ISSN: 2321-2152

IJMECE

International Journal of modern electronics and communication engineering

E-Mail
editor.ijmece@gmail.com
editor@ijmece.com

www.ijmece.com

ISSN2321-2152
www.ijmece .com
Vol 12, Issue 3, 2024

CLOUD PRIVILEGE ESCALATION ATTACK DETECTION AND MITIGATION USING ML

T ANIL KUMAR[1], S NETHAJI[2], K BHASKAR[3], K KAVITHA[4]
[1]Associate Professor, Department of MCA, Sri Venkatesa Perumal College of Engineering & Technology, Puttur, Email: anil.thumburu@gmail.com
[2]P.G Scholar, Department of MCA, Sri Venkatesa Perumal College of Engineering & Technology, Puttur, Email: sorakayapetanethaji2001@gmail.com
[3]Associate Professor, Department of MCA, Sri Venkatesa Perumal College of Engineering & Technology, Puttur, Email: bhaskark.mca@gmail.com
[4]Assistant Professor, Department of MCA, Madanapalli Institute of Technology and Science, Email:kavithagoud32@gmail.com

Abstract: This task utilizes strong ML to shield against honor acceleration dangers in cloud security. Privilege escalation attacks increment with cloud use. This undertaking further develops cloud administration security by fixing worker access privilege issues. The undertaking recognizes and mitigates privilege escalation dangers continuously utilizing ML. LightGBM, Random Forest, Adaboost, and Xgboost guard against evolving dangers. Cloud computing constructs trust by further developing information security for clients and associations. The task's security enhancements give cloud specialist organizations and organizations trust in web security. A Voting Classifier, which utilizes "soft" voting to consolidate Decision Tree, Random Forest, and Support Vector Machine expectations, further develops privilege escalation detection and mitigation. An easy to understand Flask framework with SQLite mix further develops client testing and secure information exchange and signin for commonsense establishment and evaluation.

Index Terms *- Privilege escalation, insider attack, machine learning, random forest, adaboost, XGBoost, LightGBM, classification.*

1. INTRODUCTION

Cloud computing is an original way to deal with Network access conveyance. Current foundation. Cloud storage suppliers use encryption, access control, and confirmation to get their frameworks and information. The cloud might store any type of information in numerous cloud information capacity structures basically boundlessly relying upon information openness, speed, and recurrence. Because of the volume of information traded among associations and cloud specialist organizations, both incidental and intentional breaks might happen. The very includes that make internet providers helpful for laborers and IT frameworks make it harder for firms to impede unapproved access [2]. Cloud administrations open associations to new security gambles including validation and open connection points. High level programmers access Cloud systems. Machine learning utilizes numerous procedures to further develop information the board and security. Numerous datasets

ISSN2321-2152
www.ijmece .com
Vol 12, Issue 3, 2024

are private and can't be disseminated because of security concerns or need significant factual highlights [3], [4].

The quickly developing Cloud market presents protection and security issues managed by regulation. At the point when Cloud Organization representatives shift jobs, their entrance certifications may not change. Old privileges are used awkwardly to take and harm important information. Every PC talking account has authority. Server data sets, privileged intel, and different administrations are normally restricted to allowed clients. By assuming control over a higher client account and expanding honors, a threatening aggressor can get to a delicate framework. Assailants can advance on a level plane to control more frameworks or in an upward direction to get administrator and root admittance to control the whole climate [1]. Horizontal privilege escalation happens when a client acquires the entrance consents of one more client with a similar level. Horizontal privilege escalation allows an aggressor to get to non-individual information. Severely fabricated Web applications might permit an aggressor to get to others' information [3], [5]. A flat rise of privileges hack allows the assailant to look at, change, and duplicate delicate information.[38]

Aggressors target information sources since they contain the most delicate and important data. Each cloud client's protection and security are hurt by missing information. Insider dangers are approved harm. Many firms and associations have inner organizations because of organization extension. As per current evaluations, 90% of associations dread insider assaults [7]. Honor rise gives aggressors more ways of going after an objective framework. Honor heightening is utilized by insider aggressors to get sufficiently close to delicate frameworks. Insider attacks are difficult to distinguish and forestall in light of the fact that they work beneath hierarchical security and frequently have special organization access. Insider danger detection and classification are testing and tedious [8].

