Cloud Zero-Day Attack Detection Using Hidden Markov Model with Transductive Learning

Sohel Rana (✉ jsree041@gmail.com)

Nanjing University

Md Alamin Hossan

Daffodil International University

Abidullha Adel

Kunduz University

Research Article

Keywords: Zero-day attack, Transductive Deep Learning, Hidden Markov Model (HMM), Soft Labels, K-medoids clustering

Posted Date: November 2nd, 2021

DOI: <https://doi.org/10.21203/rs.3.rs-986849/v1>

License: © ⓘ This work is licensed under a Creative Commons Attribution 4.0 International License.

[Read Full License](#)

CLOUD ZERO-DAY ATTACK DETECTION USING HIDDEN MARKOV MODEL WITH TRANSDUCTIVE LEARNING

Correspondence author: Sohel Rana¹, Md Alamin Hossan², Abidullha Adel³

¹*Nanjing University of Information & Science Technology, China*

²*Daffodil International University*

Dhaka, Bangladesh

³*Assistant Professor at Kunduz University, Afghanistan*

Abstract

In cloud security, detecting attack software is considered an essential task. Among several attack types, a zero-day attack is considered as most problematic because the antivirus cannot able to remove it. The existing attack detection model uses stored data about attack characteristics, which fails to detect zero-attack where an altered attack is implemented for an antivirus system to detect the attack. To detect and prevent zero-day attacks, this paper proposed a model stated as Hidden Markov Model Transductive Deep Learning (HMM_TDL), which generates hyper alerts when an attack is implemented. Also, the HMM_TDL assigns labels to data in the network and periodically updates the database (DB). Initially, the HMM model detects the attacks with hyper alerts in the database. In the next stage, transductive deep learning incorporates k-medoids for clustering attacks and assign labels. Finally, the trust value of the original data is computed and computed in the database based on the value network able to classify attacks and data. The developed HMM_TDL is trained with consideration of two datasets such as NSL-KDD and CIDD. The comparative analysis of HMM_TDL exhibits a higher accuracy value of 95% than existing attack classification techniques.

Keywords: Zero-day attack, Transductive Deep Learning, Hidden Markov Model (HMM), Soft Labels, K-medoids clustering

1. Introduction

In recent years, organizations and enterprises put huge attention on their network security. However, the organization is subjected to a sustained and responsible approach to investment in defense mechanisms. This is due to security constraints, where attackers bypass their organization's security with unknown attacks. Even in a well-secured network, with persistent probing attackers are able to identify loopholes and perform attacks within the network [1]. The attackers were able to influence vulnerabilities for the configuration of the network through the network. Zero-day (0-day) is defined as vulnerable software or application that is either defined by the vendor or not patched by any vendor or organization. It is exploited that the targeted network gains entry of the actor threat [2]. In this manner, attackers or hackers gain access to sensitive information like data related to enterprises and legal documents. Through the identification of vulnerabilities in a zero-day attack success rate improves, which leads to Cybercriminal. Generally, vulnerability related to zero-day attack information is not defined if not happen earlier. As a result, examining the zero-day exploits is difficult for identification [3]. On other hand, hacker incorporates vulnerability with zero-day attack facilitate then in terms of; providing information about the detected vulnerability to software vendor; an attacker may sell high crucial data to the broker, those may incorporate the highest rate of exploits [4].

Zero-data utilizes several elements that are not identified previously; an attacker will incorporate zero-day in vulnerabilities charted list and with processing program payloads are mixed, and leads to the influence of attack in the server [5]. More ever, zero-day attackers spend hours, months, or weeks to influence attacks through-line of code, to identify the weakness of the system. Upon identification of weakness in the system attacker focused on target applications [6]. Attackers always trace networks to identify weaknesses for gaining access through the network with the execution of their codes. In this manner, the network is breached and subjected to a zero-day attack [7].

When a zero-day attack is identified within the network there is no proper mechanism when observed [8]. A traditional zero-day attack prevention mechanism is involved in the identification of vulnerabilities with the generation of the signature. However, in those signature generation schemes information about zero-day is unknown, so it is difficult for attack detection. Zero-day attackers have high technical knowledge skills and they are not known to the public for a prolonged period. As stated by FireEye, conventional zero-day attacks have an average period of 310 days. Therefore, the identification of a zero-day attack is considered a challenging task [9-14].

To mitigate challenges related to the zero-day attack, this paper presented HMM_TDL, a deep learning model for detection and prevention of attack in the cloud platform. The presented model is carried out in three phases like At first, Hidden Markov Model (HMM) is incorporated for the detection of attacks. With the derived HMM model, hyper alerts are transmitted to the database for attack prevention. In the second stage, a transductive deep learning model with k-medoids clustering is adopted

for attack identification. With k-medoids clustering, soft labels are assigned for attack and data and update to the database. In the last phase, with computed HMM_TDL database is updated with computed trust value for attack prevention within the cloud.

