Adaptive Service Dependent Proximity Analysis Based Intrusion Detection in Cloud Environment

S. Priya
Department of Computer Science and Engineering,
School of Computing,
Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology,
Avadi, Chennai, India.

S. Jagan
Professor
Department of Computer Science and Engineering,
School of Computing,
Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology,
Avadi, Chennai, India.

Dr. S. P. Santhoshkumar,
Department of Computer Science and Engineering,
Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology,
Avadi, Chennai, India.
0000-0001-8531-759X

Abstract - **Intrusion attack is the most dominant threat faced by cloud environment, which targets the service behavior and QoS metrics. To handle such threats, number of approaches is defined in literature which works on data level, behavior level, and service level and so on. However, the methods face inclined performance in security as well as QoS achievement. To improve the precision of intrusion attack detection,an Adaptive Service Dependent Proximity Analysis (ASDPAM) based intrusion detection model is presented in this article. The proximity of threat against the services is the main focus in this approach. To perform this, the model starts with categorizing the services under various sensitive levels as the services would handle different data which are sensitive, highly sensitive, normal and moderate sensitive. By categorizing the services in this way, helps the model to define the threshold for the threat level and support the detection of intrusion attack. By receiving any service request, the model analyze the proximity of threat would be for the concern service request received. Using the service trace maintained, the model preprocesses the logs of service as well as user initially. Further, the method computes the User Threat Proximity Score (UTPS) for the service threat proximity Score (STPS). Considering the worth of UTPS and STPS the technique determines the intrusion attack. The suggested paradigm enhances intrusion attack detection performance and improves the QoS performance as well.**
Keywords - Intrusion Attack, Cloud Environment, Service Dependency, Proximity Analysis, ASDPA.

I. INTRODUCTION

The popularity of service orient architecture has grown to different extend at the arrival of cloud environment. Unlike earlier days, the organizations are more comfortable in maintaining their data in cloud with more accessibility. The cloud environment provides different services for their customers and users through which the data or any resource in cloud can be accessed. This makes the environment as loosely coupled one and more

prone for threats. The malformed users target the services in a way that lowers performance. To perform their scope, number of threats is generated by the malicious users. Intrusion attacks are the most common of them,which tries to steal the data by intruding in to the environment. The malicious access with intrusion has been mitigated by the environment by enforcing different access restriction methods. The access restriction in cloud is adapted in different levels like service, data and resource. Also, the data security is enforced by using various encryption methods to safeguard the data as well as resources. However, the adversaries are more successful in producing intrusion attack which must be considered with more attention.

Service dependency is a metric which focus on enforcing rigid access measures to secure the service access towards achieving higher QoS metrics. Any service would have specific task and it would access different features of a data. So, it is necessary to enforce rigid security in accessing the service and they need to be categorized under various groups according to various factors. By categorizing such services, different security measures can be adapted.

On the other side, even the registered user would access the services in wrong way by placing malicious or wrong data which is not related to the service protocol. That may be submitted mistakenly and cannot be directly classified as malicious threat. In this case, the proximity of the service must be considered. The services which are classified as sensitive and which are accessing more sensitive data must be given least proximity where the services accessing generic data can be given higher proximity. By classifying the service request and actions of the user according to the service and the proximity of the service, It is possible to detect the existence of an intrusion attack.

This article focused on designing an efficient adaptive service dependent proximity analysis model (ASDPAM) for the detection of intrusion attack. The method assesses the user trust in terms of accessing the service according to the trace being preserved. Using the trace the model would analyze the proximity of the service and user to classify the request.

II. LITERATURE REVIEW

There exists number of approaches around the detection of intrusion attack in cloud environment. This section analyzes set of recent methods on their superiority and demerits.