In late examinations, analysts distinguished and ordered insider favored height attacks. To beat these obstructions, they proposed ML and DL strategies. Ongoing exploration used SVM, Naïve Bayes, CNN, Linear Regression, PCA, Random Forest, and KNN procedures. Because of the range of assaults, fast and successful ML procedures are esteemed. Detection, classification, and alleviation of insider assaults require a successful and productive procedure. We really want complex calculations like ML calculations to classify and estimate insider dangers to further develop security [17].

Knowing the exhibition of ML calculations on recognizing insider dangers allows you to pick the best calculation for every circumstance and distinguish regions for development. So you can help security. To improve and accelerate insider assault results, this exploration applies viable and productive ML calculations. ML calculations Random Forest, AdaBoost, XGBoost, and LightGBM were tried. By expanding characterization calculation prediction, the boosting strategy prepares an unfortunate classifier to be excellent. Random Forest, AdaBoost, and XGBoost arranged insider dangers quick and accurately.

2. LITERATURE REVIEW

Cloud computing gives PC structure assets on request. Ability to store and deal with data without shopper the executives. It offers public and confidential registering and information capacity on one Web stage. Likewise, security risks and weaknesses might block distributed computing reception. [5] Cloud computing security concerns, difficulties, techniques, and arrangements are canvassed in this article. A past survey found a few security issues. Security issues and arrangements are remembered for another cloud computing engineering model evaluation. All security issues, difficulties, techniques, and answers are in this article[40].

Cloud computing gives information capacity and handling limit on request without client association. People and gatherings communicate and get information utilizing email. Credit reports, monetary information, and other delicate information are consistently traded on the web. [1] Fraudsters utilize phishing to take client information by having all the earmarks of being dependable. Phishing messages could fool you into giving over delicate data. Email phishing endeavors while sending and getting are the central question. At the point when you open and read spam messages, the aggressor gets your information. As of late, everybody has battled with it. This article recognizes new messages, utilizes various properties and calculations for classification, and utilizations different legitimate and phishing information amounts. Estimations of current strategies yield a changed dataset. SVM [8, 10], Naive Bayes (NB), and LSTM [1, 27] were applied to a feature removed CSV and name record. This investigation regards phished email acknowledgment as a grouping issue. SVM, NB, and LSTM distinguish email phishing attacks better and all the more precisely, as per examination and execution. SVM, NB, and LSTM classifiers arrange email attacks most precisely at 99.62%, 97%, and 98%.

Progresses in science and innovation make cloud computing the following huge thing. Cloud cryptography encodes information [4]. Distributed storage is not difficult to get to, has modest hardware, security, and support costs, consequently every organization utilizes it. Data is encoded to forestall undesirable access. Today, we need to shield our PC and web information from dangers. [4] Cryptography relies upon response time, mystery, transmission capacity, and respectability. To protect client information on the cloud, cloud computing security is pivotal. We think about cryptography calculations' effectiveness, utilization, and utility in our review report. Assessment discoveries uncover which strategy is best for specific information and setting.

With far reaching innovation use, security challenges have emerged. General society and confidential areas burn through huge amount of cash safeguarding their information against attacks. Insider attacks are more extreme than outer assaults in light of the fact that approved individuals have legal admittance to significant hierarchical resources [36]. Many examination have been finished to make strategies and instruments to recognize and relieve insider dangers. This article talks about insider assault avoidance techniques. A solitary order model characterizes insider danger counteraction measures into biometric-based and resource based measurements. [36, 37] Resource measurements are classed as host, organization, and blended, while biometrics are physiological, conduct, and physical. This classification arranges experimentally affirmed methods involving grounded hypothesis for

ISSN2321-2152
www.ijmece .com
Vol 12, Issue 3, 2024

exhaustive writing appraisal. The article likewise looks at and talks about hypothetical and exact elements that influence insider danger counteraction strategies (e.g., datasets, include spaces, characterization calculations, assessment measurements, certifiable reenactment, steadiness and versatility). Conveying certifiable insider danger avoidance frameworks presents significant obstacles. Some exploration holes and potential examination targets are likewise recommended.