The remainder of the paper is organized as follows: section II presented a review of conventional techniques for attack detection. In section III problem domains related to the zero-day attack and model framework are presented. Section IV described developed HMM_TDL for attack prevention. The results obtained for developed HMM_TDL are presented in Section V with comparative analysis. Finally, section VI provides the overall conclusion of developed HMM_TDL.

2. Related Works

This section presented existing proposed methods for securing a zero-day attack. Through analysis, existing security schemes are categorized as signature-based, hybrid detection, statistical-based, and behaviour-based approach [10].

In statistical-based techniques, an attack profile is generated from past elements. Through those identified elements, the profile parameters are updated in historical exploits for the detection of attacks [15]. However, these statistical-based techniques cannot be able to apply instantaneously for attack protection and detection [2]. This technique relies on a static profile of attack and requires modification in the attack detection setting manually. Signature-based attack detection methods use a library with different malware signatures. Based on the requirement of users those signatures are cross-verified with local files n network web downloads and network files. The created libraries are updated periodically with a new signature. Also, this signature mechanism exploits the new vulnerabilities within the network. Signature-based schemes are widely utilized and they demand high-class signature generation mechanisms.

A behaviour-based mechanism derives worms characteristics for accurate estimation of attack in the webserver. With the identification of attacks in the server machine able to identify victims or deny services that are not involved [16]. This involved estimation of network traffic flow within the network. To overcome the challenges associated with the statistical-based technique and behaviour-based technique, a hybrid-based technique is evolved. In a hybrid-based mechanism, signature schemes are integrated based on the applications [17-21]. Based on this, Kaur and Singh [18] developed a zero-day attack identification using a hybrid approach. But the developed hybrid approach is applicable for polymorphic worm detection alone. To evaluate vulnerabilities risk levels Hazard metrics are developed in [23, 24]. In [25] and [26] estimated hazard level frequency and impact factors. However, risk level assessment in zero-day is immeasurable where vulnerability severity is not defined [27-29]. To make it a more exploitable degree of exploits needs to be defined for zero-day risk assessment. However, the existing technology is subjected to difficulty due to the dynamic characteristics of attacks. Hence, this paper developed HMM_TDL for attack detection for improving the robustness of the cloud platform.

3. Problem Domain and Model Framework

An attack is considered a complex behaviour with several goals based on that attack phases are implemented. In fig 1. illustrates, attackers are engaged to steal data by exploiting the vulnerabilities within the intranet. The vulnerabilities are injected with the network through the following steps. Initially, to gain access to root privileges attackers need to scan the target machine. The attackers scan the target machine bypassing a firewall. In the next stage, Trojans are injected into to file server via a network file interface system. This inclusion of Trojan within the system leads to data leakage. In figure 2 zero-day attack in the cloud server is illustrated.

Figure 1. The typical process in data stealing

Figure 2. Zero-day attack scenario

Initially, to train the model with exploitation of attack vulnerabilities historical alerts are defined as $\{ah_1, ah_2, ah_3\}$. In figure 3, real-time evidence of data stream for multiple results and its corresponding probabilities are presented. For every intent of attack, through associated probabilities next attack probability can be defined.

Figure 3. Overview of proposed HMM_TDP

3.1 Model Framework

The overall framework of the proposed zero-day attack detection model is stated in figure 3. The proposed model comprises of four phases as; 1) data collection - obtain intrusion dataset; 2) pre-processing of data - Training and testing of pre-processed data; 3) Training Model - Provides historical alert to data for processing, and 4) Testing Model - Real-time attack data were processed. Initially, Hidden Markov Model (HMM) is provided with a transfer relationship between variables to provide temporal alerts to data. In the next stage, HMM two-layer model is converted into a Bayesian network with a set of rules with probabilistic inference. This HMM model with probabilistic inference uses transductive learning for rule update. By this, attacks within the network with each time is identified for unknown attacks

Figure 4: Zero-day attack alerts in HMM_TDL

In recent years, receiving original alerts from unprocessed data information cannot be achieved directly. This put forth the demand for extracting effective attack sequences based on IDS alerts and rebuilding them with effective characteristics. As shown in figure 4.

4. Developed HMM_TDL for zero-day attack

In this section, presented about detailed description of developed HMM_TDL for zero-day attack detection and prevention. Initially, HMM is explained for attack detection with hyper alerts. In next sub-section, presented about transductive model for soft labelling is described. Finally, overall performance of developed HMM_TDL is presented with algorithm.

4.1 Hidden Markov Model for Attack Detection

HMM is stated as a dynamic Bayesian network model with probabilistic characteristics in a time-series manner. It provides states in hidden form with the generation of sequences in Hidden Markov Chains and is involved in the generation of random sequences from different states. As defined, HMM has been applied in a vast range of applications like image recognition, biology, signal processing, and so on. HMM is applied in an intrusion detection system. This provides a significant relationship between undefined sequences and attack with temporal estimation. The attacks obtained from malicious insiders incorporate multiple attack steps that differ from the normal characteristics of the network which increases the detection accuracy of the network. Through temporal relationship identification complex relations in attacks are identified. Based on this proposed scheme constructs an attack plan with several hidden layer states and transmits alerts to the observation layer. With the application of HMM, malicious attacks in the cloud are identified with transfer probabilities as presented in figure 5.

