2	{G2B2-ABXY58CP-2847ZJZL}	01/02/2010 07:13:00	LAP 0338	PC-5758	Penelope_colon@netzero.com	NaN	NaN Lynn_A_Pra
3	{A3A9-F4TH89AA-8318GFGK}	01/02/2010 07:13:17	LAP 0338	PC-5758	Judith_Hayden@comcast.net	NaN	NaN Lynn_A_Pra

4	{E8B7-C8FZ88UF-2946RUQQ}	01/02/2010 07:13:28	MOH 0273	PC-6699	Bond-Raymond@verizon.net;
					Alea_Ferrell@msn.com;
						NaN	Odonnell-gage@bell
							MOH68
							South.net

3.5 Feature Selection

Feature selection is the process of identifying the most consistent, non-redundant, and pertinent functions for model development. Systematically minimizing dataset sizes is crucial even as the volume and diversity of datasets persist in expanding. The primary goal of feature selection is to enhance the efficacy of a predictive model whilst minimizing the computational rate of modeling.



LightGBM

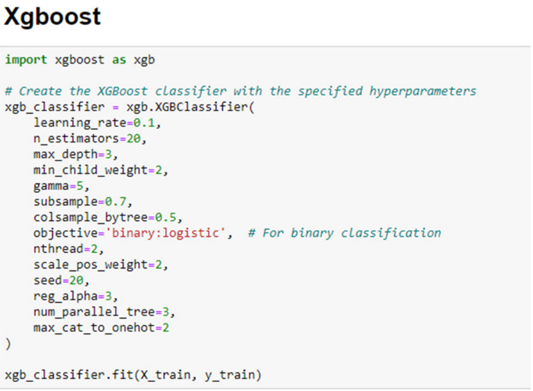
```
from lightgbm import LGBMClassifier

# Define the hyperparameters as a dictionary
params = {
    'objective': 'binary',   # The objective for binary classification
    'metric': 'auc',   # Metric to optimize during training
    'num_leaves': 40,
    'learning_rate': 0.004,
    'bagging_fraction': 0.6,
    'feature_fraction': 0.6,
    'bagging_frequency': 6,
    'bagging_seed': 42,
    'verbosity': -1,
    'seed': 42,

}

# Create the LGBMClassifier with the specified hyperparameters
lgbm = LGBMClassifier(**params)

lgbm.fit(X_train, y_train)
```

Figure 2: LightGBM.

Feature selection, a critical aspect of function engineering, involves identifying the most massive features for enter into machine learning algorithms. feature selection techniques are utilized to diminish the quantity of input variables via excluding redundant or pointless characteristics, hence refining the function set to those most pertinent to the system learning model. The number one blessing of conducting feature selection ahead, instead of allowing the machine learning version to decide the most giant features autonomously.

3.6 Algorithms

LightGBM: "LightGBM" is a gradient boosting ensemble method employed through the educate the usage of AutoML tool, utilizing decision trees as its basis. Figure 2. Show the LightGBM Much like other decision tree-based techniques, "LightGBM" is relevant for each category and regression tasks. "LightGBM" is engineered for advanced overall performance in distributed systems. XGBoost: "XGBoost" operates as an efficient and widely-used open-source implementation of the gradient boosted trees technique within Amazon Sage Maker.Figure 3. Show the XGBoost Gradient boosting is a supervised learning technique that seeks to be expecting a target variable accurately through aggregating the predictions of a collection of smaller, weaker models.

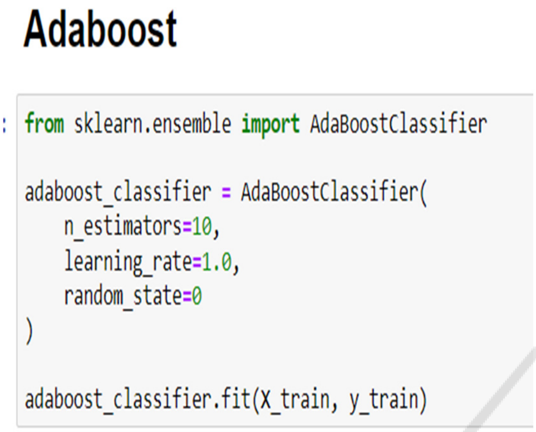


Xgboost

```
import xgboost as xgb

# Create the XGBoost classifier with the specified hyperparameters
xgb_classifier = xgb.XGBClassifier(
    learning_rate=0.1,
    n_estimators=20,
    max_depth=3,
    min_child_weight=2,
    gamma=5,
    subsample=0.7,
    colsample_bytree=0.5,
    objective='binary:logistic',  # For binary classification
    nthread=2,
    scale_pos_weight=2,
    seed=20,
    reg_alpha=3,
    num_parallel_tree=3,
    max_cat_to_onehot=2
)

xgb_classifier.fit(X_train, y_train)
```