The quick creating Internet of Things [34] utilizes networked computing devices and sensors to impart information across the organization to tackle issues and offer new types of assistance. Smart houses depend on IoT. Smart home innovation offers temperature checking, smoke detection, computerized light control, brilliant locks, and so on. Nonetheless, it likewise raises extra security and protection concerns, for example, getting to client information by means of observation hardware or misleading alarms. These weaknesses render brilliant homes defenseless against security attacks, hence many are reluctant to utilize this innovation. This review article [6] examines IoT, its development, objects and their details, the layered IoT environment, and smart home security issues for each layer. This article examines IoT-based smart home security concerns and offers arrangements.

3. METHODOLOGY

i) Proposed Work:

The proposed cloud-based insider threat detection and categorization system utilizes ML. Utilizing Random Forest, Adaboost, XGBoost, and LightGBM further develops prediction. ML techniques like Random Forest, Adaboost, XGBoost [35], and LightGBM increment insider threat detection in the proposed system. Ensemble learning upgrades cloud insider threat detection prediction by consolidating the qualities of a few techniques. For better model execution, the framework utilizes information accumulation and standardization to address missing qualities, anomalies, and superfluous attributes. To distinguish insider dangers all the more proficiently, ML models' learning rate, greatest profundity, and K-fold are advanced. Likewise, a Voting Classifier that joins Decision Tree, Random Forest, and Support Vector Machine expectations through "soft" voting improves privilege escalation detection and mitigation. An easy to understand Flask structure with SQLite reconciliation further develops client testing and secure information exchange and signin for down to earth establishment and evaluation.

ii) System Architecture:

The system architecture incorporates information assortment, preprocessing, supervised ML calculations, and results examination. A tweaked dataset made from various CERT dataset documents is utilized for information gathering. After assortment, information is collected, standardized, and feature extracated to work on quality and pertinence. The framework detects and classifies privilege escalation threats utilizing ML calculations — Random Forest, AdaBoost, XGBoost, and LightGBM [31, 32] — and a voting classifier utilizing preprocessed information. At last, the framework dissects the discoveries to evaluate every calculation's presentation and the framework's capacity to distinguish insider dangers. This engineering tends to privilege escalation threats utilizing ML in an efficient and strong way.

ISSN2321-2152
www.ijmece .com
Vol 12, Issue 3, 2024

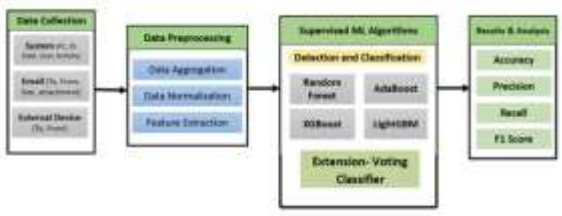

Fig 1 Proposed architecture

iii) Dataset collection:

This study utilized email-related information from various CERT documents [13, 14]. This organized dataset incorporates email insider danger events. It has a few client conduct, email content, and framework cooperation features.

Fig 2 CERT dataset

iv) Data Processing:

Data processing transforms crude information into business-valuable data. Information researchers assemble, put together, clean, check, examine, and organize information into diagrams or papers. Information can be handled physically, precisely, or electronically. Data ought to be more significant and decision-production simpler. Organizations might improve activities and pursue basic decisions quicker. PC programming advancement and other mechanized data processing innovations add to this. Huge information can be transformed into pertinent bits of knowledge for quality administration and navigation.

v) Feature selection:

Feature selection chooses the most steady, non-repetitive, and pertinent elements for model turn of events. As data sets extend in amount and assortment, purposefully bringing down their size is significant. The fundamental reason for feature selection is to increment prescient model execution and limit processing cost.