In [1], a deep blockchain framework (DBF) for distributed intrusion detection using blockchain technology is introduced. The technique makes use of IoT networks and smart contracts. To detect intrusions, the method combines deep learning and BiLSTM. In order to protect cloud servers from various attacks, [2] presents an event-based approach that performs intrusion detection by tracking the network's overall attack rate. In [3], a deep neural network-based auto encoder-based intrusion detection system is introduced. It creates particular kinds of harmful samples using a CDAAE. The second model (CDAEE-KNN) combines the K-nearest neighbour method for attack detection with CDAAE. In [4], a fog-enabled intrusion detection method is given .It employs a genetic algorithm and a multi-objective optimization model to identify intrusion attacks. The classification process takes execution time and energy consumption into account. In [5], a trusted virtual intrusion detection system (TVIDS) that protects private data in accordance with upheld policies is introduced.

A fuzzy rough set-based intrusion detection scheme is presented in [6], which performs feature selection with a rough set and trains the (Convolution Neural Network) CNN to perform intrusion detection. A deep learning model is proposed to secure Dew Computing as a Service (DaaS) in EoT systems [7]. An AI-based approach is presented in [8] towards intrusion detection. The technique selects features using the Transient Search Optimisation (TSO) algorithm and classifies them using differential evolution (TSODE). A high-precision Intrusion Detection Classification Model (IDCM) is presented in [9], which generates a k-dependency Bayesian network (KDBN) structural model toward classification. Adaptive Virtual Machine (AVM) Shield towards security is presented in [10], which uses system call features with an n-gram approach to perform classification with binary particle swarm optimization.

In [11], present virtual machine introspection (VMI) towards monitoring granular attacks in system calls.

In [12], an effective method for managing a range of attacks is created, which keeps an eye on the devices for attacks and their frequency. In accordance with that, threat detection is carried out and the issue is resolved. [13] presents an Auto IF-based method that selects features using Isolation Forest and extracts features using the deep learning Auto Encoder algorithm. Moreover, binary classification is carried out by the approach based on the chosen features.

In [14], a fuzziness-based semi-supervised learning technique for intrusion detection is introduced, which uses the labelled data to create the ensembles. In categorization, the fuzziness-based technique is applied. In [15], an intelligent intrusion detection method for Dew Computing as a Service (DaaS) in EoT ecosystems is introduced. Deep belief networks are used in the classification process. In [16], a safe method for separating rogue nodes based on real-time transmission characteristics is introduced.A CNN-based feature extraction method that also modifies the transient search optimization (TSO) for feature selection is introduced in [17]. The differential evolution

algorithm is used in classification via the TSODE method. In order to perform categorization, [18] presents a multi-level intrusion detection technique that carries out intrusion detection at several stages. Random forest is used for categorization in [19], which presents an IDS for IIoT based on genetic algorithms. For feature selection, the genetic algorithm is employed. VMShield, an introspection-based security technique that makes use of runtime process behaviour [20]. The technique uses PSO and random forest classifiers to detect intrusion attacks and extracts features from system calls. Deep IFS, a deep learning model based on forensics, is introduced to combat intrusion attacks inIIoT traffic.

III. ADAPTIVE SERVICE DEPENDENT PROXIMITY ANALYSIS BASED INTRUSION DETECTION MODEL

The proposed ASDPAM model reads the data taxonomy and service taxonomy initially, which has been used to categorize the services under various sensitive levels as the services would handle different data which are sensitive, highly sensitive, normal and moderate sensitive. By categorizing the services in this way, helps the model to define the threshold for the threat level and support the detection of intrusion attack. By receiving any service request, the model analyze the proximity of threat would be for the concern service request received. Using the service trace maintained, the model preprocesses the logs of service as well as user initially. Further, the method computes the User Threat Proximity Score (UTPS) for the service threat proximity Score (STPS). The technique determines the intrusion assault based on the values of UTPS and STPS.

This section describes the functional architecture of the proposed ASDPAM model in detail, with Figure 1 showing the model's functional architecture.

Preprocessing:

The model utilizes the data taxonomy and service taxonomy to categorize the services. To perform this, using both the taxonomy, the method identifies each service and for each of them the method finds the set of features being accessed. According to the details discovered, the method computes the Highly Sensitive Score (HSS), Moderate Sensitive Score (MSS) and Generic Score (GS). According to the value of HSS, MSS and GS, the method categorize the service to support proximity analysis.

