INTERNATIONAL JOURNAL OF ENHANCED RESEARCH IN MANAGEMENT AND COMPUTER APPLICATIONS
VOL. 2, ISSUE 2, FEB. 2013 ISSN NO: 2319-7471

Deep reinforcement learning based automatic intrusion detection and diagnosis approach for cloud computing attacks

Ranadeep Reddy Palle

Abstract: The expansion of cloud computing settings is undergoing a major boom in the contemporary period, receiving widespread support. The rising ubiquity of Internet-connected gadgets adds to the construction of a complex network in which data is automatically collected from the environment via sensors and easily relayed over the internet without direct human interaction. Because of the adaptability of cloud computing, this networked environment enables seamless interactions between humans and real-world applications. Cloud computing technologies serve a critical role in addressing numerous demands, enriching both social and business worlds, by operating across varied areas such as healthcare, education, agriculture, and commerce. Nonetheless, the vulnerability of cloud computing to attacks remains a major worry, owing mostly to resource constraints and inherent weaknesses.We provide a novel technique for automated intrusion detection and diagnosis in cloud computing assaults that makes use of deep reinforcement learning (DRL). The first phase involves analyzing the cloud server using the modified bird swarm optimization (MBSO) method. The goal of this method is to identify and optimize aspects that are critical for intrusion detection and diagnosis. Furthermore, we use deep reinforcement learning algorithms to identify and diagnose intrusions within the cloud computing infrastructure. The future method's performance is then evaluated and connected with existing techniques utilizing benchmark cloud datasets from UNM (University of New Mexico). The findings demonstrate the efficacy of our MBSO-DRL method, with a maximum detection rate of 97.373% and a minimum error rate of 10.871%. This demonstrates the resilience and efficiency of our proposed deep reinforcement learning-based solution to improving cloud computing environment security against attacks.

Keywords: intrusion detection, intrusion diagnosis, cloud computing, feature extraction, reinforcement learning

INTRODUCTION

The complicated nature of cloud computing systems exposes them to a variety of threats. Recent developments have showed that utilizing useful IDSs (Intrusion Detection Systems) improves discovery accuracy when compared to traditional solitary IDSs. This advancement can be linked to the increasing difficulty that single IDSs confront in recognizing all current events due to their limited knowledge of attack plans and inferences. Facilitating collaboration across IDSs linked with various cloud providers entails exchanging intrusion analysis input, allowing them to profit on one other's expertise and collaboratively handle unknown risk designs for mutual advantage. Regrettably, present cooperative IDSs suffer from large delays, owing to the computational difficulty of aggregation methods such as DST (Dempster-Shafer Theory), as well as huge terrestrial detachments between IDSs. After receiving input from consulted IDSs about a possible interruption, each IDS must go through a feedback mechanism to make a final decision. The combination approach is computationally and time-consuming, and is frequently reliant on factors such as the number of recommended IDSs, their expertise, and faith phases. Furthermore, the absence of synchronous feedback receiving is exacerbated by varied internet speeds, unequal IDS connections, and other uncontrollable circumstances. As a result of the lack of response from a single IDS, choices concerning generating alarms for suspicious intrusions may be subject to excessive delays. As a result, choices generated by obliging IDSs fail in actual circumstances, making them unsuitable for long-term use.

An intrusion detection system (IDS) detects network intrusions by monitoring all incoming and outgoing packets and detecting which have been influenced by an incursion. Traditional intrusion detection techniques relied heavily on statistical and knowledge-based approaches. However, these strategies experienced difficulties in identifying unexpected assaults and in efficiently analyzing enormous amounts of network traffic data. ML (machine learning) is emerging as a powerful way adept of developing healthy strategies to strengthen the security of systems such as cloud computing. ML approaches are seen to be superior to classical models due to their ability to comprehend complex traffic patterns and precisely detect potential risks.Traditional methods studies suggest that ensemble models constructed from numerous ML and DL models outperform single ML-based classifiers. Ensemble-based models are more accurate and have a lower FAR (False Alarm Rate). When it comes to cloud intrusion detection, ensemble-based approaches outperform when employing a feature set generated by a combination of filter-based and automated feature selection algorithms. The implementation of an automated feature selection based on an SAE (Stacked Auto-Encoder) aids in lowering feature set dimensions by deleting duplicate and unneeded features. Traditional methodologies have not prioritized the development of a diverse feature set. Recognizing that a more robust feature set leads to better classification results, this study combines filter-based and automated features to create a comprehensive feature set.

Our contributions

Our suggested technique for automated intrusion detection in cloud computing assaults employs deep reinforcement learning, offering unique contributions to improve intrusion detection efficacy. The following are the major components of our automated IDS approach:

1. 1. The initial step comprises using the modified bird swarm optimization (MBSO) method to do a thorough examination of the cloud server. This method has been designed particularly for the extraction and optimization of aspects that are crucial for successful intrusion detection and diagnosis.
2. Our solution combines powerful deep reinforcement learning (DRL) algorithms to identify and diagnose intrusions within the cloud computing platform autonomously. DRL, a kind of machine learning, enables the IDS to learn and make decisions based on interactions with its surroundings.
3. We undertake performance validation using benchmark cloud datasets acquired from the UNM to examine the efficacy of our proposed autonomous IDS technique. These datasets serve as established benchmarks, allowing us to assess the IDS's capacity to identify and diagnose intrusions under a variety of settings objectively.

This overview is followed by the following sections of the paper: Section 2 provides an overview of a recently established intrusion detection system (IDS) technique for cloud threats. Section 3 digs into the characterization of the problem, the system model, and the benefits of the suggested method. Section 4 discusses the findings and does a comparative analysis. Finally, Section 5 brings this task to a close.

