JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Insider Threat Detection using Optimal LSTM: A Novel Hybrid Beetle Swarm-based Cuckoo Search Optimization

S. Susila [1], K.Vaitheki [2] , K Suresh Joseph [3]
Department of Computer Science, Pondicherry University, Puducherry,
susilaselvaraju@gmail.com[1] vaidehi.balaji@gmail.com[2] ksjoseph.csc@gmail.com 3

Abstract - Insider threats are the hostile operations intending to do harm which are malevolent by authorized users such as theft of intellectual property or security information, fraud, and sabotage. While insider threats are far less common than external network assaults, they can nevertheless do significant harm. Insiders' harmful conduct is very difficult to detect since they are fully acquainted with an organization's system. Conventional techniques for detecting insider threats rely on rule-oriented techniques developed by domain specialists, but they are neither adaptable nor resilient. Insider-threat detection approaches on the basis of anomaly detection algorithms and user behavior modeling are proposed in this research. Three forms of datasets were created on the basis of user log data: e-mail distribution, daily activity summary, and weekly e-mail history. Further the malicious activities are detected by optimal LSTM, where the hidden neurons of the LSTM are tuned by novel hybrid BS-CSO by merging BSO and CSO with the intention of accuracy maximization. Experiments show that the suggested methodology works effectively for unbalanced datasets with minimal insider risks and absence of domain experts' knowledge.

Keywords—Insider Threat Detection; Optimal Long Short-Term Memory; Beetle Swarm-based Cuckoo Search Optimization; Accuracy Maximization

I. Introduction

Insider threats represents one among the major austere and common security threats that organizations face, in which harmful activities are carried out by authorized individuals within the company [11]. Insider threats are one among the major expensive and difficult to detect forms of assaults since insiders have access to a company's networked systems and are familiar with its structure as well as security processes [12]. According to cyber security estimates, insider attacks affect 53 percent of enterprises and 42 percent of US federal agencies each year. According to a recent report, insider threat assaults represent for 25% of entire attacks against organizations, while their frequency is proliferating [13]. Data breach, like trade secrets, client records are among the insider threat occurrences documented to date. In brief, networked systems are an essential component of every organization, since they share, store, and process data like sensitive information and intellectual property about workers and consumers [14]. As a result, the insider threat offers a severe cyber security risk that must be handled as soon as possible [15].

The insider threat is described by the CERT in a current technical report as threats perpetrated by unintentional or malicious insiders [16]. Malevolent behaviors conducted out both intentionally and unintentionally, like intellectual property theft, information system sabotage, and leaking of secret information [17]. Several issues of insider threat detection differ from standard intrusion detection jobs because the insider is permitted to use the systems and is knowledgeable with the protection layers [18]. Moreover, harmful insider behaviors by insiders are uncommon in the majority of firms. As a result, data to characterize the activity is frequently few and poorly recorded. Furthermore, the necessity to analyze and evaluate personnel information might provide hurdles to insider threat detection [19]. Data is also different depending on the organization. As a result, only a tiny percentage of companies contain the (human) resources and tools to understand user behavior and purpose from monitoring data [20].

Technological innovations have resulted in a steady evolution of how firms do business [21]. Employees now have permission to vast libraries of organization documents that are kept digitally on dispersed file servers. Several companies supply business computers to workers so they can work on the go, and they use e-mail to coordinate and plan appointments [22]. Employees are always linked to the Internet, in which they may acquire information on nearly everything they want for completing their task [23]. Services like video conferencing are widely utilized for organizing meetings throughout the globe. These technical improvements may make it simpler for insiders to assault due to the electronic nature of organizational documents. [24] [25].

In this research the following objectives where accomplished

To propose insider-threat detection approaches on the basis of anomaly detection algorithms and user behavior modeling.

To create three types of datasets on the basis of user log data.

To detect the malicious activities by optimal LSTM, where the hidden neurons of LSTM are optimized with the intention of accuracy maximization.

To suggest an innovative form of optimization algorithm referred as BS-CSO for enhancing the detection phase of the introduced insider threat detection model and to determine its superiority through various analyses.

The paper organization is as follows Section I is the introduction of insider threat detection. Section II has review about literature survey. Section III deals with dataset description and user behavior modeling. Section IV expounds with proposed model and preprocessing. Section V deals about optimal LSTM. Section VI explicates the results. Section VII pacts with conclusion.

