EAI Endorsed Transactions
on Cloud Systems Research Article **EAI.EU**

A Stackleberg Game Theory and Improved Fuzzy Based Intrusion Detection Approach for Virtual Machine Migration Timing Problem in Cloud Computing

Balamurugan E[1,*], Md. Shawakat Akbar Almamum[2], Md. Shahidul Hasan[2] and Sangeetha K[1]

[1]University of Africa, Toru-Orua, Nigeria
[2]Research Scholar, Texila American University, Guyana

Abstract

Current computing concepts are migrated to a an emerging technology called cloud computing. Self-adaptive resource allocation framework and intelligent machine learning framework are proposed in various research work for providing optimized resource allocation. Privacy and security are the major concerns which restricts it's adoption to clouds. Outsourcing, resource sharing and multi-tenancy are introduced by cloud to overcome security concerns. Stackelberg Game Theory Framework (SGTF) is used in proposed security model for enhancing data's confidentiality level and over cloud environment. For multiple correlated VMs (migration requests), migration problem is studied in this work and for solving the same, an Enhanced Artificial Neural Network (EANN) and IDS based on fuzzy is introduced. In this method, migration request is included with correlations between VMs and these correlated VMs are treated integrally rather than separate treatment

Keywords: Intrusion Detection System, Improved Fuzzy Logic, Stackleberg Game Theory, Migration Timing Problem, Virtual Machine Migration, Cloud Computing

Received on 18 May 2020, accepted on 25 September 2020, published on 12 October 2020

Copyright © 2020 Balamurugan E *et al.*, licensed to EAI. This is an open access article distributed under the terms of the Creative Commons Attribution license, which permits unlimited use, distribution and reproduction in any medium so long as the original work is properly cited.

doi: 10.4108/eai.12-10-2020.166552

1. Introduction

Current technological and computing concepts are migrated to a utility-like solutions as like water and electricity systems by an emerging technology paradigm called cloud computing. Service flexibility, economic savings and configurable computing resources are the major benefits of cloud.

Because of increased user request and user demand, resources cannot be accommodated by a single data centre. In academia and industry, enhancement in resource utilisation and minimization of energy consumption are trending topic of research due to increased power and physical resources like bandwidth, memory, storage and CPU in data centres.

Self-adaptive resource allocation framework and intelligent machine learning framework are proposed in our previous research work for providing optimized resource allocation. But, in those methods, privacy and security are the major concerns and these restricts it's adoption to clouds.

Outsourcing, resource sharing and multi-tenancy are introduced by cloud because of these new concepts and it creates new challenges to security concerns. In data transmission to remote server over a channel, security provision is major concern. There is a need to address security challenges before implementing cloud computing. In single and multiple data centres, various VM migration techniques are presented for avoiding Service Level Agreements (SLAs) violation, which are caused by lacking in resources of network. Energy saving purpose are achieved and resource utilization is enhanced with SLAs violation avoidance by using appropriate migration

[*]Corresponding author. Email: Rethinbs@gmail.com

strategy by researchers as allowed via these VM migration techniques.

The way toward moving a running virtual machine or application between various physical machines without detaching the customer or application is alluded to as Live Migration. Framework assets memory, stockpiling, procedure and Network assets like availability that are apportioned to the virtual machine are moved from the first host machine to the goal machine. VM live movement can benefit from outside assistance to give consistent availability and negligible personal time for clients.

Physical servers in cloud server farms have restricted assets and it might change as per the outstanding task at hand of the specific Physical Machine (PM), a few PMs may get gigantic measure of remaining burden while some get exceptionally low client traffic. The proposed structure will have a total image of all PMs' accessible assets and remaining burden, it will powerfully trigger VM movement from over-burden machines to under loaded machines to adjust the heap of physical machines. Live Migration is performed for accomplishing Energy proficiency, Load Balancing and High accessibility of physical servers in Cloud Data focus.

Cloud Migration is one of much bantered point where cloud directors face extraordinary issues at the hour of information movement from an organization's server to a server that structures cloud somewhere else. In addition, if information movement isn't done efficiently and appropriately, it can offer ascent to issues concerning information and cloud security of organization's advantages that essentially involve information. In this manner, recruiting cloud suppliers having sound understanding about the field with adequate information and ranges of abilities gets crucial for overseeing cloud all the more viably and effectively. Model: Suppose a xyz organization needs to move its information to distributed storage for expanded uptime and adaptability, it goes to cloud specialist co-op for performing such capacities. Presently, the cloud supplier begins introducing ventures for information move to cloud, yet in the middle of face issues like information crash or unapproved access by outsiders.