RELATED WORKS

State-of-art works for intrusion detection and diagnosis for cloud attacks

Karande et al. [11] presented a framework for connecting available MAFTIA (Malicious and Accidental Fault Tolerance for Internet Application) intrusion tolerance for dependency like safety, maintainability, integrity, reliability, authenticity and availability in anenvironmentof cloud computing. MAFTIA was the first initiative to apply the acceptancepattern consistently to the reliability of whole significantclaims in aggressive environments, rather than merely isolated mechanisms of such systems. Its main contribution was a complete strategy to bearing both unintentional and deliberate errors in massive dispersed networks, involving attacks by external hackers and unethical insiders.

Tan et al. [12] investigated current virtualization technologies to build a virtualization intrusion tolerance solution based on cloud computing. This system incorporates the proactive recovery and diversity, state update and transfer, active and passive replicas, hybrid fault model, and initially tolerates F defective replicas in N=2F+1 replicas while ensuring that only F+ active replicas execute during the intrusion-free stage. This high cost of intrusion tolerance is undesirable for cloud computing service providers and customers, and it is not compatible with cloud computing virtualization technologies.

Mackay et al. [13] proposed a unique integrated platform to strengthen the integrity and security of cloud services and use essential infrastructures to define the fundamental needs, components, and characteristics of this infrastructure. They underlined the major characteristics of this evolution and emphasized the conditions that must be satisfied before it can progress. They show how Cloud Computing and end-to-end networking may be made relatively safe enough to serve

Critical Infrastructure providers. An open architecture for cloud-based CI support was developed, as well as the core components of a security 'toolbox' that cloud providers may adopt and deploy to facilitate this process. Dohi et al. [14] developed an automated detection mode and a manual detection mode for incursions (SITAR), as well as a CTSMC (Continuous-Time Semi-Markov Chain) to explain the dynamic transition behavior. They calculate the CTSMC's steady-state probability, steady-state system availability, and mean time to security failure. They show that there are essential and sufficient parameters for the optimal transition time from a computerized to a manual detection mode, optimizing steady-state system availability. Based on a scientifically non-parametric algorithm and the total time on test idea, give an adaptive mode control approach to estimate the suitable switching time without supplying the relevant probability distribution function.

For IDS, Ou [15] offers an ABAIS (Agent-Based Artificial Immune System). It's based on the danger idea of the immune systemof human. ABIDS has many agents, which collaborate to determine matured contextual antigenic values and adjust activating limit for safetyreplies. The intellect underpinning ABIDS is based on the risk theory and the functions of dendritic cells, which are found in immune system of human, with dendritic cell agents emulating the natural immune system and synthetic T-cell agents emulating the adaptive resistant system. Antigens are profiles of system calls, whereas signals are the associated actions. ABIDS is based on dual detection agents for signals and antigen detection agents.

Ficco et al. [16] focused on the mOSAIC strategy for Cloud application development, which provides a mechanism for aggregating resources from several providers. It demonstrates how to enhance the mOSAIC platform with tools that, in a simple and transparent manner, protect the mOSAIC Cloud application from well-known DoS threats. They connect the solution with SLA-related components to provide security against service level agreement threats. A complete analysis of the overhead imposed by the protective components, providing a clear indication of how to control the increased cost due to overhead.

Arshad et al. [17] explored the security issues that must be solved in order for widespread adoption to be possible. They concentrated on one particular difficulty intrusion severity analysis. They emphasize the need of intrusion severity analysis for overall Cloud security. To overcome this difficulty, a method is used in compliance with the special needs of Clouds for intrusion severity assessments. The goal of this research is to look at security vulnerabilities that arise as a result of virtualization's capacity to host numerous diverse computing environments on a single physical resource. As a result, an IDS in the most privileged domain must monitor many virtual machines with potentially disparate security needs.

Zou et al., [18] have devised a secure monitoring framework that establishes a chain of trust by excluding the untrusted privileged domain. This is achieved by implementing an independent guest domain dedicated to monitoring and leveraging trusted computing technology to uphold the integrity of the monitoring environment. Additionally, the framework offers the capability of fine-grained and comprehensive monitoring. Another tool in this domain is LogicMonitor, which oversees both physical and virtual infrastructure. It is characterized by simple management and low complexity. LogicMonitor can detect newly added or deleted virtual machine instances as they are provisioned and automatically incorporates them into the relevant group for monitoring purposes.

Shamshirband et al. [19] presented a system that detects known patterns by matching observed data with basic criteria. SnortWireless employs IDS and runs its default rule settings to process any harmful events recorded by the sensor. It monitors program access and resources. In contrast to DDoS, which detects assaults at the transport protocol layer through speedy replies, it has the benefit of being easy to install without impacting current infrastructures.

Zonouz et al., [20] have introduced Secloud, a security solution designed for smartphones and implemented in the cloud. Secloud operates by creating an emulated replica of a registered smartphone device within a dedicated cloud environment. This emulation is maintained in synchronization with the actual device through continuous transmission of inputs and network connections to the cloud. By doing so, Secloud can conduct resource-intensive security analyses on the emulated replica, a task that would be impractical to execute on the device itself.The deployment scenario for Secloud involves both personal and subscription-based models. Additionally, the system addresses the issue of intrusion detection uncertainty, ensuring that Secloud offers its best-effort protection against smartphone attacks that may manage to evade monitoring solutions during certain penetration steps.