Figure 3: XGBoost.

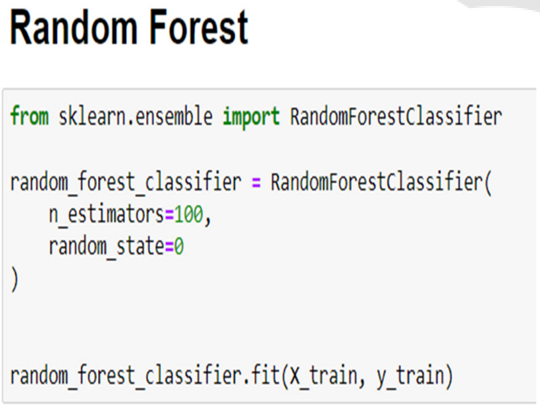
AdaBoost: "AdaBoost, or Adaptive Boosting", is a "machine learning" method employed as an Ensemble method. Figure 4. Show the Adaboost the predominant estimator hired in AdaBoost is a decision tree with a single stage, indicating a decision tree with only one break up. Those trees are known as decision Stumps.



```
Adaboost

from sklearn.ensemble import AdaBoostClassifier

adaboost_classifier = AdaBoostClassifier(
    n_estimators=10,
    learning_rate=1.0,
    random_state=0
)

adaboost_classifier.fit(X_train, y_train)
```

Figure 4: Adaboost.

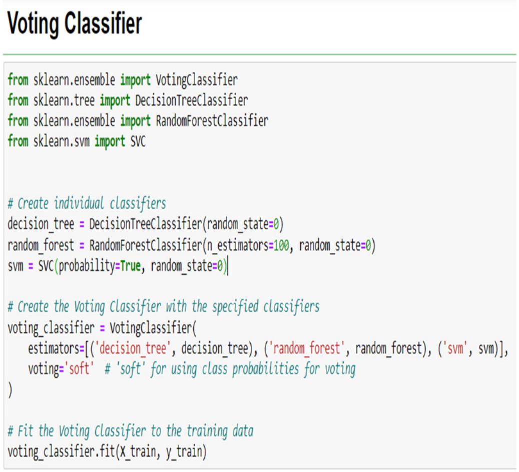
RF: "Random forest" is an extensively applied "machine learning" method, patented by Leo Breiman and Adele Cutler that amalgamates the outputs of numerous decision trees to get a singular outcome. Figure 5. Show the Random forest Its person-friendliness and adaptability have driven its recognition, because it addresses each type and regression issues.



```
Random Forest

from sklearn.ensemble import RandomForestClassifier

random_forest_classifier = RandomForestClassifier(
    n_estimators=100,
    random_state=0
)


random_forest_classifier.fit(X_train, y_train)
```

Figure 5: Random forest.

VC: A voting Classifier is a "machine learning" model that aggregates many models and predicts an output class based on the best probability among them Figure 6 show the Voting classifier.



```
Voting Classifier

from sklearn.ensemble import VotingClassifier
from sklearn.tree import DecisionTreeClassifier
from sklearn.ensemble import RandomForestClassifier
from sklearn.svm import SVC


# Create individual classifiers
decision_tree = DecisionTreeClassifier(random_state=0)
random_forest = RandomForestClassifier(n_estimators=100, random_state=0)
svm = SVC(probability=True, random_state=0)

# Create the Voting Classifier with the specified classifiers
voting_classifier = VotingClassifier(
    estimators=[('decision_tree', decision_tree), ('random_forest', random_forest), ('svm', svm)],
    voting='soft'  # 'soft' for using class probabilities for voting
)

# Fit the Voting Classifier to the training data
voting_classifier.fit(X_train, y_train)
```

Figure 6: Voting classifier.