Figure 5: HMM model for attack detection

In HMM model the state are represented as s at time instance t with number of node as n_i . The HMM model is defined using following equation (1)

$$\lambda = (B, H, C, J, \pi) \quad (1)$$

As defined in figure 5 observation sequences are measured in observation layer and it is denoted as $N = (n_1, n_2, \dots, n_T)$. At certain time instances, attack are intents are denoted as $n_t = v_i$. In hidden layer attack intents are denoted as $H(i_1, i_2, \dots, i_T)$. Also, at some time instances $i_t = S_i$. The conditional probability of attack sequences and intents are given as $P(al_i | S_i)$ for vertical attacks. Similarly, for horizontal attack intents conditional probability of S_j as $P(S_j | S_i)$.

In general HMM incorporates three different challenges such as: calculation of probability, parameter estimation and decoding. Among those challenges this paper examined parameter estimation, which provides information about sequence of attacks. In this paper, transductive transfer learning mechanism for examining attack stage are measured.

The alerts are generated with attack sequences with random length of $L = (n_1, n_2, \dots, n_M)$. In this, M is defined as positive integer value given by $N = (al_1, al_2, \dots, al_n)$. The hidden layer attack intents are given as H . The probabilistic model is represented as follows equation (2):

$$P(N|\lambda) = \sum_I P(N, I|\lambda) = \sum_I P(N|I, \lambda)P(I|\lambda) \quad (2)$$

To minimize intents each attack intents are evaluated based on consideration of forward and backward intents. The hidden state time is represented as t_i . For the forward probability $\alpha_t(i)$ the observed node are represented as $n_1, n_2, \dots, n_t$. For same hidden state time $t + 1$, the corresponding observed states are denoted as $n_{t+1}, n_{t+2}, \dots, n_T$. The backward probability $\beta_t(i)$ is derived as follows stated in equation (3) and (4):

$$\alpha_t(i) = P(n_1, n_2, \dots, n_t, i_t = q_i | \lambda) \quad (3)$$

$$\beta_t(i) = P(n_{t+1}, n_{t+2}, \dots, n_T | i_t = q_i, \lambda) \quad (4)$$

The probability state is presented as in equation (5)

$$\gamma_t(i) = P(i_t = q_i | N, \lambda) = \frac{P(i_t = q_i, N | \lambda)}{P(N | \lambda)} \quad (5)$$

For backward probability it is given in equation (6),

$$P(i_t = q_i, N | \lambda) = \alpha_t(i) \beta_t(i) \quad (6)$$

Which provides,

$$\gamma_t(i) = \frac{\alpha_t(i) \beta_t(i)}{\sum_{j=1}^N \alpha_t(j) \beta_t(j)} \quad (7)$$

For the defined model λ , the sequence of observation is given as N , the probability of state q_i and q_j with time t and $t + 1$ is given in equation (8) - (10)

$$\delta_t(i, j) = P(i_t = q_i, i_{t+1} = q_j | N, \lambda) = \frac{P(i_t = q_i, i_{t+1} = q_j | N, \lambda)}{P(N | \lambda)} \quad (8)$$

$$P(i_t = q_i, i_{t+1} = q_j, N | \lambda) = \alpha_t(i) a_{ij} b_j(N_{t+1}) \beta_{t+1}(j) \quad (9)$$

$$\delta_t(i, j) = \frac{\alpha_t(i) a_{ij} b_j(N_{t+1}) \beta_{t+1}(j)}{\sum_{i=1}^N \sum_{j=1}^N \alpha_t(i) a_{ij} b_j(N_{t+1}) \beta_{t+1}(j)} \quad (10)$$

The simplified equation is presented as in equation (11),

$$P(N | \lambda) = \sum_{i=1}^N \sum_{j=1}^N \alpha_t(i) a_{ij} b_j(N_{t+1}) \beta_{t+1}(j) \quad (11)$$

Through this HMM construct a trained model as $\lambda = (C, J, \pi)$

4.2 Transductive transfer learning framework

In next phase, this paper constructed transductive transfer learning (TL) framework for prevention of zero-day attack. The constructed TL perform binary classification with leverage of labelled instances denoted as L_s . To prevent zero-day attack A_s . To improve zero-day attack prevention, performance labels are assigned based on class label of source cluster based on class labels. In this technique, instances with target soft label with satisfied threshold value able to involve in construction of cluster for data transfer. The labels assigned with TL is based on the derived HMM model values. In this, cluster or group without any attack is defined as λ . The developed transductive model is applied in HMM model $\lambda = (C, J, \pi)$ for detection and prevention of zero-day attack. In figure 6 overall architecture of HMM_TDL is presented.