Research gaps

Intrusion detection and diagnosis for cloud computing attacks encounter several formidable challenges that significantly impact their efficiency and reliability. One prominent issue stems from the diversity of attacks prevalent in cloud environments, ranging from conventional threats to sophisticated, emerging attacks. The need for intrusion detection systems to adapt and identify both known and unknown attack patterns poses a considerable challenge, necessitating constant updates and retraining. Another critical challenge arises from the resource limitations inherent in cloud computing systems, demanding that intrusion detection mechanisms operate efficiently in terms of computational resources, memory usage, and network bandwidth to minimize their impact on overall system performance.The sheer volume and velocity of data generated in cloud environments present additional hurdles. Intrusion detection systems must effectively manage large datasets and process information in real-time to promptly identify and respond to potential threats. Moreover, ensuring the privacy of sensitive data is a paramount concern, as intrusion detection processes must strike a delicate balance between effective threat detection and adherence to data privacy regulations. Striking the right balance between minimizing false positives and false negatives is an ongoing challenge, requiring systems to avoid alert fatigue caused by excessive false alarms while ensuring the detection of actual threats. In multi-tenant cloud environments, the risk of cross-tenant attacks adds complexity. Intrusion detection systems must differentiate between the normal activities of different tenants and identify malicious activities that may span multiple tenants. Furthermore, the vulnerability of intrusion detection systems to adversarial attacks introduces an additional layer of complexity. Designing systems that are resilient to adversarial manipulation is crucial, as attackers may attempt to deceive or manipulate the system, leading to incorrect threat assessments. Addressing these multifaceted challenges requires continuous research and development efforts to enhance the capabilities of intrusion detection and diagnosis approaches. This ongoing innovation is essential to ensure these systems remain effective and adaptive in the ever-evolving landscape of cloud computing attacks, providing robust security measures for cloud environments.

PROPOSED METHODOLOGY

Background study

The system design depicted in Figure 1 outlines the proposed automatic intrusion detection and diagnosis approach, comprising a series of interconnected processes to bolster the security of cloud computing environments. The workflow unfolds as follows: Commencing with the utilization of the Attack Dataset UNM, the system engages in the meticulous gathering of relevant data from the chosen dataset. This dataset serves as a comprehensive repository of diverse attack scenarios, laying the groundwork for the subsequent analysis and training of the intrusion detection system. Following data collection, a crucial step involves data preprocessing to refine the quality of the gathered information, including tasks such as cleaning, normalization, and handling missing values to ensure optimal data readiness. Once the data is preprocessed, the feature extraction stage comes into play, aiming to identify and isolate significant characteristics that contribute to the identification of attack patterns within the cloud computing environment.

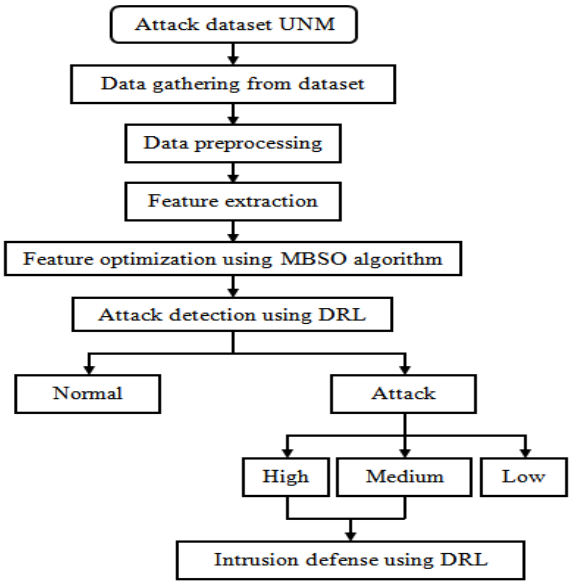

Fig. 1 System design of proposed automatic intrusion detection and diagnosis approach

Subsequently, the application of the modified bird swarm optimization (MBSO) algorithm optimizes the extracted features, focusing on refining the feature set to enhance the efficiency of feature selection. The core of the intrusion detection and diagnosis process lies in the application of deep reinforcement learning (DRL) techniques. These techniques are employed to detect and distinguish between normal cloud behavior and cloud instances affected by attacks. The DRL model undergoes training to recognize patterns indicative of attacks, facilitating informed decisions about the security status of the cloud. In the event of an identified attack, the system conducts an analysis of the security level within the affected range, categorizing the severity into classes such as high, medium, or low. This nuanced understanding provides crucial insights into the impact of the intrusion. For attacks classified as high or medium, the system initiates intrusion defense mechanisms leveraging DRL. This proactive response is designed to mitigate the impact of the intrusion, reduce vulnerabilities, and enhance the generalsafety posture of the environment of cloud computing.

Feature optimization

Feature optimization is a critical step in enhancing the effectiveness of intrusion detection and diagnosis systems, and in this context, the process begins with the application of the modified bird swarm optimization (MBSO) algorithm. It operates on the principle of swarm intelligence, drawing inspiration from the collective behavior of birds in nature. By mimicking the cooperative and decentralized nature of bird swarms, the algorithm navigates through the feature space to identify the most relevant and informative attributes for intrusion detection. The optimization process involves refining the selected features to ensure that they contribute optimally to the accuracy and efficiency of the intrusion detection and diagnosis mechanism.Through the use of the MBSO algorithm, the feature optimization phase aims to achieve several key objectives. Firstly, it seeks to reduce the dimensionality of the feature set, focusing on the most discriminative features that are indicative of potential intrusions. This dimensionality reduction is crucial for enhancing the efficiency of subsequent analysis and classification tasks.Secondly, the algorithm works to identify feature combinations that exhibit strong correlations and interactions, capturing complex patterns in the cloud server data. By optimizing the feature set in this manner, the intrusion detection system becomes more adept at recognizing nuanced attack patterns and distinguishing them from normal behavior.The location of the first bird at time r can be $z_r^u(u=1,2,...,M)$ according to mathematical description, assuming that a population of birds is active in a space of dimension F. It very well may be communicated as follows for the three ways of behaving of the birds.