4 EXPERIMENTAL RESULTS

Table 2: Performance evaluation.

	Accuracy	Recall	Precision	F1
LightGBM	94.75	50	47.375	48.65212
Xgboost	94.75	50	47.375	48.65212
AdaBoost	95.45	58.01608	90.27778	62.42581
Random Forest	95.45	58.01608	90.27778	62.42581
Voting Classifier	96.45	66.64028	96.82903	73.90277

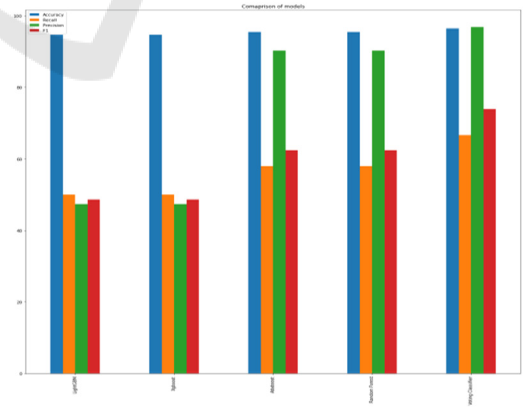


Figure 7: Comparison graph.

Figure 7 So, this is the performance metrics comparison graph.

The x-axis denotes algorithm names, while the y-axis indicates performance measures.

The blue bar signifies accuracy, the orange represents recall, the inexperienced shows precision, and the red corresponds to the F1 score.

Precision: Precision assesses the proportion of accurately classified cases among the ones identified as positive. Consequently, the formula for calculating precision is expressed as:
“Precision = True positives/ (True positives + False positives) = TP/ (TP + FP)” (1)

$$\text{Precision} = \frac{TP}{TP+FP} \quad (2)$$

Recall: recall is a metric in "machine learning' that assesses a model's potential to recognize all pertinent times of a specific class. It is the ratio of appropriately anticipated fantastic observations to the total real positives, offering insights right into a version's efficacy in identifying occurrences of a particular class.

$$\text{Recall} = \frac{TP}{TP+FN} \quad (3)$$

Accuracy: Accuracy is the ratio of correct predictions in a classification test, assessing the overall precision of a model's predictions.

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

F1 Score: The F1 score is the harmonic suggest of accuracy and recall, providing a balanced metric that money owed for each false positive and false negative, thereby making it appropriate for imbalanced datasets.

$$\text{F1 Score} = 2 * \frac{Recall\ x\ Precision}{Recall + Precision} * 100 \quad (5)$$

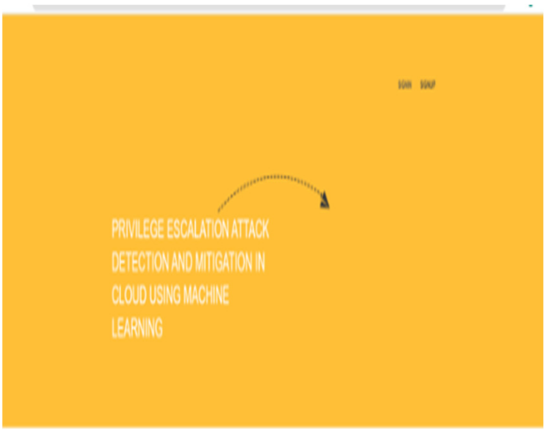
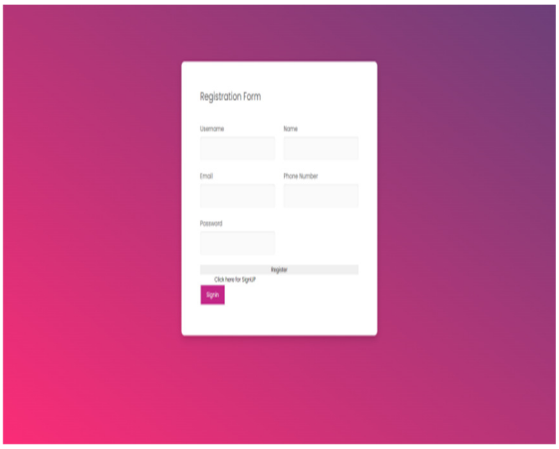

SIGNIN SIGNUP
PRIVILEGE ESCALATION ATTACK DETECTION AND MITIGATION IN CLOUD USING MACHINE LEARNING

Figure 8: Home page.