II. Literature survey

A. Related Works

In 2020, Le *et al.* [1] have designed and tested a user-centered insider threat detection method on the basis of machine learning. Machine learning is used to analyze data at several levels of granularity beneath realistic situations in order to determine harmful insiders as well as malicious outsiders. A detailed examination is offered, along with several performance measurements, to aid in the realistic evaluation of system performance.

In 2021, Le and Heywood [2] have described an anomaly detection strategy for insider threats on the basis of unsupervised learning. We investigate several data descriptions with temporal information using four unsupervised learning algorithms including diverse working principles. Additionally, several computational intelligence approaches are being investigated in order to integrate these systems to develop anomaly detection ensembles that will improve detection performance. The technique's evaluation findings suggest that it can learn from unlabeled data under difficult situations to detect insider threats. Insider threats are recognized with great sensitivity and a low proportion of false positives. For instance, 60 percent of malicious insiders are caught with a budget of less than 0.1 percent, and complete harmful insiders are identified with a budget of less than 5%. Moreover, we investigate the durability of the suggested technique in terms of finding novel anomalous behaviors in diverse datasets. Furthermore, the findings show that a voting-oriented ensemble of anomaly detection may increase both detection performance and resilience. The suggested technique's efficacy is confirmed by comparisons to the conventional methods.

In 2018, Chattopadhyay *et al.* [3] have suggested a method for detecting insider threats based on user activity time series categorization. Firstly, the user activity records are used to construct a collection of single-day characteristics. The statistics of every single-day feature across time are then used to create a time-series feature vector. The data adjusted time-series feature group is classified with good recall, accuracy, and f-score by both deep AE and RF classifiers. Despite its excellent recall, the MLP has worse accuracy and f-score than the remaining two classifiers.

In 2019, Greitzer *et al.* [4] have concentrated on methods for gathering information regarding insider risks and applying that information to enhance insider risk assessments. By helping to promote a deeper consideration, enabling the information exchange of insider threat indicator knowledge all over organizations, increasing awareness, this data helps organizations set up or enhance conventional insider threat mitigation programmes.

In 2020, Alsowail and Shehari [5] have concentrated on empirical detection methods that are supported by empirical evidence. It shows various empirical detection methodologies' perspectives. Important criteria are also provided in order to determine the effectiveness of detection systems against insider threat situations (e.g., protection coverage, feature domains, classification techniques, etc.). The goal of this work is to improve projects in this area by standardizing methodologies. It also identifies the obstacles and limitations that need to be addressed in order to develop more workable responses for predicting, detecting, and preventing new attack occurrences. There exist also few suggestions for future study directions.

In 2017, Legg *et al.* [6] have presented a computerized system capable of identifying insider threats inside a company. We develop a tree-structure profiling technique that takes into account the intricacies of every user's and job role's actions, and then utilize it to offer a consistent description of characteristics that give a detailed explanation of the user's behavior. Deviation may be measured by comparing the amount of variation every user gaining recognition different qualities to their peers. We tested the system utilizing 10 simulated data-driven situations and discovered that it can detect abnormal behavior that might indicate a possible danger. We also demonstrate how the detection technology may be used in conjunction with visual analytics tools to aid analyst examination.

In 2020, Hammadi *et al.* [7] have provided a prototype for a platform that evaluates EEG signals to identify insider threats employing a model learned utilizing a deep learning algorithm. On the basis of four category risk matrices, the system could categorize various mental states. It examines brainwave signals utilizing LSTM, which is meant to recall every insider's prior mental states and match them to the present categorization. On the similar dataset, we conducted a comparison study utilizing LR to characterize the connection to assess the effectiveness of the introduced scheme. In comparison to LR, the experimental findings imply that LSTM could attain a classification accuracy of 80%.

In 2019, Liu *et al.* [8] have proposed an innovative method for dealing with a range of security logs. We can estimate the posterior probabilities for insider behaviors utilizing the Word2vec method trained with the corpus. As a result, we identify altered events as questionable if their behavioral probability falls below a certain level, and we identify users as malevolent if they are linked to several suspicious events. The testing show that the suggested technique was efficient and adaptable in real-world scenarios, but also give suggestions for modifying the thresholds and parameters.

In 2021, Nasir *et al.* [9] have concentrated on detecting insider threats using user behavior analysis. During the implementation stage, chosen feature vectors are utilized to fit the classifier. A deep learning-oriented technique that detects insiders having improved accuracy and a low FPR is offered. For detection, a robust event/user role feature group encompassing User role, Logoff/Logon events, Functional unit, and other features is employed. It have been compared to the performance of the proposed algorithm. The unique technique generates comparatively excellent performance.