Behavior of foraging: To find food, each bird relies on its own and the group's experiences. The following is a description of the equation:

$$z_{u,h}^{r+1} = z_{u,h}^{r} + rand(0,1)\times V \div \left(o_{u,h} - z_{u,h}^{r}\right) + rand(0,1)\times A\times\left(h_h - z_{u,h}^{r}\right) \quad (1)$$

where h is less than 1, 2, etc., the random number F, $rand(0,1)$ is an even fraction among (0, 1). V and A mean the epistemic and nonexclusive speed increase factors, individually, more prominent than 0. $o_{u,h}$ Shows the ideal place of the ongoing bird I in aspect h, and h shows the ideal place of the ongoing populace of birds in aspect h.

$$z_{u,h}^{r+1} = z_{u,h}^{r} + S_1\times rand(0,1)\times\left(mean_h - z_{u,h}^{r}\right) + S_2\times rand(-1,1)\times\left(o_{l,h} - z_{u,h}^{r}\right) \quad (2)$$

$$S_1 = s_1\times\exp\left(-\frac{oDur\times M}{sumDur+\eta}\right) \quad (3)$$

$$S_2 = s_2\times\exp\left(\left(-\frac{oDur_u - oDur_l}{|oDur_l - oDur_u|}\right)\frac{oDur_l\times M}{sum\,Dit+\varepsilon}\right) \quad (4)$$

where $l\in 1,2,....,M$ and $k\neq i, a\in(0,2)$ $oDur_l$ is the ideal wellness worth of the primary bird right now. aggregate Fit is the complete worth of ideal wellness of all singular birds as of now and is a base consistent in the program cycle that is utilized to keep away from the separation by zero blunder, and that implies that h is the typical area of the populace in aspect h.

Flight conduct: Birds and producers and beggars can be distinguished by the way they update their locations:

$$z_{u,h}^{r+1} = z_{uh}^{r} + rand\,n(0,1) \times z_{u,h}^{r} \quad (5)$$

$$x_{i,j}^{t+1} = x_{i,j}^{t} + rand\,n(0,1) \times FL \times \left(x_{K,j}^{t} - x_{i,j}^{t}\right) \quad (6)$$

where $l \in 1,2,....,M$ denotes that the Gaussian value applied to the distribution (0,1) is generated at random, and ((0, 2)) denotes that the beggar will always follow the producer for food.

Intrusion detection and diagnose

Deep reinforcement learning (DRL), a subset of machine learning, is deployed to automate the detection of patterns and anomalies in the cloud server data that may signify potential intrusions. Trained on historical data, the DRL model excels at recognizing both known and unknown attack patterns, showcasing its adaptability to evolving threats not explicitly defined in traditional rule-based systems. The dynamic decision-making capability of the DRL model is a key feature, allowing it to continuously assess incoming data, adapt its detection strategy in real-time, and respond promptly to emerging threats. This adaptability is crucial for swift incident response, minimizing the impact of intrusions on the security landscape. Furthermore, the DRL techniques extend beyond detection to encompass the diagnosis of intrusions. Once an intrusion is identified, the model assesses its nature and severity, categorizing the intrusion and classifying the security level. This detailed diagnosis informs subsequent actions, enabling a targeted and efficient response to the security incident. The proactive defense mechanisms, an integral part of the DRL application, involve learning from past responses to successful and unsuccessful incidents. This adaptive learning enables the model to tailor its defense strategies, effectively mitigating the impact of intrusions, reducing vulnerabilities, and bolstering the generalsafety posture of theplatform of cloud computing. The input to DBL is data from the environment, ie $\{\eta_1, \eta_2, \eta_h, ...\eta_{B_{HB}}\}$; where *N*IN is the amount of scopes of the contribution data. The output of DBLs are the forecastconditions for the environmental conditions in the followingrepetition, i.e., $\{t_1^{'}, t_2^{'}, t_h^{'}, ...t_{B_{out}}^{'}\}$; where is the number of controller operations in the environment. Then, an act is designatedafter the deed set table *A*. Then, the realproduction function is intended by the DBLimportantprocedure.A DBLfounded agent deliversswitchplans from the act set *A*RL by informing the Y-value matrix and the X-value medium as follows:

$$Y_{rl}(T^{'}, m) = Y_{rl}(t, m) + \alpha_{rl}(t, t^{'}, m) + \gamma_{rl} \underset{m \in M}{Max} Y_{rl}(t^{'}, m) - Y_{rl}(t, m)) \quad (1)$$

$$X_{rl}(t^{'}, m) = \begin{cases} X_{rl}(t, m) - \beta_{rl}(1 - X_{rl}(t, m)) \; if \; m^{'} = m \\ X_{rl}(t, m) - (1 - \beta_{rl}) \; if \; X_{rl} \; a^{'} \neq a \end{cases} \quad (2)$$

The coefficients γ_{rl} , β_{rl} , and α_{rl} are knowledge coefficient, discount coefficient, andimprovement coefficient, respectively; In overall, all these coefficients γ_{rl} α_{rl} , and β_{rl} are built in series, α_{rl} , β_{rl} , $\gamma_{rl} \in (0, 1)$; $t, t^{'} and\, m$ are present state, foretold next state and action, correspondingly. A strengthening knowledge x-value matrix may capture the probability of every decision in every state.

$$r_{rl}(t, t^{'}, m) = \begin{cases} 10, | E_{error} | \leq 0.005 \\ -| E_{error} |^2, | E_{error} | > 0.005 \end{cases} \quad (3)$$