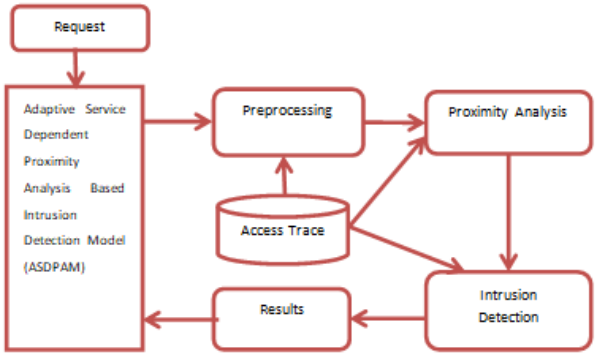

Figure 1: Architecture of ASDPAM Model

IV. PROXIMITY ANALYSIS

The proximity of the service threat that was created in the past is examined by the proximity analysis technique. The technique reads the service trace and splits it into distinct time stamps in order to accomplish this. At each time stamp, numbers of threats received by various users are counted and numbers of threats classified as intrusion attack are counted. Using both these values, the average of proximity threshold is measured. Such measured proximity threshold has been used to perform intrusion detection.

Algorithm:
Input: Service Trace SeTr, Service S
Output: Proximity Threshold PT.
Start
Read SeTr and S.
Find time stamps Tss = $\left(\sum_{i=1}^{size(SeTr)} SeTr(i).Time \ni Tss\right) \cup Tss$
For each time T

Collect Service Trace ST = $\sum_{i=1}^{size(SeTr)} SeTr(i).Service == S$

Compute Threat Rate Tr = ■$(Size(ST)@Count(ST(i).State == Threat)@i = 1) / (Size(ST))$

Compute Classification Rate Cr = ■$(Size(ST)@Count(ST(i).State == Threat\&\&ST(i).Class == Threat)@i = 1) / (Size(ST))$

Compute Proximity Threshold PrT = $\frac{Cr}{Tr}$

End

Compute PT = $\frac{\sum PrT}{size(Tss)}$

Stop

The above discussed algorithm computes the proximity threshold of the service given to support intrusion detection.

V. INTRUSION DETECTION

The proposed model reads the service traces and applies preprocessing to categorize the services. Further for each of the service, the method applies proximity analysis to measure the proximity threshold for the service. With this, the method receives the user request and computes User Threat Proximity Score (UTPS) for the service threat proximity Score (STPS). The technique determines the intrusion assault based on the values of UTPS and STPS.

Algorithm:
Given: Service Trace SeTr, Service Taxonomy ST, Data Taxonomy DT
Obtain: Null
Start
    Read SeTr, ST, DT.
    Service Set Ss = Perform Preprocessing (ST, DT)
    For each service set ss_i
        For each service s
            PT = perform Proximity Analysis (SeTr, s)
        End
    End
    While true
        Receive user request Req.
        Identify service S= Req.Service
        Identify user U = req.user
    Compute UTPS = ■$(Size(SeTr)@Count(SeTr(i).State == Threat\&\&SeTr(i).User == U)@i = 1) / (Size(SeTr))$
    Compute STPS = ■$(Size(SeTr)@Count(SeTr(i).State == Threat\&\&SeTr(i).User == U\&\&SeTr(i).Service == S)@i = 1) / Size(SeTr)$
    Compute Inclination Trust IT = $\frac{UTPS}{STPS}$
        If IT>Th and STPS>ss(s).PT then
            Declare threat
        End
    End
Stop

The above method computes UTPS and STPS values to measure IT value which has been used to decide according to the value of proximity threshold of the service.

VI. FINDINGS AND CONVERSATION

The performance of the suggested ASDPAM model has been tested across a range of simulation scenarios. In every instance, the method's effectiveness has been contrasted with the outcomes of alternative approaches.