One of the vital pieces of feature engineering is picking the main attributes for machine learning algorithms. To diminish input factors, feature selection methodologies take out copy or superfluous elements and limit the assortment to those generally critical to the ML model. Rather than permitting the ML model pick the main qualities, feature selection ahead of time enjoys a few benefits.[42]

vi) Algorithms:

LightGBM: In view of decision trees, LightGBM is a gradient boosting ensemble approach used by the Train Utilizing AutoML device. LightGBM is a decision tree-based procedure that might be applied to relapse as well as order. Elite execution with disseminated frameworks is the focal point of LightGBM's advancement [31, 32].

ISSN2321-2152
www.ijmece .com
Vol 12, Issue 3, 2024

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)
```

Fig 3 LightGBM

XGBoost: A successful and broadly utilized open-source rendition of the gradient boosted trees procedure is Amazon SageMaker XGBoost. Gradient boosting is a methodology for supervised learning that joins the evaluations of a few more fragile, less complex models with an end goal to foresee an objective variable with a serious level of accuracy [35].

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)
```

Fig 4 XGBoost

AdaBoost: Otherwise called Adaptive Boosting, AdaBoost is an ML ensemble strategy technique. Decision trees with one level, or decision trees with just a single split, are the most famous assessor utilized with AdaBoost. One more name for these trees is 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)
```

Fig 5 Adaboost

RF: Leo Breiman and Adele Cutler are the brand name holders of the generally utilized ML method known as "random forest," which totals the result of a few decision trees to create a solitary end. Its fame has been prodded by its flexibility and convenience, since it can deal with both regression and classification issues [34].

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)
```

Fig 6 Random forest

VC: An ML model known as a voting classifier is prepared on a huge ensemble of models and figures a result (class) in view of the models' best probability of creating the ideal class.[44]

ISSN2321-2152
www.ijmece .com
Vol 12, Issue 3, 2024

Fig 7 Voting classifier

4. EXPERIMENTAL RESULTS

	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
RandomForest	95.45	58.01608	90.27778	62.42581
Voting Classifier	96.45	66.64028	96.82903	73.90277

Fig 8 Performance evaluation

Here is the performance metrics table. Here we can see the names of the algorithms and the values of accuracy, precision, recall, f-score and specificity achieved by them. Thus, we can see that the enhanced voting classifier outperforms all other models in all performance metrics.

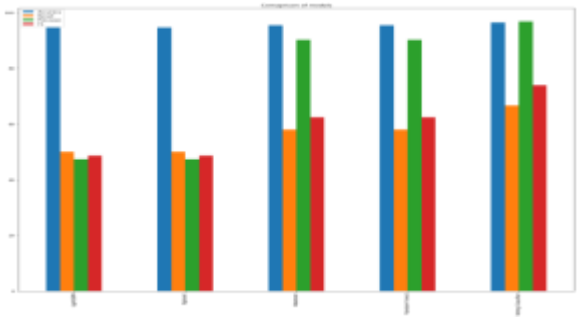

Fig 9 Comparison graph

Here is a comparison table of performance metrics.

Here, the x-axis represents the algorithm name and the y-axis represents the performance metric.

The blue bars here represent precision, orange represents recall, green represents accuracy, and red represents F1 score.

Precision: Precision estimates the level of positive cases or tests precisely sorted. Precision is determined utilizing the recipe:

$$\text{Precision} = \text{True positives}/ (\text{True positives} + \text{False positives}) = TP/(TP + FP)$$

$$\text{Precision} = \frac{True\ Positive}{True\ Positive + False\ Positive}$$

Recall: Machine learning recall assesses a model's ability to perceive all significant examples of a class. It shows a model's culmination in catching occasions of a class by contrasting accurately anticipated positive perceptions with complete positives.