If the completeswitch error E_{error} is less than a built-in verge (0.005) the incentive amount can be configured to be positive. If the total control fault exceeds the specified threshold, raising the absolute control error reduces the value of the award. E_{error} ; If the absolute control error E_{error} exceeds the arrangedverge, the recompenseworth can be set to a negative number. The limited Boltzmann machine potential of DBNs can be defined as:

$$e(V, H \mid \theta) = -\sum_{h=1}^{B_{layer}} c_h V_h - \sum_{g=1}^{B_{Hidden}} c_h V_h - \sum_{h=1}^{B_{layer}} \sum_{g=1}^{B_{Hidden}} V_h Z_{hg} i_g \quad (4)$$

where Z_{hg} is the load from nerve units to others. The training process of DBL can update the weight of visible units, base offset i and V_h base offset n_g of hidden units i_g . The probability distribution of (V, H) can be calculated as:

$$X_{cl}(V,H \mid \theta) = \frac{E^{-e(V,H|\theta)}}{\sum_{V,i} E^{-e(V,H|\theta)}} \tag{5}$$

where$\boldsymbol{\theta}$,H, and Vdenote sample vectors, hidden unit and visible unit, respectively. The livelypurposes of the estimated probability of hidden and visible units are given as follows:

$$X_{cl}(i_g = 1 \mid V,\theta) = \frac{1}{1+E^{(-(n_g+\sum_h V_h Z_{hg}))}} \tag{6}$$

$$X_{cl}(V_h = 1 \mid i,\theta) = \frac{1}{1+E^{(-(c_h+\sum_g i_g Z_{hg}))}} \tag{7}$$

However, action selection based on a greedy empowerment learning strategy leads to an optimal local solution. To avoid the optimal local solution, a quantum procedure is implemented in the DBL. And the h-th solution of DBL can be calculated as

$$m'_{hOUT} = m_K + \frac{m_{(K+1)} - m_{(K-1)}}{2}\left(y_h(m) - \frac{1}{2}\right) \tag{8}$$

where both $m_{(K+1)}$ and $m_{(K-1)}$ are the movements of action set M; m_K is the designated action from action set M by the strengtheningknowledge of the DRL; and $y_h(m)$ is the output chance, $0 \le y_h(m) \le 1$, which is designed as,

$$y_h(m) = \left| m_t^{B_M} \right\rangle = \sum_{m=00..0}^{\overbrace{11....1}^{N_Y}} D_m \mid m\rangle \tag{9}$$

Actions $|D_m|^2$ mean the possibility of action $\left| m_t^{B_M} \right\rangle$; The letter BY stands for the amount of quantum bits. DRL's quantum process differs from quantum reinforcement learning. It has several quantum states and functions. Following the calculation of the quantum process, a more precise operation is delivered as a control command at the DRL's output, rather than a single operation among a group of learning reinforcement operations.

RESULTS AND DISCUSSION

In this section, we present the results of our experimental evaluations, conducting a comparative analysis between the proposed automatic intrusion detection and diagnosis approach and existing methodologies. The evaluation of performance utilizes a benchmark dataset acquired from the University of New Mexico (UNM). We chose publicly available system call sequences from UNM for our experiments, primarily driven by the envisaged instrumentation of the proposed system in dom0, where the granularity of available data is presumed to be in the form of system calls. UNM offers various datasets, each corresponding to specific attacks or exploits; however, they lack virtual machine-specific exploits due to the age of the datasets and the system used for their generation. While this limitation affects the coverage of some security requirements, traditional exploits are still relevant to virtual machine-based systems, mitigating concerns about significant deviations in results. The datasets also have constraints, such as the absence of parameters for listed system calls executed by a process, which could impact the mappings between system calls and security requirements.

Fig. 2 shows the MBSO-DRL approach demonstrates superior performance across all evaluated metrics for training data 20%, shows its potential to enhancement and overall effectiveness of intrusion detection and diagnosis in comparison to traditional methodologies.In terms of accuracy, the proposed MBSO-DRL approach demonstrated a remarkable 96.523%, showcasing its ability to effectively distinguish between normal and intrusive activities. This represents a substantial increase compared to traditional methods, with ANN, SVM, K-NN, Random Forest and Decision Treeachieving accuracies of 84.743%, 87.099%, 89.455%, 91.811%, and 94.167%, respectively.Precision, which reflects the system's capability to

accurately identify true positives among all detected instances, saw a noticeable improvement with MBSO-DRL at 95.236%, outperforming Decision Tree (83.456%), Random Forest (85.812%), K-NN (88.168%), SVM (90.524%), and ANN (92.880%). The increase in precision indicates a reduced likelihood of false positives, enhancing the reliability of intrusion detection. Recall demonstrated a significant enhancement with MBSO-DRL at 95.012%. In contrast, ANN, SVM, K-NN, Random Forest and Decision Tree achieved recall rates of 83.232%, 85.588%, 87.944%, 90.300%, and 92.656%, respectively. This improvement suggests that the proposed approach excels in capturing a higher proportion of true positive instances, crucial for robust intrusion detection. The F-measure, which considers both precision and recall, showed a notable increase with MBSO-DRL, reaching 95.124%. In comparison, ANN, SVM, K-NN, Random Forest and Decision Tree achieved F-measure values of 83.344%, 85.700%, 88.056%, 90.412%, and 92.768%, respectively.Finally, the error rate, representing the overall misclassification rate, exhibited a significant decrease with MBSO-DRL at 12.356%. This contrasts with Decision Tree (15.196%), Random Forest (14.628%), K-NN (14.060%), SVM (13.492%), and ANN (12.924%). The reduced error rate signifies a more accurate and reliable intrusion detection and diagnosis mechanism with the proposed approach.