Figure 6: Overall Architecture of HMM_TDL

4.2.1 Attack prevention with HMM_TDL

The cluster construction is based on the capturing semantics of domains. In this, based on the calculation obtained by HMM model is utilized for ranking of clusters with consideration of global mean value of cluster group. The relationship exists with i^{th} cluster leads to construction of cluster of length $(i-1)^{th}$ and $(i+1)^{th}$ for other cluster domains. Based on this, i^{th} cluster similarity matrix is constructed as $M_s^{p,q}$. For the i^{th} cluster domain p and i^{th} domain of q provides the value of 1. Similarly, for $(i-1)^{th}$ and $(i+1)^{th}$ for domain p and q assigned values as 0.5. For other it assigned with 0. The source domain transformation is performed for target mapping function with consideration of latent space d between attack scenario. After, the conversion of attack domains in to latent space transformation abundant label instances are classified for target domain of zero-day attack for prevention. To improve zero-day attack prevention soft labelling involved in labelling target instances with appropriate training for construction of classifier.

Based on the derived HMM, model deep learning framework involved in assigning score to cluster group for attack prevention. Initially, all cluster sources are assigned as either “normal” or “attack” class with cluster label. The domain attack source domain and targeted domain is represented as D_1^t and D_2^t with assigned Euclidean distance value of. The i^{th} cluster group source label is ranked as $r_i, r_i + 1, r_i - 1$, with HMM model and labelled with following steps such as:

Step 1: Initially, set label value as zero

Step 2: If cluster source ranked as r_i the attack α is included else it will eliminated from the cluster group.

Step 3: For source cluster ranked as $r_i + 1$, then attack $\frac{\alpha}{2}$ is included within the system else it will be removed from cluster group.

Step 4: For source cluster ranked as $r_i - 1$, then attack $\frac{\alpha}{2}$ is included within the system else it will be removed from cluster group.

Finally, with estimation of target scores values of 0 and 1 are normalized with estimation of attack or normal cluster instances. The assigned soft labels for threshold instances of threshold T_1 is considered as “attack” else T_2 is set as below threshold value is defined as “normal”. The target instances are denoted as follows:

$$T_1 = \alpha \quad \text{\textbackslash\ Set as attack label}$$

$$T_2 = 1 - \alpha \quad \text{\textbackslash\ Set as normal label}$$

In this label, the assignment scheme with labeled instances attacks is classified and prevented from injecting within the network through the generation of soft labels.

The assigned labels are incorporated within the cluster group with the inclusion of three parts with zero-day attack classification. The node within the cluster consists of the following factors such as prior knowledge, edge probability, and conditional probability table (CPT). The HMM is involved in the estimation of attacks in the network with consideration of causality. This paper uses HMM model with transductive transfer learning. Hence, based on the assigned labels unknown attack labels are estimated with the update of rule in equation (12)

$$U_{ij}^t = \begin{cases} \delta + (1 - \delta)U_{ij}^{t-1}, & P(u_i|y_t) = 1 \quad P(u_j|y_t) = 1 \\ (1 - \delta)U_{ij}^{t-1}, & P(u_i|y_t) = 1 \quad P(u_j|y_t) = 0 \\ U_{ij}^{t-1} & \text{otherwise} \end{cases} \quad (12)$$

With respect to assigned label T_1 and T_2 the unknown attack is estimated with consideration of CPT attack as $U_{ij} = P(X = x_j | U = u_i)$. In figure 7 overall flow of developed HMM_TDL is illustrated with attack detection and prevention mechanism. Once the attack is detected by HMM model transductive network is trained for attack based on trust computational value of database.

Figure 7: Overall Flow of HMM_TDL

For construction of label assigned with unknown attack new dataset is constructed with elimination of attacks defined as $D(D = \{y_1, y_2, y_3, \dots\})$ with estimation of missing data attack as y_t . The attack scenario with HMM model for attack scenario is defined as $S = (I_1, I_2, \dots, I_n)$. Based on assigned label

in transductive deep learning HMM estimate unknown attacks in zero-day. The algorithm 1 provides the HMM for attack estimation is presented.

Algorithm 1: Parameter Estimation

Input: Sequence of attack in network = $\{(al_1, al_2, \dots)(al_3, al_4, \dots) \dots\}$

Output: $\delta^{n+1} = (C^{n+1}, J^{n+1}, \mathcal{X}^{n+1})$

// Start

For n = 0 generate δ_i^0

For $a_{ij}^0 = \delta_i^0$ set $b_j(k)^0$

For unknown attack n = 0, 1, 2,

do

Calculate using equation (11)

Calculate using equation (12)

End for

End for

Set values

Set comparison value

If $P(Z_i = 1 | I_i = 1) > trustValue$

then

Compare T_1 and T_2 with estimated value

End if

for $value(Z_i)$ compare attack value

If $value(Z_i) > trustValue$ then

Compute new set Z_i

End if

End for

End for

In transductive framework involved in the generation of source mapping for construction of target domain with consideration of latent space. After the conversion of latent space, the source domain is designed with instance label probable classification of attacks. With the assigned soft label in the data accuracy of zero-day is improved with building training classifier with target instance. In algorithm 2 label assigned for zero-day attack, estimation is presented.