In 2016, Bao *et al.* [10] have suggested a BLITHE detection of data monitor devices in smart grids, in which operations must be continuous and accurate. A compliance-distance-oriented and rule-weight grading technique is devised in particular that considerably increases the efficacy of the typical grading approach for trustee assessment. The statistical property, i.e., the mathematical assumption of every trustee's conformance degree, is examined in depth from both practical and theoretical perspectives, with the goal of achieving an acceptable good compromise among false alarms and detection accuracy in order to detect extra hidden and sophisticated attackers. Furthermore, we show that BLITHE exceeds the traditional for identifying anomalous behaviors in ubiquitous smart grid applications using actual data.

III. Dataset description and user behavior modeling for the insider threat detection

A. Dataset Description

In this research we have utilized the "CERT Insider Threat Tools" dataset since obtaining genuine business system logs is extremely challenging. Employee computer usage logs (device, logon, file, http, and email) are included in the CERT dataset, along with certain organizational data like employee departments as well as responsibilities. Every table has columns for the ID of the user, timestamps, and actions. On the basis of the dataset version, the categories of usage data, the count of employees, the amount of variables, and the count of harmful insider actions vary. R6.2, the most recent and biggest dataset, was used in this investigation. The sample now has 4000 individuals, with just five of them engaging in harmful behavior.

B. User Behaviour Modeling

User behaviors in the CERT dataset are: login, http, USB, file, and email. To fully exploit data, the behavioral information must be integrated into a single standardized data table in chronological sequence. We initially combined classification algorithm, so the suggested user-level insider-threat detection methods developed in this research on a weekly or daily basis. It is feasible to capture the count of times within a certain day using the information contained in the login table.

The research focuses the input factors utilized in previous research to find suitable input variables. We produced entire potential variables that may be derived from the CERT dataset using these references. There are 60 possible input variables in all. A total of 1,394,010 occurrences were retrieved when this daily summarizing procedure was finished. Every instance reflects a day's worth of action for a given user.

It was identified that three roles conduct the majority of anomalous actions (almost 90%): "Information Technology (IT) Admin," "Salesman," and "Electrical Engineer." It is not only hard to design an effective detection system that contains fewer than three abnormal examples. As a result, we built detection algorithms and tested their efficacy for the three jobs mentioned above.

The input variables employed to train machine learning algorithm, particularly anomaly detection, have a significant impact on their performance [26]. When the independence among input variables is established, the methods should enhance as the count of variables grows. Yet, owing to the strong reliance among variables as well as the presence of noise, a vast count of input variables can occasionally degrade the system performance when subjected to a real-world dataset. As a result, rather than employing every variable to ensure improved performance, it is required to pick a group of useful variables.

IV. Proposed model and preprocessing for the insider threat detection

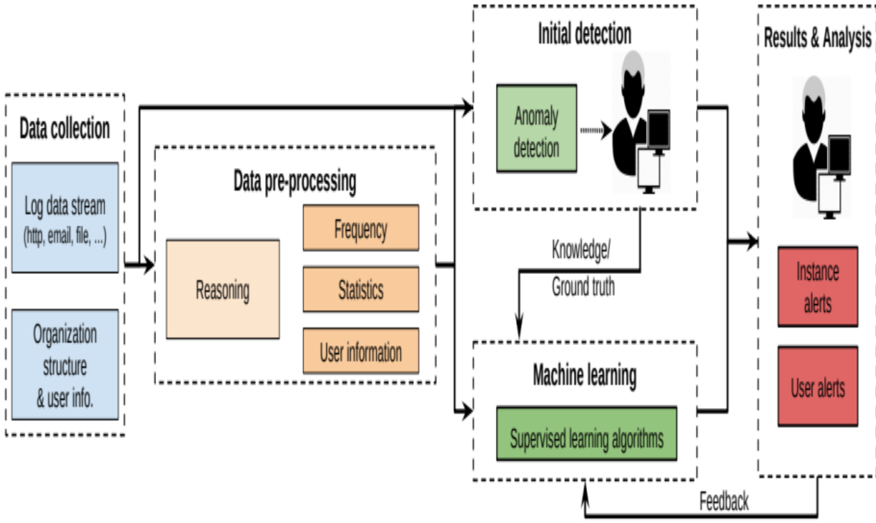
A. Proposed Model

This paper presents a deep learning-oriented approach for detecting insider threats in corporate computer networks. The system's parts are shown in Figure 1. The data collecting process in this study is based on the CERT insider threat dataset [27]. The system is built on a modular approach, which includes various modules to be readily customized to meet the demands of various businesses. Moreover, as shown in Figure 1, the system analyst acts as a crucial role in the introduced scheme.