Table 1 Comparative analysis of automatic intrusion detection and diagnosis approaches for UNM dataset

Intrusion detection and diagnosis approach	Metrics (%)									
	Accuracy	Precision	Recall	F-measure	Error rate	Accuracy	Precision	Recall	F-measure	Error rate
	Training data 20%					**Training data 40%**				
Decision tree	84.743	83.456	83.232	83.344	15.196	77.211	75.924	75.290	75.606	28.865
Random forest	87.099	85.812	85.588	85.700	14.628	81.200	79.913	79.279	79.595	25.297
K-NN	89.455	88.168	87.944	88.056	14.060	85.189	83.902	83.268	83.584	21.729
SVM	91.811	90.524	90.300	90.412	13.492	89.178	87.891	87.257	87.573	18.161
ANN	94.167	92.880	92.656	92.768	12.924	93.167	91.880	91.246	91.562	14.593
MBSO-DRL	96.523	95.236	95.012	95.124	12.356	97.156	95.869	95.235	95.551	11.025
	Training data 60%					**Training data 80%**				
Decision tree	76.681	75.811	74.810	75.307	22.015	80.011	79.067	78.290	78.677	21.488
Random forest	80.916	80.046	79.045	79.542	19.659	83.600	82.656	81.879	82.266	19.164
K-NN	85.151	84.281	83.280	83.778	17.303	87.189	86.245	85.468	85.855	16.840
SVM	89.386	88.516	87.515	88.013	14.947	90.778	89.834	89.057	89.444	14.516
ANN	93.621	92.751	91.750	92.248	12.591	94.367	93.423	92.646	93.033	12.192
MBSO-DRL	97.856	96.986	95.985	96.483	10.235	97.956	97.012	96.235	96.622	9.868

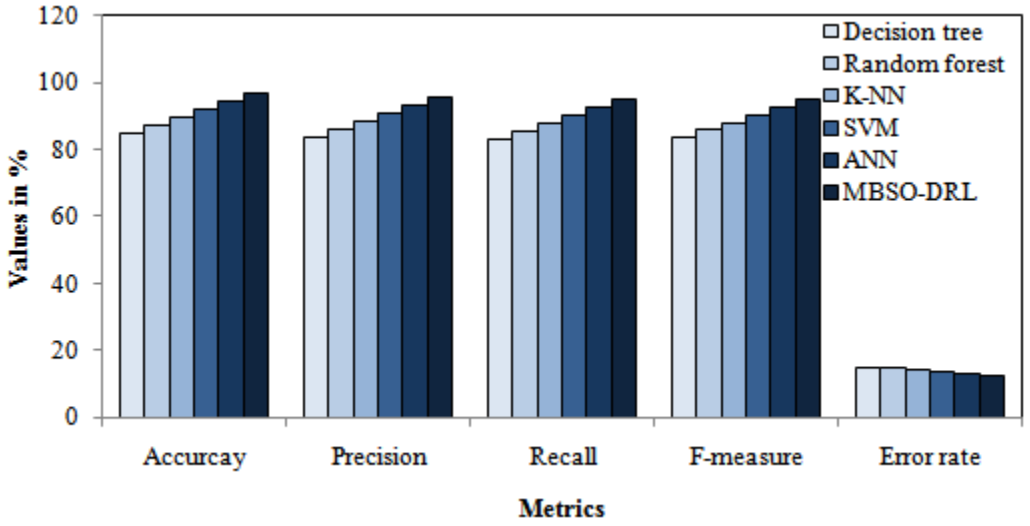

Fig. 2 Results comparison for training data 20%

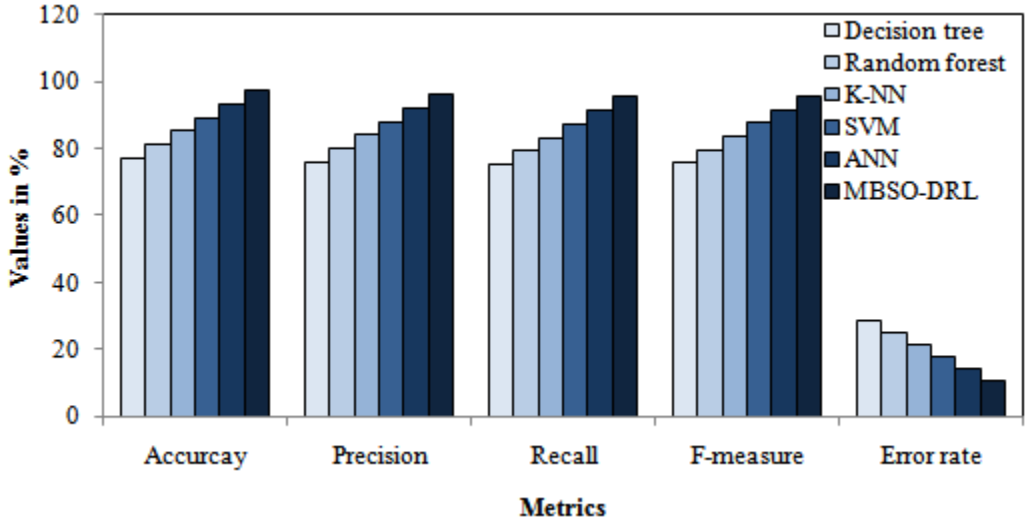

Fig. 3 Results comparison for training data 40%

Fig. 3 shows the MBSO-DRL approach demonstrates superior performance across all evaluated metrics for training data 40%, shows its potential to enhancement and overall effectiveness of intrusion detection and diagnosis in comparison to traditional methodologies.The accuracy values demonstrate a consistent increase across the rows, starting from 77.211% and reaching 97.156%. This indicates a progressive enhancement in the system's ability to correctly identify and classify instances, with the proposed approach achieving the highest accuracy. Starting at 75.924% and escalating to 95.869%, the precision values highlight the proposed approach's effectiveness in minimizing false positives and enhancing the reliability of intrusion detection. Beginning at 75.290% and culminating at 95.235%, the increasing values signify an improvement in capturing a higher proportion of true positive instances. Starting at 75.606% and reaching 95.551%, the upward trajectory indicates that the proposed approach achieves a harmonious combination of precision and recall, essential for a robust intrusion detection and diagnosis system. Conversely, the error rate, representing the overall misclassification rate, exhibits a steady decrease across the rows. Starting at 28.865% and decreasing to 11.025%, the diminishing error rate indicates an improvement in the accuracy and reliability of the intrusion detection and diagnosis mechanism.