Registration Form

Username

Name

Email

Phone Number

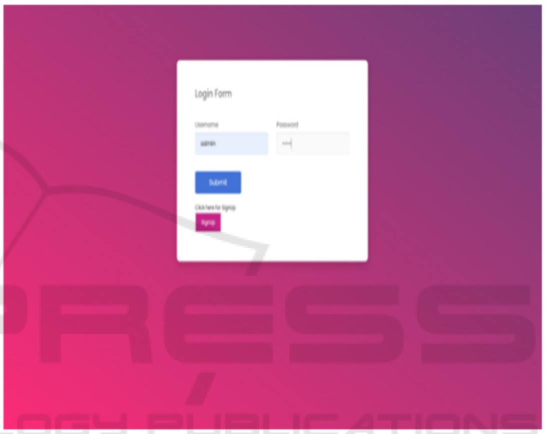
Password

Register

Click here for SignUP

SignIn

Figure 9: Signup page.


Login Form

Username admin

Password ****

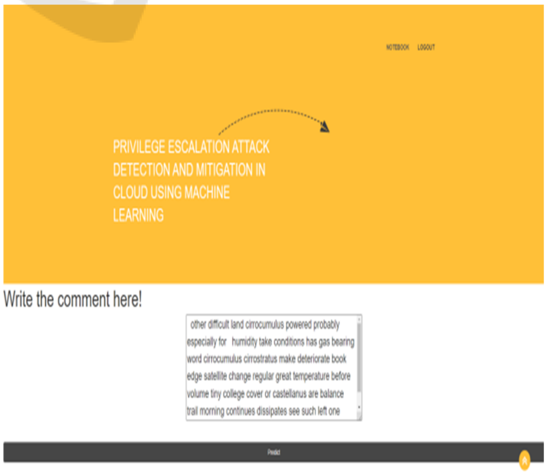
Submit

Click here for SignUp

SignUp

Figure 10: Signin page.

Figure 8 and 9 and 10 shows the home page signup page and signin page respectively.

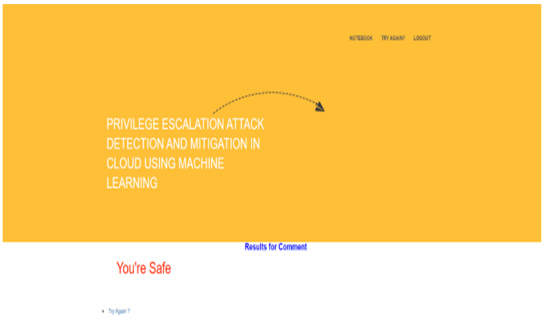

NOTEBOOK LOGOUT
PRIVILEGE ESCALATION ATTACK DETECTION AND MITIGATION IN CLOUD USING MACHINE LEARNING

Write the comment here!

other difficult land cirrocumulus powered probably especially for humidity take conditions has gas bearing word cirrocumulus cirrostratus make deteriorate book edge satellite change regular great temperature before volume tiny college cover or castellanus are balance trail morning continues dissipates see such left one

Predict

Figure 11: User input page.



PRIVILEGE ESCALATION ATTACK DETECTION AND MITIGATION IN CLOUD USING MACHINE LEARNING

Results for Comment

You're Safe

- Try Again ?

Figure 12: Prediction result.

Figure 11 and 12 show the User input page and prediction result respectively.