Data gathering as well as pre-processing are the initial stages in the technology. Data includes firewall logs, web and email logs, network traffic captures, and various forms of user records [28] [29]. This study considers the below data sources as system input, on the basis of publicly accessible CERT: (i) activity log data stream, like browser, log on/off records, or device and file access logs and (ii) user information and organization structure. The initial type of data, which represents dynamic and constantly created, is the most important source based on their actions. The next type is for giving background information or perspective. The LDAP is used to manage the data source for CERT insider threat data.

Security analysts, on the other hand, may spot suspicious behaviors or strange variations in user behavior and conduct a more thorough investigation. In any case, this procedure is labor intensive [30] [31]. Moreover, we investigate the impact of various feature engineering strategies on the algorithms' accuracy. The goal of this stage is to generalize from the initial, and frequently restricted, knowledge of harmful and regular user behavior to discover previously undetected hostile insider situations. In this stage, the clear benefit of supervised learning algorithms is that they can build classifiers with far higher accuracy, and hence lower false alarm rates, when compared with the unsupervised learning techniques [32] [31]. Furthermore, security analyst judgments on alarms and warnings may be a valuable source of information for machine learning methods.

The introduced system not only gives outcomes for particular data instances, like harmful behaviors, but also user-oriented outcomes, like accurately discovered malicious insiders, at the final stage. In the majority of circumstances, user behaviors over a lengthy period of time must be considered when processing an alert about questionable user activity (data example) [33]. Moreover, in this application instance, in which normal data makes up the great bulk of the data gathered, a low FAR may need a huge amount of attention if it labels data from a variety of individuals as dangerous. As a result, user-oriented reporting may accurately reflect the security analysts' burden on insider detection duties.



B. Data pre processing

In majority of the circumstances, the data obtained lacks adequate background information for feature extraction, like mandated working hours or PC ownership. As a result, data pre-processing includes a reasoning stage. This stage is completed to acquire useful auxiliary data for subsequent processing. The data for the CERT datasets was evaluated, and acceptable systems for defining user-user relationships, and website classifications were developed.

In this paper, we investigate data granularity depending on the period: user-day, user session, and user-week data. It records user behaviors from the time they log in to the time they log out on a PC. Because a session is generally short and focused in one time period, this data type has fewer properties. However, because bad individuals prefer to undertake harmful acts in particular sessions and remaining sessions may be legitimate, session-oriented data may be useful in identifying malicious behaviors [36]. Day and week-oriented data points, consequently, summarize users' behaviors throughout the respective time periods. With a greater feature count, these forms of data may offer a better summary of behavior throughout a day or week, and learning may be accelerated because to the smaller amount of data. Nevertheless, they may cause the true hostile acts to be averaged out, requiring a lengthier reaction time if insiders are found. Furthermore, the data gathering and processing procedures are meant to be adaptable, and they will require to be tweaked to meet the unique context of a company.

Optimal LSTM for the insider threat detection

A. Optimal LSTM

LSTMs are somewhat of a RNN that, by convention, can learn long-term associations and apply knowledge for lengthy periods of time. It is arranged in the format of a chain. The recurring module, on the other hand, has a slight variation. It features four interacting layers having a unique form of communication, rather than a single NN like a normal RNN. LSTMs are aimed at avoiding the long-term reliance difficulty.

The initial stage is to make reports. The sigmoid function, which allows us to obtain of the last LSTM unit (i_{u-1}) at time $u-1<$ and the corresponding output (Y_u) at time u, determines the data. The forget gate (or g_u) is a gate in which g_u represents a vector having values ranging from 0 to 1 that corresponds to every count in the cell state, D_{u-1}.

$$g_u = \sigma\left(X_g[i_{u-1}, Y_u] + c\right) \quad (1)$$

Here, σ represents the sigmoid function, and $X_g$and $X_g$represents the forget gate's weight matrices and bias, appropriately. The next stage is to decide and store data from the innovative input (Y_u) in the cell state, as well as to revise the cell state. This innovative memory is subsequently combined with D_{u-1}, giving in D_u.

$$j_u = \sigma\left(X_j[i_{u-1}, Y_u] + c_j\right) \quad (2)$$

$$O_u = tanh\,(X_o[i_{u-1}, Y_u] + c_o) \quad (3)$$

$$D_u = D_{u-1}g_u + O_u j_u \quad (4)$$

D_{u-1} and D_u represents the cell states at time $u-1$ and u, accordingly, whereas X and c represents the cell state's weight matrices and bias, accordingly. The output values (i_u) in the last step are filtered versions of the output cell state (P_u).

$$D_u = \sigma\left(X_p[i_{u-1}, Y_u] + c_p\right) \quad (5)$$

$$i_u = P_u \, tanh \, tanh \, (D_u) \tag{6}$$

The output gate's weight matrices and bias, accordingly, are X_p and c_p.