Table 1: Evaluation Details

Parameter	Value

Tool Used	Python
Data Set	Amazon
Platform	Microsoft Azure
Number of Records	1 million
Number of Services	100
Number of Users	5000

The constraints considered for the evaluation of proposed approach is shown in Table 1. The methods are evaluated for their performance on the following factors:

Table 2: Analysis on intrusion detection accuracy

Intrusion Detection Accuracy %			
No of Records	3 Lakhs	5 Lakhs	10 Lakhs
GA-RF	69	74	79
VMShield	73	77	82
Deep-IFS	79	85	87
ASDPAM	91	95	99

Table 2 presents the measured effectiveness of several ways in detecting intrusion assault. Compared to existing models, the suggested ADSPAM model improves intrusion detection accuracy.

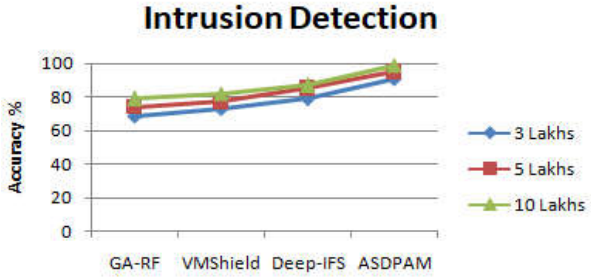

Figure 2: Analysis on intrusion detection accuracy

Figure 2 displays the approaches' estimated effectiveness in detecting intrusion attacks. Compared to previous models, the suggested ADSPAM model performs better in terms of intrusion detection accuracy.

Table 3: Analysis on False Ratio in intrusion detection

False Ratio in Intrusion Detection %			
Number of Records	3 Lakhs	5 Lakhs	10 Lakhs
GA-RF	31	26	21
VMShield	27	23	18
Deep-IFS	21	15	13
ADSPAM	9	5	1

Table 3 shows the false classification ratio, which was measured and shown to be lower for the suggested ADSPAM model than for the others.

Figure 3 shows the measured rate of false classification, with the suggested ADSPAM model producing a lower false rate than the others.

Table 4 measures and displays the time complexity in classification; the ADSPAM model has created less time complexity than the others.

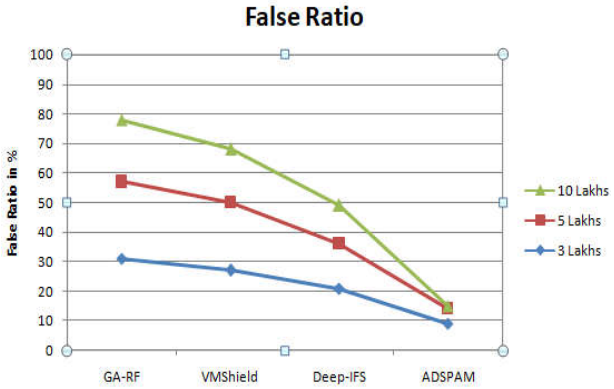

Figure 3: Analysis on False Ratio in intrusion detection

Table 4: Analysis on Time Complexity in intrusion detection

Time Complexity in Intrusion Detection in Seconds			
Number of Records	3 Lakhs	5 Lakhs	10 Lakhs
GA-RF	33	56	89
VMShield	28	43	78
Deep-IFS	25	35	67
ADSPAM	12	21	32

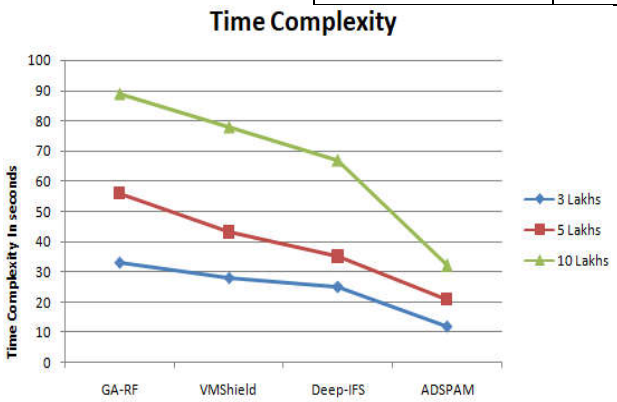

Figure 4: Analysis on Time Complexity in Intrusion detection

Figure 4 compares and measures the time complexity in classification; the ADSPAM model has attained a lower time complexity than the others.