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

Accuracy: A test's accuracy is its ability to recognize debilitated from sound cases. To quantify test accuracy, figure the small part of true positive and true negative in completely broke down cases. Numerically, this is:

$$\text{Accuracy} = TP + TN\ TP + TN + FP + FN.$$

ISSN2321-2152
www.ijmece .com
Vol 12, Issue 3, 2024

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

F1 Score: Machine learning model accuracy is estimated by F1 score. Consolidating model precision and recall scores. The accuracy measurement estimates how frequently a model anticipated accurately all through the dataset.

$$\text{F1 Score} = 2 * \frac{\text{Recall} \times \text{Precision}}{\text{Recall} + \text{Precision}} * 100$$

Fig 10 Home Page

Fig 11 Signup Page

Fig 12 Signin Page

Fig 13 User input Page

Fig 14 Prediction Result

5. CONCLUSION

Malignant insiders have more access and opportunity to cause serious harm, making them a main pressing issue. Insiders get select admittance to data and assets. This examination gave insider attack detection and classification ML strategies. [14] This study utilizes a custom fitted CERT dataset from different records. That dataset performed better with four ML methods. These calculations are Random Forest, AdaBoost,

XGBoost, and LightGBM. This article showed that these supervised ML strategies further develop classification accuracy in exploratory information. The LightGBM calculation has the best accuracy of 97%, trailed by RF (86%), AdaBoost (88%), and XGBoost (88.27%) [31, 32]. The introduced models might improve by broadening the dataset's size and variety of qualities and utilizing new insider assailant designs. New concentrate on recognizing and ordering insider attacks in different areas of association might result. Organizations settle on trustworthy business choices utilizing ML models, and better model results upgrade decisions. Botches are exorbitant, yet model accuracy diminishes them. ML-based research allows individuals to take care of PC calculations tremendous volumes of information to break down, suggest, and choose.[46]

6. FUTURE SCOPE

Future upgrades ought to enhance the framework's adaptability to oversee more noteworthy responsibilities in enormous cloud establishments and guarantee smooth handling as information intricacy and volume grow. Dynamic response systems that can rapidly distinguish and go against new honor heightening techniques ought to be carried out in later progressions to safeguard against creating insider dangers. Coordinating techniques that make sense of model choices is urgent. This receptiveness assists security examiners with understanding danger recognizable proof factors, supporting framework certainty [29, 30]. Making a framework for refreshing and expanding the model preparation dataset is fundamental. Persistent enhancement helps the framework distinguish and moderate new attacks and insider danger patterns.

REFERENCES

[1] 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.

[2] 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.

[3] 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.

[4] A. 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.

[5] 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.

[6] 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.

[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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] X. Sun, Y. Wang, and Z. Shi, ‘‘Insider threat detection using an unsupervised learning method: COPOD,’’ in Proc. Int. Conf. Commun., Inf. Syst. Comput. Eng. (CISCE), May 2021, pp. 749–754.

[14] J. Kim, M. Park, H. Kim, S. Cho, and P. Kang, ‘‘Insider threat detection based on user behavior modeling and anomaly detection algorithms,’’ Appl. Sci., vol. 9, no. 19, p. 4018, Sep. 2019.

[15] L. Liu, O. de Vel, Q.-L. Han, J. Zhang, and Y. Xiang, ‘‘Detecting and preventing cyber insider threats: A survey,’’ IEEE Commun. Surveys Tuts., vol. 20, no. 2, pp. 1397–1417, 2nd Quart., 2018.

[16] P. Chattopadhyay, L. Wang, and Y.-P. Tan, ‘‘Scenario-based insider threat detection from cyber activities,’’ IEEE Trans. Computat. Social Syst., vol. 5, no. 3, pp. 660–675, Sep. 2018.