LSTM returns benefits like it does not require fine adjustments, gap length insensitivity, etc. But, it suffers from shortcomings such as longer training time, need more memory, etc. Hence, to overcome the limitations, the hidden neurons of LSTM are tuned with the consideration of accuracy maximization, thus referred as optimal LSTM. This optimal LSTM saves time and memory and also avoids computational complexity.

B. Proposed BS-CSO

The BS-CSO is used for enhancing the detection phase of the insider threat model. It optimizes the hidden neuron count of LSTM with the intention of accuracy maximization. The Cuckoo Search method [34] defines a meta-heuristic optimization. Ordinarily, the parameters of the cuckoo search are maintained constant for a specified period of time, which reduces the algorithm's effectiveness. A good method for tweaking the cuckoo search parameters must be established to tackle this problem. Cuckoos are intriguing birds, not just for their wonderful calls, but also for their proactive breeding method. Furthermore, we predict that user-oriented outcome reporting will be critical when fewer species, like Ani and Guira cuckoos, hatch their eggs in host bird nests and destroy other eggs to improve the birth chance of their own. The technique is used in real-life circumstances. The advantage of CSO is its simplicity, easier implementation, etc. but, it limits from multi modal optimization problems. Thus, to overcome its shortcomings BSO is integrated into it and the so formed novel hybrid optimization algorithm is referred as BS-CSO.

The standard PSO is developed from BSO [35] that analyzes the fitness function estimates of their left and right sides and evaluate the better of the two, which may be employed to maintain the movement of the beetle swarm.

In the proposed BS-CSO, the algorithm can be functioned according to the random concept. If $rand \leq 0.5$, then the update occurs using BSO as below.

$$y_j^{l+1} = y_j^l + w_j^{l+1} \tag{7}$$

$$w_j^{l+1} = w_j^{l+1} + d_1 \cdot rand \cdot \left(Pc_j^l - y_j^l\right) + d_2 \cdot rand \cdot \left(Ph_j^l - y_j^l\right) + d_3 \cdot rand \cdot vc \tag{8}$$

Here, the update rate is shown by vc, position after l^{th} iteration is y_j^{l+1}, learning factors are d_1, d_2, d_3, speed of j^{th} particle is w_j^{l+1}, individual optimal solution is Pc_j^l, and global optimal solution is Ph_j^l respectively.

Otherwise, if $rand > 0.5$, then the update occurs through CSO as below.

$$Y_j^{(l+1)} = Y_j^{(l)} + \alpha \oplus Levy(\lambda) \tag{9}$$

Here, the step size is α, new solution is $Y_j^{(l+1)}$, existing solution is $Y_j^{(l)}$, and levy flight is $Levy(\lambda)$ respectively. The pseudo code of BS-CSO is in Algorithm 1.

Algorithm 1: BS-CSO
Begin
Population initialization
Parameter initialization
Fitness computation
While $l < l_{max}$
If $rand \leq 0.5$
$y_j^{l+1} = y_j^l + w_j^{l+1}$
else
$Y_j^{(l+1)} = Y_j^{(l)} + \alpha \oplus Levy(\lambda)$
End if
$l = l + 1$
Stop