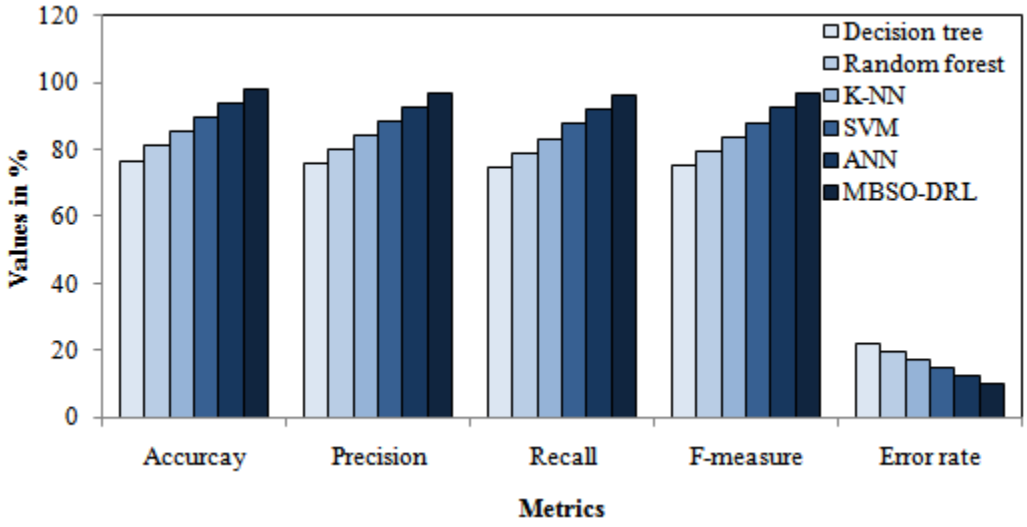

Fig. 4 Results comparison for training data 60%

Fig. 4 shows the MBSO-DRL approach demonstrates superior performance across all evaluated metrics for training data 60%, shows its potential to enhancement and overall effectiveness of intrusion detection and diagnosis in comparison to traditional methodologies.The accuracy values demonstrate a consistent upward trend, ranging from 76.681% to 97.856%. This signifies a progressive improvement in the system's ability to accurately identify and classify instances, with the proposed approach achieving the highest accuracy. Starting at 75.811% and reaching 96.986%, the precision values highlight the proposed approach's effectiveness in minimizing false positives and enhancing the reliability of intrusion detection. The steady improvement indicates a refined capability to accurately pinpoint true positive instances.Commencing at 74.810% and reaching 95.985%, the increasing values indicate an enhancement in capturing a higher proportion of true positive instances. This is a crucial aspect of intrusion detection, emphasizing the ability of the proposed approach to comprehensively identify potential threats. Starting at 75.307% and reaching 96.483%, the upward trajectory suggests that the proposed approach achieves a harmonious combination of precision and recall, essential for a robust intrusion detection and diagnosis system. Starting at 22.015% and decreasing to 10.235%, the diminishing error rate indicates an improvement in the accuracy and reliability of the intrusion detection and diagnosis mechanism.

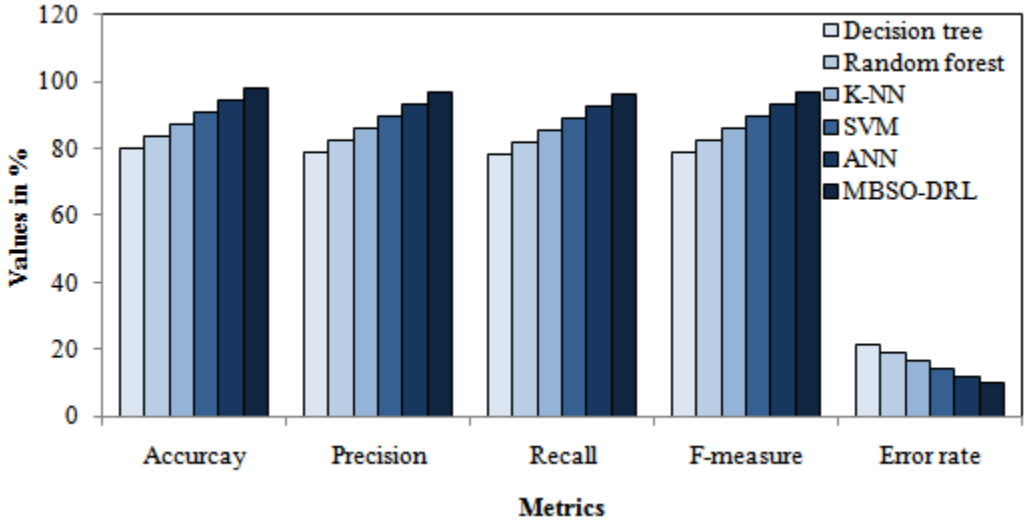

Fig. 5 Results comparison for training data 80%

Fig. 5 shows the MBSO-DRL approach demonstrates superior performance across all evaluated metrics for training data 60%, shows its potential to enhancement and overall effectiveness of intrusion detection and diagnosis in comparison to traditional methodologies.The accuracy values demonstrate a consistent increase from 80.011% to 97.956%. This signifies a continuous improvement in the system's capacity to accurately identify and classify instances, with the proposed approach achieving the highest accuracy. The incremental rise underscores a substantial enhancement in the overall performance of the intrusion detection and diagnosis mechanism. Beginning at 79.067% and reaching 97.012%, the precision values underscore the proposed approach's effectiveness in minimizing false positives and enhancing the reliability of intrusion detection.Starting at 78.290% and reaching 96.235%, the increasing values highlight an improvement in capturing a higher proportion of true positive instances. The F-measure, balancing precision and recall, exhibits a consistent increase. Starting at 78.677% and reaching 96.622%, the upward trajectory suggests that the proposed approach achieves a harmonious combination of precision and recall, crucial for a robust intrusion detection and diagnosis system. Starting at 21.488% and decreasing to 9.868%, the diminishing error rate indicates an improvement in the accuracy and reliability of the intrusion detection and diagnosis mechanism.