This is the place the difficult untruths. The owner of information that recruited cloud administrator would confront notoriety misfortunes as well as fiscal misfortunes. Comparable case was experienced when Amazon cloud disappointment occurred and a few organizations endured massive misfortunes because of it. In this way, making sure about information stays a most extreme need of cloud administrators to forestall worldwide cloud security dangers that likewise incorporate cross fringe security concerns.

So, there is a need to design a new migration algorithm for optimizing, multiple correlated virtual machines or a VM migration request migration performances. Stackelberg Game Theory Framework (SGTF) is used in proposed security model for enhancing data’s confidentiality level and over cloud environment, it enhances data security too. For multiple correlated VMs (migration requests), migration problem is studied in this work and for solving the same, an efficient algorithm called Enhanced Artificial Neural Network (EANN) and IDS based on fuzzy is introduced.

The remaining section is organized as follows. Section 2 reviews cloud security and virtual machine migration techniques. Section 3 provides system model, concepts of stackleberg game theory and fuzzy based intrusion detection system techniques. Section 4 illustrates experimental analysis and evaluation of cost parameters. Section 5 deals with conclusion and future work.

2. Literature Review

In this section reviews the advantages and disadvantages of the resource allocation and virtual machine migration timing problem along with the recent techniques.

2.1. Virtual Machine Allocation Strategies

Ahmad et al [12] built up a data transmission advancement plans, server combination systems, dynamic voltage recurrence scaling (DVFS)- empowered force enhancement, and capacity streamlining strategies over WAN connections. The live VM movement plans, topical scientific categorizations are proposed to sort the detailed writing. The basic parts of virtual machine movement plans are explored through a thorough investigation of the current plans. The commonalties and contrasts among existing Virtual Machine (VM) relocation plans are featured through a lot of parameters.

Wang et al [13] proposed another multi-operator frameworks (MAS) design for compelling convention in distributed computing condition. In this MAS, the Virtual Enterprise (VE) initiator can be spoken to by either fixed or versatile specialists to haggle with VE accomplices. The mixture convention consolidates both the fixed and portable operator exchange stages to form a progressively effective and fruitful multilateral specialist communication guideline.

In this arrangement procedure, portable specialist based exchange is first started, it will at that point change to fixed operator based exchange when versatile specialist movement is dismissed or collaboration is hindered in the remote host. In addition, the cosmology based methodology is embraced in the MAS and an implanting philosophy activity convention is built up to refine the information articulation design in the specialist exchange process. The legitimacy and productivity of the convention are checked through the execution of a theoretical VE arrangement case.

Aslam et al [14] proposed a Trust Token based VM relocation convention which ensures that the client VM must be moved to a dependable cloud stage. Unique in relation to past plans, this arrangement isn't reliant on a functioning (on-line) confided in outsider. This work show the proposed systems satisfy significant security and trust necessities for secure VM movement in cloud situations.

Fu et al [15] built up a cross breed portability for load-adjusting in reconfigurable disseminated VMs. To handle this issue from three viewpoints: movement up-and-comer assurance, relocation timing and goal server choice. The administration movement timing and goal server choice are figured as two improvement models. What's more, infer the ideal relocation arrangement for conveyed and heterogeneous frameworks dependent on stochastic improvement hypotheses.

Restoration forms are applied to display the elements of movement. WIn this work, take care of the operator relocation issue by powerful programming and expand the ideal assistance movement choice by thinking about the interaction of the half breed versatility. This choice arrangement is reciprocal to the current help and specialist relocation strategies. Its exactness is confirmed by recreations.

Sammy et al [16] proposed a safe vitality mindful provisioning of distributed computing assets on combined and virtualized stages. Vitality proficiency is accomplished through perfectly unique Round-Robin provisioning component and the capacity to shut down sub-frameworks of a host framework that are not required by VMs mapped to it. Further propose answers for security challenges looked during VM live movement. What's more, approve this methodology by leading a lot of thorough execution assessment study utilizing CloudSim toolbox. The test results show that this methodology accomplishes diminished vitality utilization in server farms while not settling on security.