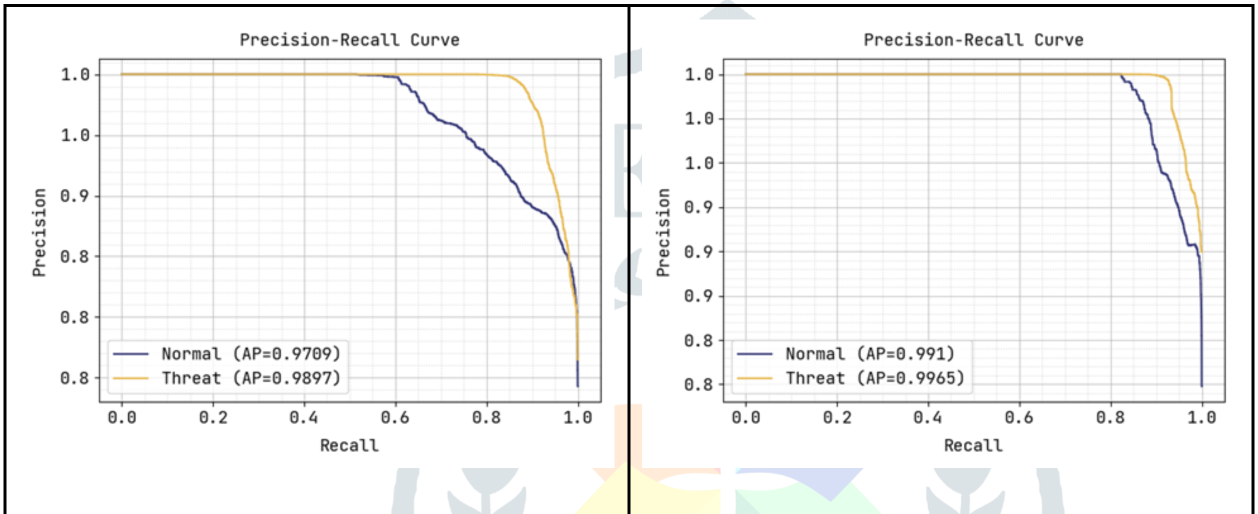
VI. Results

A. Experimental Setup

The proposed insider threat detection model has been done using the base as optimal LSTM and the outcomes were analyzed. Here, the implementation has been performed in terms of various analysis such as precision recall analysis, ROC analysis, and confusion matrix analysis respectively.

B. Precision Recall Analysis

This analysis of different methods such as LSTM and optimal LSTM is shown here. Precision describes a measure for expressing the quantity. Similarly, recall represents the positive class prediction count out of the total positive illustrations.

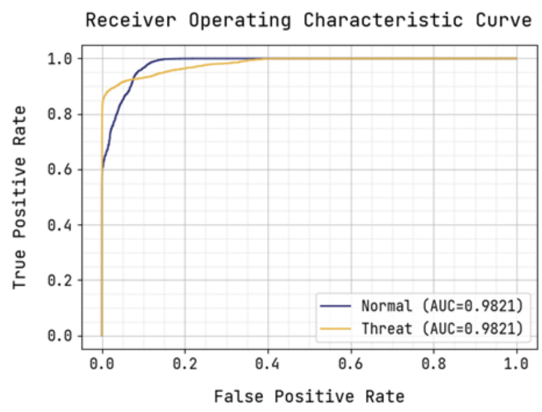


LSTM	Optimal LSTM

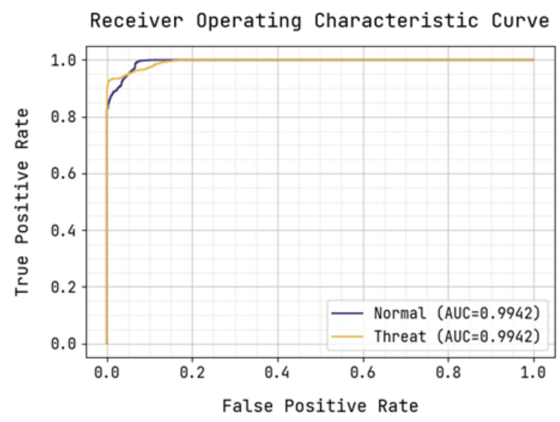
Fig. 2. Precision Recall Analysis

C. ROC Analysis

This graph depicts the ROC analysis of several approaches like LSTM and optimal LSTM. It defines a graphical plot for describing the capability of the binary classifier system when its discrimination threshold varies. The accuracy within the predictive methods is compared here.



LSTM

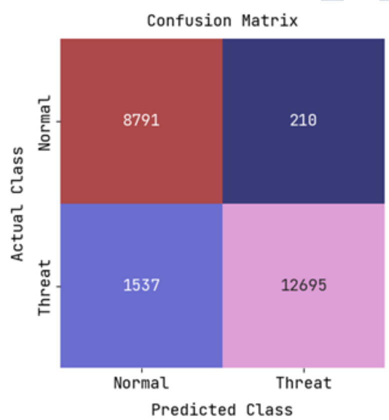


Optimal LSTM

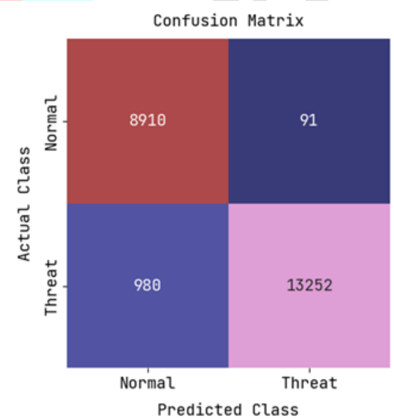
Fig. 3. ROC Analysis

D. Confusion Matrix Analysis

The confusion matrix analysis of different techniques, such as LSTM and optimal LSTM, is shown in this graph. It evaluates the detection model's performance. It visualizes the significant predictive analysis.