[17] G. Ravikumar and M. Govindarasu, ‘‘Anomaly detection and mitigation for wide-area damping control using machine learning,’’ IEEE Trans. Smart Grid, early access, May 18, 2020, doi: 10.1109/TSG.2020.2995313.

[18] M. I. Tariq, N. A. Memon, S. Ahmed, S. Tayyaba, M. T. Mushtaq, N. A. Mian, M. Imran, and M. W. Ashraf, ‘‘A review of deep learning security and privacy defensive techniques,’’ Mobile Inf. Syst., vol. 2020, pp. 1–18, Apr. 2020.

[19] D. S. Berman, A. L. Buczak, J. S. Chavis, and C. L. Corbett, ‘‘A survey of deep learning methods for cyber security,’’ Information, vol. 10, no. 4, p. 122, 2019.

[20] N. T. Van and T. N. Thinh, ‘‘An anomaly-based network intrusion detection system using deep learning,’’ in Proc. Int. Conf. Syst. Sci. Eng. (ICSSE), 2017, pp. 210–214.

[21] G. Pang, C. Shen, L. Cao, and A. V. D. Hengel, ‘‘Deep learning for anomaly detection: A review,’’

ACM Comput. Surv., vol. 54, no. 2, pp. 1–38, Mar. 2021.

[22] R. A. Alsowail and T. Al-Shehari, ‘‘Techniques and countermeasures for preventing insider threats,’’ PeerJ Comput. Sci., vol. 8, p. e938, Apr. 2022.

[23] L. Coppolino, S. D’Antonio, G. Mazzeo, and L. Romano, ‘‘Cloud security: Emerging threats and current solutions,’’ Comput. Electr. Eng., vol. 59, pp. 126–140, Apr. 2017.

[24] M. Abdelsalam, R. Krishnan, Y. Huang, and R. Sandhu, ‘‘Malware detection in cloud infrastructures using convolutional neural networks,’’ in Proc. IEEE 11th Int. Conf. Cloud Comput. (CLOUD), Jul. 2018, pp. 162–169.

[25] F. Jaafar, G. Nicolescu, and C. Richard, ‘‘A systematic approach for privilege escalation prevention,’’ in Proc. IEEE Int. Conf. Softw. Quality, Rel. Secur. Companion (QRS-C), Aug. 2016, pp. 101–108.

[26] N. Alhebaishi, L. Wang, S. Jajodia, and A. Singhal, ‘‘Modeling and mitigating the insider threat of remote administrators in clouds,’’ in Proc. IFIP Annu. Conf. Data Appl. Secur. Privacy. Bergamo, Italy: Springer, 2018, pp. 3–20.

[27] F. Yuan, Y. Cao, Y. Shang, Y. Liu, J. Tan, and B. Fang, ‘‘Insider threat detection with deep neural network,’’ in Proc. Int. Conf. Comput. Sci. Wuxi, China: Springer, 2018, pp. 43–54.

[28] I. A. Mohammed, ‘‘Cloud identity and access management—A model proposal,’’ Int. J. Innov. Eng. Res. Technol., vol. 6, no. 10, pp. 1–8, 2019.

[29] F. M. Okikiola, A. M. Mustapha, A. F. Akinsola, and M. A. Sokunbi, ‘‘A new framework for detecting insider attacks in cloud-based e-health care system,’’ in Proc. Int. Conf. Math., Comput. Eng. Comput. Sci. (ICMCECS), Mar. 2020, pp. 1–6.

[30] G. Li, S. X. Wu, S. Zhang, and Q. Li, ‘‘Neural networks-aided insider attack detection for the average consensus algorithm,’’ IEEE Access, vol. 8, pp. 51871–51883, 2020.

[31] A. R. Wani, Q. P. Rana, U. Saxena, and N. Pandey, ‘‘Analysis and detection of DDoS attacks on cloud computing environment using machine learning techniques,’’ in Proc. Amity Int. Conf. Artif. Intell. (AICAI), Feb. 2019, pp. 870–875.