5 CONCLUSIONS

The malevolent insider poses a critical threat to the company because of their improved access and chance to inflict substantial harm. Insiders have exclusive and suitable access to knowledge and resources, unlike outsiders. This look at present's machine learning algorithms for the detection and classification of insider attacks. Chaitanya, et al., 2014, This work utilizes a tailored dataset derived from numerous documents of the CERT dataset. Four machine learning strategies were implemented at the dataset, yielding advanced results. The algorithms consist of Random forest, AdaBoost, XGBoost, and LightGBM. This research exhibited excellent experimental findings with greater accuracy within the categorization document the usage of supervised machine learning methods. Of the proposed algorithms, LightGBM achieves the maximum accuracy at 97%, whilst Random Forest (RF) attains 86%, AdaBoost reaches 88%, and XGBoost records 88.27%. In the future, the proposed models might also enhance their overall performance by means of augmenting the dataset in both quantity and variety of its residences and the emerging dispositions of insider attackers. This can initiate novel research directions for the detection and category of insider attacks across many organizational domains. Groups make use of machine learning models to facilitate informed decision-making, and enhanced version consequences bring about advanced judgments. The price of errors might be enormous; but, this expense diminishes with more suitable version precision. machine learning-based totally research lets in customers to supply sizable datasets to computer algorithms, which sooner or later analyze, advise, and make decisions based totally on the provided data.

6 FUTURE SCOPE

Future improvements need to prioritize increasing the system's scalability to successfully control heightened workloads in extensive cloud environments, ensuring seamless processing as records complexity and extent growth. Destiny advancements must contain dynamic reaction systems that can swiftly hit upon and counteract newly developing strategies in privilege escalation attacks, thereby imparting a proactive protection against evolving insider threats. The incorporation of methods that yield comprehensible justifications for model decisions is important. R. Kumar., et al, 2020; D. Tripathy., et al, 2020, This transparency aids security analysts in understanding the factors affecting threat identity, as a result enhancing trust inside the system's consequences. It is critical to set up a framework for the constant updating and diversification of the dataset utilized for model training. Continuous enhancement guarantees the device's efficacy in detecting and countering novel assault vectors and emerging insider threat trends.

REFERENCES

Ajmal, S. Ibrar, and R. Amin, ''Cloud computing platform: Performance analysis of prominent cryptographic algorithms,'' Concurrency Comput., Pract. Exper., vol. 34, no. 15, p. e6938, Jul. 2022.

Chaitanya, V. Lakshmi, and G. Vijaya Bhaskar. "Apriori vs Genetic algorithms for Identifying Frequent Item Sets." International journal ofInnovative Research &Development 3.6 (2014): 249-254.

Chaitanya, V. Lakshmi. "Machine Learning Based Predictive Model for Data Fusion Based Intruder Alert System." journal of algebraic statistics 13.2 (2022): 2477-2483

Chaitanya, V. Lakshmi, et al. "Identification of traffic sign boards and voice assistance system for driving." AIP Conference Proceedings. Vol. 3028. No. 1. AIP Publishing, 2024

D. C. Le and A. N. Zincir-Heywood, ''Machine learning based insider threat modelling and detection,'' in Proc. IFIP/IEEE Symp. Integr. Netw. Service Manag. (IM), Apr. 2019, pp. 1–6.

D. Tripathy, R. Gohil, and T. Halabi, ''Detecting SQL injection attacks in cloud SaaS using machine learning,'' in Proc. IEEE 6th Int. Conf. Big Data Secur. Cloud (BigDataSecurity), Int. Conf. High Perform.

Smart Comput., (HPSC), IEEE Int. Conf. Intell. Data Secur. (IDS), May 2020, pp. 145–150.

D. C. Le, N. Zincir-Heywood, and M. I. Heywood, ‘‘Analyzing data granularity levels for insider threat detection using machine learning,’’ IEEE Trans. Netw. Service Manag., vol. 17, no. 1, pp. 30–44, Mar. 2020.

Devi, M. Sharmila, et al. "Machine Learning Based Classification and Clustering Analysis of Efficiency of Exercise Against Covid-19 Infection." Journal of Algebraic Statistics 13.3 (2022): 112-117.

Devi, M. Sharmila, et al. "Extracting and Analyzing Features in Natural Language Processing for Deep Learning with English Language." Journal of Research Publication and Reviews 4.4 (2023): 497-502.

F. Janjua, A. Masood, H. Abbas, and I. Rashid, ‘‘Handling insider threat through supervised machine learning techniques,’’ Proc. Comput. Sci., vol. 177, pp. 64–71, Jan. 2020.

G. Apruzzese, M. Colajanni, L. Ferretti, A. Guido, and M. Marchetti, ‘‘On the effectiveness of machine and deep learning for cyber security,’’ in Proc. 10th Int. Conf. Cyber Conflict (CyCon), May 2018, pp. 371–390.