LSTM



Optimal LSTM

Fig. 4. Confusion Matrix Analysis

VII. Conclusion

This work proposed insider-threat detection methodologies depending on anomaly detection algorithms and user behavior modeling. On the basis of user log data, we developed three types of datasets: e-mail subject distribution, daily activity summary, and weekly e-mail communication history. The harmful behaviors are then identified using an optimum LSTM, with the hidden neurons of the LSTM being modified using an unique hybrid BS-CSO that combines BSO and CSO with the goal of maximizing accuracy. Experiments revealed that the suggested technique may work for datasets with negligible insider risks and without the knowledge of domain experts.

References

[1] D. C. Le, N. Zincir-Heywood and M. I. Heywood, "Analyzing Data Granularity Levels for Insider Threat Detection Using Machine Learning," in IEEE Transactions on Network and Service Management, vol. 17, no. 1, pp. 30-44, March 2020.

[2] D. C. Le and N. Zincir-Heywood, "Anomaly Detection for Insider Threats Using Unsupervised Ensembles," in IEEE Transactions on Network and Service Management, vol. 18, no. 2, pp. 1152-1164, June 2021.

[3] P. Chattopadhyay, L. Wang and Y. -P. Tan, "Scenario-Based Insider Threat Detection From Cyber Activities," in IEEE Transactions on Computational Social Systems, vol. 5, no. 3, pp. 660-675, Sept. 2018.

[4] F. L. Greitzer, J. Purl, Y. M. Leong and P. J. Sticha, "Positioning Your Organization to Respond to Insider Threats," in IEEE Engineering Management Review, vol. 47, no. 2, pp. 75-83, 1 Secondquarter,june 2019.

[5] R. A. Alsowail and T. Al-Shehari, "Empirical Detection Techniques of Insider Threat Incidents," in IEEE Access, vol. 8, pp. 78385-78402, 2020.

[6] P. A. Legg, O. Buckley, M. Goldsmith and S. Creese, "Automated Insider Threat Detection System Using User and Role-Based Profile Assessment," in IEEE Systems Journal, vol. 11, no. 2, pp. 503-512, June 2017.

[7] A. Y. Al Hammadi et al., "Novel EEG Sensor-Based Risk Framework for the Detection of Insider Threats in Safety Critical Industrial Infrastructure," in IEEE Access, vol. 8, pp. 206222-206234, 2020.

[8] L. Liu, C. Chen, J. Zhang, O. De Vel and Y. Xiang, "Insider Threat Identification Using the Simultaneous Neural Learning of Multi-Source Logs," in IEEE Access, vol. 7, pp. 183162-183176, 2019.

[9] R. Nasir, M. Afzal, R. Latif and W. Iqbal, "Behavioral Based Insider Threat Detection Using Deep Learning," in IEEE Access, vol. 9, pp. 143266-143274, 2021.

[10] H. Bao, R. Lu, B. Li and R. Deng, "BLITHE: Behavior Rule-Based Insider Threat Detection for Smart Grid," in IEEE Internet of Things Journal, vol. 3, no. 2, pp. 190-205, April 2016.

[11] A. Azaria, A. Richardson, S. Kraus, and V. S. Subrahmanian, "Behavioral analysis of insider threat: A survey and bootstrapped prediction in imbalanced data," IEEE Trans. Comput. Social Syst., vol. 1, no. 2, pp. 135–155, Jun. 2014.

[12] J. Glasser and B. Lindauer, "Bridging the gap: A pragmatic approach to generating insider threat data," in IEEE SPW, 2013.

[13] K. Padayachee, "An assessment of opportunity-reducing techniques in information security: An insider threat perspective," Decision Support Systems, vol. 92, pp. 47–56, 2016.

[14] P. Legg, N. Moffat, J. Nurse, J. Happa, I. Agrafiotis, M. Goldsmith, and S. Creese, "Towards a conceptual model and reasoning structure for insider threat detection," J. Wireless Mobile Netw., Ubiquitous Comput., & Depend. Appl. (JoWUA), vol. 4, no. 4, pp. 20–37, 2013.

[15] P. Parveen and B. Thuraisingham, "Unsupervised incremental sequence learning for insider threat detection," in IEEE Int. Conf. on Intelligence and Security Informatics, 2012.