Algorithm 2: Parameter Estimation

Input: Estimation of target domain

Output: Label with consideration of attacks with d-dimension latent space

1. Construct matrix for data node $Z = \begin{pmatrix} X_1 & 0 \dots & 0 \\ \dots & \dots & \dots \\ 0 \dots & 0 & X_k \end{pmatrix}$

2. Estimate matrix W_k with estimation of distance between nodes $W_k(i, j) = e^{-\|x_i - x_j\|^2}$

3. Compute Laplacian transformation with similarity indices $L_x = D_x - W_x$

4. Estimate the Laplacian matrix for computing attacks in node $L = \begin{pmatrix} L_1 & 0 \dots & 0 \\ \dots & \dots & \dots \\ 0 \dots & 0 & L_k \end{pmatrix}$

5. Compute dimensionality of mapping function for computing eigen value $Z(\delta L + L_s)Z^T x = \delta Z L_d Z^T x$

6. Transform target domain with consideration of latent data dimensions

The estimation of zero-day attack involved in HMM model for attack estimation. HMM involved in zero-day attack detection with consideration of threshold in the calculation, with the estimation of threshold labels are assigned and set of parameters are constructed.

The analysis of developed transductive deep neural network involved in training phase for discriminator generation. To characterize zero-day attack it is defined as A_{attack} . The real-data in the network is defined as D , hence the first order training in real-time data is given as $D(S(z))$ the term S provides transductive layer with value of 1. The second order of transductive neural network is about maximizing $V(S, D)$ in this S is layer and D is trained data. Similarly, for trained data $D(S(z))$ with second order 1 minimization of zero-day attack or prevention of attack is performed with $V(S, D)$ as

$$\min_S \max_D V(D, S) = E_x - A_{attack(x)} [\log D(x)] + E_{z-p_z(Z)} [\log(1 - D(S(z)))]$$

The $V(D, S)$ involved in formulation of convergence with estimation of distributed data. The transductive learning for attack detection is computed as (Z_{ij}) . It is defined as in equation (13)

$$Z_{ij} = \sum_{a=0}^{m-1} \sum_{b=0}^{m-1} w_{ij} x_{ij} \quad (13)$$

To compute zero-day attack in from the TDL it is given as in equation (14) and (15),

$$\min_S \log(1 - D(S(Z))) \quad (14)$$

$$\Leftrightarrow D(S(Z)) \approx 1 \quad (15)$$

$$\Leftrightarrow S(z) \approx x \in \chi; \text{ the real-time dataset is denoted as } \chi$$

The complete training data from HMM-TDL is stated as in equation (16)

$$P(D^*, S^*) \leq P(D^*, S) \forall S \quad (16)$$

The attack detected from HMM is incorporated in transductive deep learning model which subjected to two constraints such as defined as follows from equation (17) - equation (27):

Case 1: If $A_{attack} \approx A_s$ for training all data

Consider $P(D^*, S^*)$ as minimal value for data $A_{attack}(x) \leq A_s(x)$

This will be $A_{attack}(x) \leq A_s^*(x)$

$$P(D^*, S) = \int_x A_{attack}(x) D^*(x) dx + \int_x A_{data}(x) D^*(S(z)) dz \quad (17)$$

$$= \int_x A_{attack}(x) D^*(x) + A_s(x)(1 - D^*(x)) dx \quad (18)$$

$$= \int_x A_{attack}(x) D^*(x) - p_s(x) dx + \int_x p_s(x) dx \quad (19)$$

$$= \int_x 1 A_{attack}(x) > A_s(x)(A_{attack}(x) - A_s(x)) dx + \int_x A_s(x) dx \quad (20)$$

$$\geq \int_x A_s(x) dx \quad (21)$$

Case 2: Consider $P(D^*, S^*)$ as minimal value for data $A_{attack}(x) \geq A_s(x)$

This will be $A_{attack}(x) \geq A_s^*(x)$

$$P(D^*, S) = \int_x A_{attack}(x)(1 - D(x)) dx + \int_x A_{data}(x) D(S^*(z)) dz \quad (22)$$

$$= \int_x A_{attack}(x)(1 - D(x)) dx + \int_x A_s(x)(D(x)) dx \quad (23)$$

$$= \int_x D(x) - (p_{G^*}(x) - p_{data}(x))dx + \int_x p_{data}(x)dx \quad (24)$$

$$= \int_x 1A_{attack}(x) > A_{G^*}(x)(A_{G^*}(x) - A_{data}(x))dx + \int_x A_{data}(x)dx \quad (25)$$

$$\geq \int_x 1A_{data}(x) > A_{G^*}(x)(A_{data}(x))dx \quad (26)$$

$$\geq -M \quad (27)$$

5. Experimental Analysis & Results

This research focused on improving security in the cloud from zero-day attack scenarios. The proposed scheme transmits hyper alerts with the estimation of the time window. HMM estimate the attacks in the network and the attack is classified based on consideration of threshold values on the network. The developed transductive framework was evaluated based on consideration of two datasets such as NSL-KDD and CIDD dataset. Both datasets involved in examination of features in data the description of the dataset are presented below:

5.1 Availability of Data and materials

NSL-KDD

NSL - KDD is stated as a standard dataset with the distribution of packets with experimentation of IDS. This dataset consists of features and instances count of 43 and 147,907 respectively. The attack and normal instances are in the count of 76,967 and 70,940 respectively. NSL-KDD dataset incorporates attacks such as a probe, U2R, DoS, and R2L. The overall features selected for analysis are presented in Table 1.

Table 1. NSL-KDD Features

Attack	Traces
DoS	52,987
Probe	13,971
R2L	3863
U2R	119

5.2 CIDD Dataset

CIDD dataset provides identification of cloud dataset with consideration of DoS attack and attack in cloud environment. CIDD dataset is based on time-based data distribution with 5274 instances and 25 features with data dimensionality. The data of CIDD dataset incorporates udp_flood, tcp_syn_flood, pod, dns_flood, land, icmp_flood (smurf) and slowloris. In table 2 presented features of CIDD

Table 2: CIDD Features

Attack	Traces
Land	44
Pod	63
Udp_flood	35
Icmp_flood	15
Dns_flood	34
Slowloris	438
TCP_SYN_Flood	52

5.3 Performance Metrics

The performance of developed HMM_TDP is examined with consideration of parameters such as accuracy, False Positive Rate (FPR), F1-Score and Specificity.

Accuracy is stated as number of websites those are phished to the number of all websites and it is calculated using the equation (28):

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \quad (28)$$

F1-Score provides the classification performance, which provides average of precision and recall and it is calculated using equation (29)

$$F1-Score = 2 \times \frac{(Precision \times Recall)}{(Precision + Recall)} \quad (29)$$

Specificity describes the attacks those are correctly classified and it is calculated using equation (30)

$$Specificity = \frac{TN}{TN + FP} = 1 - FPR \quad (30)$$

Where, FPR - False positive rate
FPR provides the probability of model that reject the original data as attack in the network and it is presented in equation (31)

$$FPR = \frac{FP}{FP + TN} \quad (31)$$

For equation (28) - (31) Where, TP - True Positive provides correctly classified attacks
TN - True Negative normal data without attack correctly identified
FP - False Positive defines normal attack classified
FN - False Negative defines normal data classified as attack

5.4 Experimental Setup

To evaluate the performance of developed model zero-day data attack detection in cloud is considered.

5.4.1 Test Scenario: Zero-day attack detection in Cloud

The CIDD attack consists of a different attack, this paper considers the DoS attack module for detection of zero-day attack in cloud dataset. From the analysis, it is observed that smurf, pod, and land are considered as common attack modules for both CIDD and NSL-KDD datasets. Here, NSL-DoS and CIDD incorporate this common instance with consideration of source and target domains. For analysis of complete labelled NSL-DoS module and CIDD, no label module is included within the framework were stated in Table 3.

Table 3: Attack Modules for HMM_TDL

Parameters		DoS→R2L	DoS→Probe	NSL DoS→CIDD
Cluster transformation	before	11	11	23
Cluster transformation	after	23	17	23
α		0.92327	0.9364	0.9643
T ₁		0.92327	0.9364	0.9643
T ₂		0.03566	0.0326	0.0168

As presented in table 3, the purity node α is evaluated with the generation of cluster group with a size of 13. As stated, hyper alerts use k-medoids for R2L modules with DoS and cloud server. The k-value of medoids is considered as 25, with an assigned value of $\alpha = 0.92327$. Based on this R2L instances are generated in a cloud server with consideration of 25 clusters. The threshold estimated for identification of cluster purity α for T₁ = 0.92327 and T₂ = 0.03566. The labels for attack are assigned with a set of instances for R2L module with cloud value of 0.92327 and normal attack module of R2L includes instances of cloud value of 0.03566

Figure 8: ROC curve for DoS→R2L with AUC = 0.83

Figure 9. Overall Comparison of HMM_TDL in DoS→R2L

The DoS module label instances are assigned with soft instances in R2L modules for training the DNN module. The DoS→R2L provides the accuracy of 0.9275, FPR of 0.0563, and the corresponding ROC curve is presented in figure 8. The transductive DNN provides an improved classification for zero-day attack detection compared with the existing classifier presented in figure 9. The comparative results stated that transductive deep learning scheme provides improved performance than existing ML methods.