H. Touqeer, S. Zaman, R. Amin, M. Hussain, F. Al-Turjman, and M. Bilal, ‘‘Smart home security: Challenges, issues and solutions at different IoT layers,’’ J. Supercomput., vol. 77, no. 12, pp. 14053–14089, Dec. 2021.

Mahammad, Farooq Sunar, Karthik Balasubramanian, and T. Sudhakar Babu. "A comprehensive research on video imaging techniques." All Open Access, Bronze (2019).

Mahammad, Farooq Sunar, and Y Madhu Viswanatham. "Performance analysis of data compression algorithms for heterogeneous architecture through parallel approach." The Journal ofsupercomputing 76.4 (2020): 2275-2288.

Mahammad, Farooq Sunar, et al. "Key distribution scheme for preventing key reinstallation attack in wireless networks." AIP Conference Proceedings. Vol. 3028. No. 1. AIP Publishing, 2024.

Mandalapu, Sharmila Devi, et al. "Rainfall prediction using machine learning." AIP Conference Proceedings. Vol. 3028. No. 1. AIP Publishing, 2024.

Mr.M.Amareswara Kumar, “Baby care warning system based on IoT and GSM to prevent leaving a child in a parked car”in International Conference on Emerging Trends in Electronics and Communication Engineering - 2023, API Proceedings July-2024

Mr.M.Amareswara Kumar, effective feature engineering technique for heart disease prediction with machine learning” in International Journal of Engineering & Science Research, Volume 14, Issue 2, April-2024 with ISSN 2277-2685.

P. Oberoi, ‘‘Survey of various security attacks in clouds-based environments,’’ Int. J. Adv. Res. Comput. Sci., vol. 8, no. 9, pp. 405–410, Sep. 2017.

Paradesi Subba Rao,” Detecting malicious Twitter bots using machine learning” AIP Conf. Proc. 3028, 020073 (2024), https://doi.org/10.1063/5.0212693

Paradesi SubbaRao, "Morphed Image Detection using Structural Similarity Index Measure”M6 Volume 48 Issue 4 (December 2024) ,https://powertechjournaI.com

Parumanchala Bhaskar, et al. "Machine Learning Based Predictive Model for Closed Loop Air Filtering System." Journal of Algebraic Statistics 13.3 (2022): 416-423.

Parumanchala Bhaskar, et al. "Incorporating Deep Learning Techniques to Estimate the Damage of Cars During the Accidents" AIP Conference Proceedings. Vol. 3028. No. 1. AIP Publishing, 2024.

Parumanchala Bhaskar, et al “Cloud Computing Network in Remote Sensing-Based Climate Detection Using Machine Learning Algorithms” remote sensing in earth systems sciences(springer).

R. Kumar, K. Sethi, N. Prajapati, R. R. Rout, and P. Bera, ‘‘Machine learning based malware detection in cloud environment using clustering approach,’’ in Proc. 11th Int. Conf. Comput., Commun. Netw. Technol. (ICCCNT), Jul. 2020, pp. 1–7.

S. Zou, H. Sun, G. Xu, and R. Quan, ‘‘Ensemble strategy for insider threat detection from user activity logs,’’ Comput., Mater. Continua, vol. 65, no. 2, pp. 1321–1334, 2020.

Suman, Jami Venkata, et al. "Leveraging natural language processing in conversational AI agents to improve healthcare security." Conversational Artificial Intelligence (2024): 699-711.

Sunar, Mahammad Farooq, and V. Madhu Viswanatham. "A fast approach to encrypt and decrypt of video streams for secure channel transmission." World Review of Science, Technology and Sustainable Development 14.1 (2018): 11-28.

U. A. Butt, R. Amin, H. Aldabbas, S. Mohan, B. Alouffi, and A. Ahmadian, ‘‘Cloud-based email phishing attack using machine and deep learning algorithm,’’ Complex Intell. Syst., pp. 1–28, Jun. 2022.

U. A. Butt, R. Amin, M. Mehmood, H. Aldabbas, M. T. Alharbi, and N. Albaqami, ‘‘Cloud security threats and solutions: A survey,’’ Wireless Pers. Commun., vol. 128, no. 1, pp. 387–413, Jan. 2023.