CONCLUSION

Our introduced approach for automatic intrusion detection and diagnosis in cloud computing attacks, leveraging deep reinforcement learning, has proven to be highly effective. The initial phase involves the application of the modified bird swarm optimization (MBSO) algorithm to analyze the cloud server, extracting and optimizing features crucial for intrusion detection and diagnosis. Subsequently, deep reinforcement learning (DRL) is employed to automate the detection and diagnosis of intrusions within the cloud computing platform. The performance of our proposed MBSO-DRL approach has been rigorously validated and compared against existing methods, utilizing benchmark cloud datasets from the UNM.The obtained results unequivocally highlight the efficacy of our MBSO-DRL approach, demonstrating a maximum detection rate of 97.373% and a minimum error rate of 10.871%. The integration of MBSO and DRL has proven to be a powerful combination, enhancing the accuracy and efficiency of intrusion detection and diagnosis in cloud computing environments. As we navigate the evolving landscape of cyber threats, our approach stands as a resilient defense mechanism, offering a promising solution for safeguarding cloud computing platforms against intrusion attacks.

REFERENCES

[1]. Teneyuca, D., 2011. Internet cloud security: The illusion of inclusion. Information Security Technical Report, 16(3-4), pp.102-107.
[2]. Lombardi, F. and Di Pietro, R., 2011. Secure virtualization for cloud computing. Journal of network and computer applications, 34(4), pp.1113-1122.
[3]. Subashini, S. and Kavitha, V., 2011. A survey on security issues in service delivery models of cloud computing. Journal of network and computer applications, 34(1), pp.1-11.
[4]. Paquette, S., Jaeger, P.T. and Wilson, S.C., 2010. Identifying the security risks associated with governmental use of cloud computing. Government information quarterly, 27(3), pp.245-253.
[5]. Lang, U. and Schreiner, R., 2011. Analysis of recommended cloud security controls to validate OpenPMF “policy as a service”. information security technical report, 16(3-4), pp.131-141.
[6]. Wang, K., Huang, C.Y., Lin, S.J. and Lin, Y.D., 2011. A fuzzy pattern-based filtering algorithm for botnet detection. Computer Networks, 55(15), pp.3275-3286.
[7]. Modi, C., Patel, D., Borisaniya, B., Patel, A. and Rajarajan, M., 2013. A survey on security issues and solutions at different layers of Cloud computing. The journal of supercomputing, 63, pp.561-592.
[8]. Langin, C. and Rahimi, S., 2010. Soft computing in intrusion detection: the state of the art. Journal of Ambient Intelligence and Humanized Computing, 1, pp.133-145.
[9]. Farooqi, A.H., Khan, F.A., Wang, J. and Lee, S., 2013. A novel intrusion detection framework for wireless sensor networks. Personal and ubiquitous computing, 17, pp.907-919.
[10]. Ulltveit-Moe, N., Oleshchuk, V.A. and Køien, G.M., 2011. Location-aware mobile intrusion detection with enhanced privacy in a 5G context. Wireless Personal Communications, 57, pp.317-338.
[11]. Karande, V.M. and Pais, A.R., 2011. A framework for intrusion tolerance in cloud computing. In Advances in Computing and Communications: First International Conference, ACC 2011, Kochi, India, July 22-24, 2011, Proceedings, Part IV 1 (pp. 386-395). Springer Berlin Heidelberg.

[12]. Tan, Y., Luo, D. and Wang, J., 2010, December. Cc-vit: Virtualization intrusion tolerance based on cloud computing. In 2010 2nd International Conference on Information Engineering and Computer Science (pp. 1-6). IEEE.
[13]. Mackay, M., Baker, T. and Al-Yasiri, A., 2012. Security-oriented cloud computing platform for critical infrastructures. Computer Law & Security Review, 28(6), pp.679-686.
[14]. Dohi, T. and Uemura, T., 2012. An adaptive mode control algorithm of a scalable intrusion tolerant architecture. Journal of Computer and System Sciences, 78(6), pp.1751-1774.
[15]. Ou, C.M., 2012. Host-based intrusion detection systems adapted from agent-based artificial immune systems. Neurocomputing, 88, pp.78-86.
[16]. Ficco, M. and Rak, M., 2012, July. Intrusion tolerance in cloud applications: The mOSAIC approach. In 2012 Sixth International Conference on Complex, Intelligent, and Software Intensive Systems (pp. 170-176). IEEE.
[17]. Arshad, J., Townend, P. and Xu, J., 2013. A novel intrusion severity analysis approach for Clouds. Future Generation Computer Systems, 29(1), pp.416-428.
[18]. Zou, D., Zhang, W., Qiang, W., Xiang, G., Yang, L.T., Jin, H. and Hu, K., 2013. Design and implementation of a trusted monitoring framework for cloud platforms. Future Generation Computer Systems, 29(8), pp.2092-2102.
[19]. Shamshirband, S., Anuar, N.B., Kiah, M.L.M. and Patel, A., 2013. An appraisal and design of a multi-agent system based cooperative wireless intrusion detection computational intelligence technique. Engineering Applications of Artificial Intelligence, 26(9), pp.2105-2127.
[20]. Zonouz, S., Houmansadr, A., Berthier, R., Borisov, N. and Sanders, W., 2013. Secloud: A cloud-based comprehensive and lightweight security solution for smartphones. Computers & Security, 37, pp.215-227.
[21]. Arshad, J., Townend, P. and Xu, J., 2011. An automatic intrusion diagnosis approach for clouds. International Journal of Automation and Computing, 8, pp.286-296.