In the zero-day attack detection module label instances are utilized on the Probe module for the DoS module for task DoS→R2L. The best validation is measured and obtained for transductive DNN with batch size 100 and epochs count of 90. The DoS→Probe attack provides an accuracy value of 0.9249, FPR of 0.8416 with the ROC curve presented in figure 10. and figure 12 provides the ROC curve

for NSL_DoS→CIDD. Also, from analysis of figure 11 and 13, it is observed that for all parameters accuracy, FPR, F1-Score, and sensitivity developed HMM_TDL exhibits improved performance.

Figure 10: ROC curve for DoS→Probe

Figure 11: Comparison of HMM_TDL in DoS→Probe

Figure12: ROC curve for Figure 10: ROC curve for NSL_DOS→CIDD

Figure 13: Comparison of HMM_TDL in NSL_DOS→CIDD

In table 4 for different medoids the performance characteristics of HMM_TDL for two datasets such as NSL-KDD and CIDD. In table 4 for different medoids performance in NSL-KDD dataset is presented.

Table 4. Performance of k-medoids for NSL-KDD

Points	Accuracy (%)	FPR (%)	F1-Score (%)	Specificity (%)	Time (sec)	cost
500	93	18	89	94	0.06	
1000	89	21	94	87	0.45	
1500	90	25	92	91	0.54	
2000	87	14	93	89	0.38	
2500	92	09	88	90	0.27	

3000	88	13	91	90	0.34
3500	94	10	87	93	0.67
4000	86	16	87	92	0.45
4500	91	11	91	88	0.56
5000	87	16	94	87	0.43

Table 5. Performance of k-medoids for CIDD

Points	Accuracy (%)	FPR (%)	F1-Score (%)	Specificity (%)	Time (sec)	cost
500	86	12	94	87	0.45	
1000	95	15	91	96	0.17	
1500	91	07	88	93	0.06	
2000	87	11	93	91	0.37	
2500	87	18	87	86	0.38	
3000	94	09	95	92	0.27	
3500	93	06	84	86	0.04	
4000	88	14	90	93	0.18	
4500	91	12	89	85	0.27	
5000	89	06	89	90	0.45	

Table 4 provides the analysis of the performance of HMM_TDL in terms of accuracy and time cost. For fairness in the system, medoids are implemented in NSL-KDD and CIDD datasets. Also, table 5 presented the performance characteristics of CIDD is presented.

6. Conclusion

This paper presented HMM_TDL, a deep learning model for the detection and prevention of zero-day attacks in the cloud environment. In this model, HMM model is incorporated for detection of attack with k-medoids clustering for refining attack datasets. The difference between attack and original data is evaluated based on consideration of NSL-KDD and CIDD features. The constructed model is applied in a transductive deep learning network for attack prevention with a classifier. Finally, with estimated HMM_TDL performance of attack prevention is estimated with different performance metrics. Also, the performance of NSL-KDD and CIDD dataset performance for varying k-medoids are presented. In the feature, optimal feature-based classification can be implemented for a real-time network platform.

REFERENCES

1. Parra, G. D. L. T., Rad, P., Choo, K. K. R., & Beebe, N. (2020). Detecting Internet of Things attacks using distributed deep learning. *Journal of Network and Computer Applications*, 102662.
2. Kaur, S., & Singh, M. (2015). A proactive framework for automatic detection of zero-day HTTP attacks on educational institutions. *Computer Fraud & Security*, 2015(2), 10-16.
3. KASIM, Ö. (2020). An efficient and robust deep learning based network anomaly detection against distributed denial of service attacks. *Computer Networks*, 180, 107390.
4. Velliangiri, S., & Pandey, H. M. (2020). Fuzzy-Taylor-elephant herd optimization inspired Deep Belief Network for DDoS attack detection and comparison with state-of-the-arts algorithms. *Future Generation Computer Systems*.
5. de Assis, M. V., Carvalho, L. F., Rodrigues, J. J., Lloret, J., & Proença Jr, M. L. (2020). Near real-time security system applied to SDN environments in IoT networks using convolutional neural network. *Computers & Electrical Engineering*, 86, 106738.
6. Wei, W., Ke, Q., Nowak, J., Korytkowski, M., Scherer, R., & Woźniak, M. (2020). Accurate and Fast URL Phishing Detector: A Convolutional Neural Network Approach. *Computer Networks*, 107275.
7. Sameera, N., & Shashi, M. (2020). Deep transductive transfer learning framework for zero-day attack detection. *ICT Express*.
8. Blaise, A., Bouet, M., Conan, V., & Secci, S. (2020). Detection of zero-day attacks: An unsupervised port-based approach. *Computer Networks*, 180, 107391.
9. Tran, H., Campos-Nanez, E., Fomin, P., & Wasek, J. (2016). Cyber resilience recovery model to combat zero-day malware attacks. *computers & security*, 61, 19-31.
10. Singh, U. K., Joshi, C., & Kanellopoulos, D. (2019). A framework for zero-day vulnerabilities detection and prioritization. *Journal of Information Security and Applications*, 46, 164-172.
11. O. I. Khalaf, M. Sokiyna, Y. Alotaibi, A. Alsufyani and S. Alghamdi, "Web attack detection using the input validation method: dpda theory," *Computers, Materials & Continua*, vol. 68, no.3, pp. 3167–3184, 2021.