[32] N. M. Sheykhkanloo and A. Hall, ‘‘Insider threat detection using supervised machine learning algorithms on an extremely imbalanced dataset,’’ Int. J. Cyber Warfare Terrorism, vol. 10, no. 2, pp. 1–26, Apr. 2020.

[33] M. Idhammad, K. Afdel, and M. Belouch, ‘‘Distributed intrusion detection system for cloud environments based on data mining techniques,’’ Proc. Comput. Sci., vol. 127, pp. 35–41, Jan. 2018.

[34] P. Kaur, R. Kumar, and M. Kumar, ‘‘A healthcare monitoring system using random forest and Internet of Things (IoT),’’ Multimedia Tools Appl., vol. 78, no. 14, pp. 19905–19916, 2019.

[35] J. L. Leevy, J. Hancock, R. Zuech, and T. M. Khoshgoftaar, ‘‘Detecting cybersecurity attacks using different network features with LightGBM and XGBoost learners,’’ in Proc. IEEE 2nd Int. Conf.

Cognit. Mach. Intell. (CogMI), Oct. 2020, pp. 190–197.

[36] R. A. Alsowail and T. Al-Shehari, ‘‘Techniques and countermeasures for preventing insider threats,’’ PeerJ Comput. Sci., vol. 8, p. e938, Apr. 2022.

[37] B. Alouffi, M. Hasnain, A. Alharbi, W. Alosaimi, H. Alyami, and M. Ayaz, ‘‘A systematic literature review on cloud computing security: Threats and mitigation strategies,’’ IEEE Access, vol. 9, pp. 57792–57807, 2021.

[38] G.Viswanath, “Hybrid encryption framework for securing big data storage in multi-cloud environment”, Evolutionary intelligence, vol.14, 2021, pp.691-698.

[39] Viswanath Gudditi, “Adaptive Light Weight Encryption Algorithm for Securing Multi-Cloud Storage”, Turkish Journal of Computer and Mathematics Education (TURCOMAT), vol.12, 2021, pp.545-552.

[40] Viswanath Gudditi, “A Smart Recommendation System for Medicine using Intelligent NLP Techniques”, 2022 International Conference on Automation, Computing and Renewable Systems (ICACRS), 2022, pp.1081-1084.

[41] G.Viswanath, “Enhancing power unbiased cooperative media access control protocol in manets”, International Journal of Engineering Inventions, 2014, vol.4, pp.8-12.

[42] Viswanath G, “A Hybrid Particle Swarm Optimization and C4.5 for Network Intrusion Detection and Prevention System”, 2024, International Journal of Computing, DOI: https://doi.org/10.47839/ijc.23.1.3442, vol.23, 2024, pp.109-115.

[43]G.Viswanath, “A Real Time online Food Ording application based DJANGO Restfull Framework”, Juni Khyat, vol.13, 2023, pp.154-162.

[44] Gudditi Viswanath, “Distributed Utility-Based Energy Efficient Cooperative Medium Access Control in MANETS”, 2014, International Journal of Engineering Inventions, vol.4, pp.08-12.

[45] G.Viswanath,“ A Real-Time Video Based Vehicle Classification, Detection And Counting System”, 2023, Industrial Engineering Journal, vol.52, pp.474-480.

[46] G.Viswanath, “A Real- Time Case Scenario Based On Url Phishing Detection Through Login Urls ”, 2023, Material Science Technology, vol.22, pp.103-108.

[47] Manmohan Singh,Susheel Kumar Tiwari, G. Swapna, Kirti Verma, Vikas Prasad, Vinod Patidar, Dharmendra Sharma and Hemant Mewada, “A Drug-Target Interaction Prediction Based on Supervised Probabilistic Classification” published in Journal of Computer Science, Available at: https://pdfs.semanticscholar.org/69ac/f07f2e756b79181e4f1e75f9e0f275a56b8e.pdf