VII. CONCLUSION

In order to identify intrusion attacks in cloud environments, this research introduced a novel Adaptive Service Dependent Proximity Analysis Based Intrusion Detection Model (ASDPAM). The model model reads the data taxonomy and service taxonomy initially, which has been used to categorize the services under various sensitive levels as the services would handle different data which are sensitive, highly sensitive, normal and moderate sensitive. By categorizing the services in this way, helps the model to define the threshold for the threat level and support the detection of intrusion attack. By receiving any service request, the model analyze the proximity of threat would be for the concern service request received. Using the service trace maintained, the model preprocesses the logs of service as well as user initially. Further, the method computes the User Threat Proximity Score (UTPS) for the service threat proximity Score (STPS). The technique determines the intrusion assault based on the values of UTPS and STPS. The suggested approach reduces temporal complexity while improving intrusion detection performance.

REFERENCES

[1]. O. Alkadi, N. Moustafa, B. Turnbull and K. K. R. Choo, "A deep blockchain framework-enabled collaborative intrusion detection for protecting IoT and cloud networks," in *IEEE Internet of Things Journal,* vol. 8, no. 12, pp. 9463-9472, 2021, doi: 10.1109/JIOT.2020.2996590.

[2]. M. Nadeem, A. Arshad, S. Riaz, S. S. Band and A. Mosavi, “Intercept the cloud network from brute force and DDoS attacks via intrusion detection and prevention system," in *IEEE Access,* vol. 9, pp. 152300-152309, 2021, doi: 10.1109/ACCESS.2021.3126535.

[3]. L. Vu, Q. U. Nguyen, D. N. Nguyen, D. T. Hoang and E. Dutkiewicz, “Deep generative learning models for cloud intrusion detection systems,” in *IEEE Transactions on Cybernetics,* vol. 53, no. 1, pp. 565-577, 2023, doi: 10.1109/TCYB.2022.3163811.

[4]. Mourad, H. Tout, O. A. Wahab, H. Otrok and T. Dbouk, “Ad Hoc vehicular fog enabling cooperative low-latency intrusion detection,” in *IEEE Internet of Things Journal,* vol. 8, no. 2, pp. 829-843, 2021, doi: 10.1109/JIOT.2020.3008488.

[5]. J. Wang, S. Hao, Y. Li, Z. Hong, F. Yan *et al.,* “TVIDS: Trusted virtual IDS with SGX,” in *China Communications,* vol. 16, no. 10, pp. 133-150, 2019, doi: 10.23919/JCC.2019.10.009.

[6]. Y. Wu, L. Nie, S. Wang, Z. Ning and S. Li, “Intelligent intrusion detection for internet of things security: A deep convolutional generative adversarial network-enabled approach,” in *IEEE Internet of Things Journal,* vol. 10, no. 4, pp. 3094-3106, 2023, doi: 10.1109/JIOT.2021.3112159.

[7]. P. Singh, A. Kaur, G. S. Aujla, R. S. Batth and S. Kanhere, “DaaS: dew computing as a service for intelligent intrusion detection in edge-of-things ecosystem,” in *IEEE Internet of Things Journal,* vol. 8, no. 16, pp. 12569-12577, 2021, doi: 10.1109/JIOT.2020.3029248.

[8]. H. Yin, M. Xue, Y. Xiao, K. Xia and G. Yu, “Intrusion detection classification model on an improved k-dependence bayesian network,” in *IEEE Access,* vol. 7, pp. 157555-157563, 2019, doi: 10.1109/ACCESS.2019.2949890.