[16] D. C. Le, S. Khanchi, A. N. Zincir-Heywood, and M. I. Heywood, "Benchmarking evolutionary computation approaches to insider threat detection," in ACM Genetic and Evolutionary Computation Conf., 2018.

[17] S. C. Roberts, J. T. Holodnak, T. Nguyen, S. Yuditskaya, M. Milosavl jevic, and W. W. Streilein, "A model-based approach to predicting the performance of insider threat detection systems," in IEEE SPW, 2016.

[18] A. Harilal et al., "The wolf of sutd (twos): A dataset of malicious insider threat behavior based on a gamified competition." JoWUA, vol. 9, no. 1, pp. 54–85, 2018.

[19] O. Brdiczka, J. Liu, B. Price, J. Shen, A. Patil, R. Chow, E. Bart, and N. Ducheneaut, "Proactive insider threat detection through graph learning and psychological context," in IEEE SPW, 2012, pp. 142–149, 2012.

[20] D. C. Le and A. N. Zincir-Heywood, "Evaluating insider threat detection workflow using supervised and unsupervised learning," in IEEE SPW, 2018.

[21] B. Bose, B. Avasarala, S. Tirthapura, Y. Y. Chung, and D. Steiner, "Detecting insider threats using radish: A system for real-time anomaly detection in heterogeneous data streams," IEEE Systems Journal, 2017.

[22] A. Azaria, A. Richardson, S. Kraus, and V. S. Subrahmanian, "Behav ioral analysis of insider threat: A survey and bootstrapped prediction in imbalanced data," IEEE Transactions on Computational Social Systems, vol. 1, no. 2, pp. 135–155, Jun. 2014.

[23] C. P. Pfleeger, "Reflections on the insider threat," in Insider Attack and Cyber Security. Boston, MA, USA: Springer, 2008, pp. 5–16, 2008.

[24] A. Coden et al., "Uncovering insider threats from the digital footprints of individuals," IBM J. Res. Develop., vol. 60, no. 4, pp. 8:1–8:11, Jul./Aug. 2016.

[25] G. B. Magklaras and S. M. Furnell, "Insider threat prediction tool: Evaluating the probability of IT misuse," Comput. Secur., vol. 21, no. 1, pp. 62–73, 2001.

[26] Guyon, I.; Elisseeff, A. "An introduction to variable and feature selection", J. Mach. Learn. Res, vol. 3, pp. 1157-1182, 2003.

[27] CERT and ExactData, LLC . Insider Threat Tools. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=508099. Accessed July 09, 2019.

[28] Collins ML, Theis MC, Trzeciak RF, et al. "Common Sense Guide to Mitigating Insider Threats", Fifth Edition. tech. rep., The CERT Insider Threat Center; 2016.

[29] Rosenblat A, Kneese T, boyd d. "Workplace Surveillance", tech. rep., Open Society Foundations' Future of Work Commis sioned Research Papers; 2014.

[30] Liu L, De Vel O, Han QL, Zhang J, Xiang Y. "Detecting and Preventing Cyber Insider Threats: A Survey", IEEE Communications Surveys & Tutorials 2018.

[31] Bhuyan MH, Bhattacharyya DK, Kalita JK. "Network Anomaly Detection: Methods, Systems and Tools", IEEE Communications Surveys & Tutorials, vol. 16, no. 1, pp. 303-336, 2014.

[32] Buczak AL, Guven E. "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.

[33] Werlinger R, Hawkey K, Muldner K, Jaferian P, Beznosov K. "The Challenges of Using an Intrusion Detection System: Is It Worth the Effort?", In: Proceedings of the 4th Symposium on Usable Privacy and Security. ACM; pp. 107-118, 2008.

[34] A.S.Joshi, OmkarKulkarni, G.M.Kakandikar, and V.M.Nandedkar, "Cuckoo Search Optimization- A Review", Materials Today: Proceedings, vol.4, no.8, pp.7262-7269, 2017.

[35] T. Chen, Y. Zhu and J. Teng, "Beetle swarm optimisation for solving investment portfolio problems," in The Journal of Engineering, vol. 2018, no. 16, pp. 1600-1605, 11 2018.

[36] Homoliak I, Toffalini F, Guarnizo J, Elovici Y, Ochoa M. "Insight Into Insiders and IT: A Survey of Insider Threat Taxonomies, Analysis, Modeling, and Countermeasures", ACM Computing Surveys, vol. 52, no. 2, pp. 30-40, 2019.