12. Sudhakar Sengan,P. Vidya Sagar,Osamah Ibrahim Khalaf and R. Dhanapal" The optimization of reconfigured real-time datasets for improving classification performance of machine learning algorithms" Vol 12 No 1 (2021): Mathematics in Engineering, Science and Aerospace (MESA)
13. Abdulsahib, G.M., Khalaf, O.I."An Improved Cross-Layer Proactive Congestion in Wireless Networks"International Journal of Advances in Soft Computing and its Applications, 2021, 13(1), pp. 178–192
14. Khalaf, O. I., Ajesh, F., Hamad, A. A., Nguyen, G. N., & Le, D. N. (2020). Efficient Dual-Cooperative Bait Detection Scheme for Collaborative Attackers on Mobile Ad-hoc Networks. IEEE Access. vol.8, pp.227962-227969
15. Kim, J. Y., Bu, S. J., & Cho, S. B. (2018). Zero-day malware detection using transferred generative adversarial networks based on deep autoencoders. Information Sciences, 460, 83-102.
16. Hammarberg, D. (2014). The Best Defenses against Zero-day Exploits for Various-sized Organizations. SANS Institute InfoSec Reading Room, 21.
17. Kaur, R., & Singh, M. (2014, February). Efficient hybrid technique for detecting zero-day polymorphic worms. In 2014 IEEE International Advance Computing Conference (IACC) (pp. 95-100). IEEE.
18. Li, G., Liu, F., Sharma, A., Khalaf, O. I., Alotaibi, Y., Alsufyani, A., & Alghamdi, S. (2021). Research on the natural language recognition method based on cluster analysis using neural network. Mathematical Problems in Engineering, 2021.
19. Alotaibi, Y., Malik, M. N., Khan, H. H., Batool, A., Islam, S. U., Alsufyani, A., & Alghamdi, S., (2021), Suggestion mining from opinionated text of big social media data, Computers, Materials & Continua, vol. 68, no.3, pp. 3323–3338.
20. Suryanarayana, G., Chandran, K., Khalaf, O. I., Alotaibi, Y., Alsufyani, A., & Alghamdi, S. A. (2021). Accurate Magnetic Resonance Image Super-Resolution Using Deep Networks and Gaussian Filtering in the Stationary Wavelet Domain. IEEE Access, 9, 71406-71417.
21. Alotaibi, Y. (2020, March). Automated Business Process Modelling for Analyzing Sustainable System Requirements Engineering. In 2020 6th International Conference on Information Management (ICIM) (pp. 157-161). IEEE.
22. Kaur, R., & Singh, M. (2014). A survey on zero-day polymorphic worm detection techniques. IEEE Communications Surveys & Tutorials, 16(3), 1520-1549.
23. Singh, U. K., & Joshi, C. (2016). Quantifying security risk by critical network vulnerabilities assessment. International Journal of Computer Applications, 156(13), 26-33.
24. Alraja, M. N., Farooque, M. M. J., & Khashab, B. (2019). The effect of security, privacy, familiarity, and trust on users' attitudes toward the use of the IoT-based healthcare: the mediation role of risk perception. IEEE Access, 7, 111341-111354.
25. Singh, U. K., Joshi, C., & Gaud, N. (2016). Information security assessment by quantifying risk level of network vulnerabilities. International Journal of Computer Applications, 156(2), 37-44.
26. Ma, X., Niu, Y., Gu, L., Wang, Y., Zhao, Y., Bailey, J., & Lu, F. (2020). Understanding adversarial attacks on deep learning based medical image analysis systems. Pattern Recognition, 107332.
27. Khalaf, O. I., Sokiyna, M., Alotaibi, Y., Alsufyani, A., & Alghamdi, S., (2021). Web Attack Detection Using the Input Validation Method: DPDA Theory. Computers, Materials & Continua, vol. 68, no.3, pp. 3167–3184.
28. Alotaibi, Y. (2021). A New Database Intrusion Detection Approach Based on Hybrid Meta-Heuristics. CMC-COMPUTERS MATERIALS & CONTINUA, 66(2), 1879-1895.
29. Zhao, H., Chen, P.-L., Khan, S. and Khalafe, O.I. (2020), "Research on the optimization of the management process on internet of things (Iot) for electronic market", The Electronic Library, Vol. ahead-of-print No. ahead-of-print. <https://doi.org/10.1108/EL-07-2020-0206>

Availability of data and material

Used CICIDS & NSL - KDD

Competing interests

Not Applicable

Funding

Not Applicable

Authors' contributions

I formulated the design of proposed model for security enhancement in Intrusion Detection System (IDS). The proposed part is written by me.

Alamin

I perform practical analysis and wrote abstract, Introduction and review related to the concept

Adel

In paper I did comparative analysis and performance of proposed approach compared with existing technique.

Acknowledgements

Not Applicable