[9]. P. Mishra, P. Aggarwal, A. Vidyarthi, P. Singh, B. Khan *et al.*, “VMShield: Memory introspection-based malware detection to secure cloud-based services against stealthy attacks,” in *IEEE Transactions on Industrial Informatics,* vol. 17, no. 10, pp. 6754-6764, 2021, doi: 10.1109/TII.2020.3048791.

[10]. P. Mishra, V. Varadharajan, E. S. Pilli and U. Tupakula, "VMGuard: A VMI-Based Security Architecture for Intrusion Detection in Cloud Environment," in IEEE Transactions on Cloud Computing, vol. 8, no. 3, pp. 957-971, 1 July-Sept. 2020, doi: 10.1109/TCC.2018.2829202.

[11]. M. Nadeem, A. Arshad, S. Riaz, S. S. Band and A. Mosavi, "Intercept the Cloud Network From Brute Force and DDoS Attacks via Intrusion Detection and Prevention System," in IEEE Access, vol. 9, pp. 152300-152309, 2021, doi: 10.1109/ACCESS.2021.3126535.

[12]. K. Sadaf and J. Sultana, "Intrusion Detection Based on Autoencoder and Isolation Forest in Fog Computing," in IEEE Access, vol. 8, pp. 167059-167068, 2020, doi: 10.1109/ACCESS.2020.3022855.

[13]. Y. Gao, Y. Liu, Y. Jin, J. Chen and H. Wu, "A Novel Semi-Supervised Learning Approach for Network Intrusion Detection on Cloud-Based Robotic System," in IEEE Access, vol. 6, pp. 50927-50938, 2018, doi: 10.1109/ACCESS.2018.2868171.

[14]. P. Singh, A. Kaur, G. S. Aujla, R. S. Batth and S. Kanhere, "DaaS: Dew Computing as a Service for Intelligent Intrusion Detection in Edge-of-Things Ecosystem," in IEEE Internet of Things Journal, vol. 8, no. 16, pp. 12569-12577, 15 Aug.15, 2021, doi: 10.1109/JIOT.2020.3029248.

[15]. Thiagarajan, R., Ganesan, R., Anbarasu, V. , M. Baskar., K. Arthi.,J. Ramkumar., Optimised with Secure Approach in Detecting and Isolation of Malicious Nodes in MANET. *Wireless Pers Commun* (2021). https://doi.org/10.1007/s11277-021-08092-0.(SCI)

[16]. Fatani, M. Abd Elaziz, A. Dahou, M. A. A. Al-Qanessand S. Lu, "IoT Intrusion Detection System Using Deep Learning and Enhanced Transient Search Optimization," in IEEE Access, vol. 9, pp. 123448-123464, 2021, doi: 10.1109/ACCESS.2021.3109081.

[17]. K. Bala, A.ChandraSekar, M. Baskar, J. Paramesh, An Efficient Multi Level Intrusion Detection System for Mobile Ad-Hoc Network Using Clustering Technique, International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-8 Issue-6, August, 2019, 1977-1985.

[18]. S. M. Kasongo, "An Advanced Intrusion Detection System for IIoT Based on GA and Tree Based Algorithms," in IEEE Access, vol. 9, pp. 113199-113212, 2021, doi: 10.1109/ACCESS.2021.3104113.

[19]. P. Mishra et al., "VMShield: Memory Introspection-Based Malware Detection to Secure Cloud-Based Services Against Stealthy Attacks," in IEEE Transactions on Industrial Informatics, vol. 17, no. 10, pp. 6754-6764, Oct. 2021, doi: 10.1109/TII.2020.3048791.

[20]. M. Abdel-Basset, V. Chang, H. Hawash, R. K. Chakrabortty and M. Ryan, "Deep-IFS: Intrusion Detection Approach for Industrial Internet of Things Traffic in Fog Environment," in IEEE Transactions on Industrial Informatics, vol. 17, no. 11, pp. 7704-7715, Nov. 2021, doi: 10.1109/TII.2020.3025755.