2.2. Strategies of VM Migration Timing problem

Tao et al [17] presented a triple-target streamlining model for dynamic movement of VMs (DM-VM) is built up, which takes vitality utilization, correspondence among VMs, and relocation cost into account under the circumstance that the stage works regularly. The DM-VM issue is partitioned into two sections: (I) framing VMs into gatherings, and (ii) deciding the most ideal approach to put the gatherings into certain physical hubs. A Binary Graph Matching-based Bucket-code Learning Algorithm (BGM-BLA) is intended for taking care of the DM-VM issue.

In BGM-BLA, pail coding and learning is utilized for finding the ideal arrangements, and paired chart coordinating is utilized for assessing the up-and-comer arrangements. The computational outcomes show that the proposed BGM-BLA calculation performs moderately well as far as the Pareto sets got and computational time in correlation with two enhancement calculations, i.e., Non-commanded Sorting Genetic Algorithm (NSGA-II) and parallel chart coordinating based normal coding calculation.

Qiu et al [18] structured a unique control calculation to ideally put substance and dispatch demands in a crossover cloud foundation traversing geo-conveyed server farms, which limits in general operational cost extra time, subject to support reaction time limitations. Thorough examination shows that the calculation pleasantly limits the reaction times inside the preset QoS target, and ensures that the general expense is inside a little steady hole from the ideal accomplished by a T-space look ahead instrument with known future data. We check the exhibition of our dynamic calculation with model based assessment.

Wood et al [19] introduced a lot of enhancements that limit the expense of moving stockpiling and virtual machine memory during relocations over low transmission capacity and high inertness Internet joins. To assess this framework on an operational cloud stage circulated over the mainland US. During concurrent movements of four VMs between server farms in Texa sand Illinois, Cloud Net's enhancements diminish memory relocation time by 65% and lower transmission capacity utilization for the capacity and memory move by 19GB, a half decrease.

Li et al [20] proposed a disconnected VM situation strategy through imitated VM movement, while the on-line VM position is comprehended by a genuine VM relocation process. The relocation calculation is a heuristic methodology, where place the VM to its best PM straightforwardly, as long as it has enough limit.

Something else, if the relocation limitation is fulfilled, move another VM from this PM to suit the new VM. Moreover, crossover plot where a bunch is utilized to acknowledge up and coming VMs for the on-line situation. Assessment results demonstrate the high proficiency of the proposed calculations.

Sun et al [21] built up a proficient online live movement of different related VMs in virtual server farm of Migration (VDC-M) demands, for upgrading the relocation execution. What's more, utilize the system as substrate system to direct broad re-enactment tests. Reproduction results show that the presentation of the proposed calculation is promising as far as the all-out VDC remapping cost, the blocking proportion, the normal movement time and the normal personal time.

Anwar et al [22] built up a game-hypothetical system for the VM relocation timing issue in which the cloud supplier chooses when to move a VM to an alternate physical machine to decrease the danger of being undermined by an assembled vindictive VM. The foe chooses the rate at which dispatches new VMs to gather with the casualty VMs. This definition catches an information spillage model in which the expense brought about by the cloud supplier relies upon the span of collocation with pernicious VMs.

It additionally catches costs caused by the enemy in propelling new VMs and by the safeguard in relocating VMs. Also, set up adequate conditions for the presence of Nash equilibria for general cost capacities, just as for explicit launches, and portray the best reaction for the two players.

Besides, stretch out the model to portray its effect on the assailant's result when the cloud uses interruption identification frameworks that identify side-channel assaults. The hypothetical discoveries are substantiated with broad numerical outcomes in different settings just as a proof-of-idea execution in a sensible cloud setting.

Hong et al [23] developed a virtual Trusted Platform Module (vTPM) live migration scene in clouds and its security and performance requirements are analyzed. Furthermore, a trusted VM-vTPM live migration protocol and its detailed design are presented. At last, the protocol was evaluated from the aspects of security and performance. As far as we know, the trusted VM-vTPM live migration protocol based on the pre-copy is firstly proposed.

From the above audit give a thorough investigation of distributed computing security and protection concerns. Furthermore, distinguish cloud vulnerabilities, arrange known security dangers and assaults, and present the best in class practices to control the vulnerabilities, kill the dangers, and align the assaults.

Nonetheless, virtual machine movement security issue can't be overlooked because of its juvenile improvement. While, these strategies either depend on equipment, or need satisfactory security and expansibility. So this work centersaround building up a system and examine the security dangers of the virtual machine movement, and give a viable answer for relocation timing issue.

3. Proposed Technique

Stackelberg Game Theory Framework (SGTF) is used in proposed security model for enhancing data's confidentiality level and over cloud environment, it enhances data security too. For multiple correlated VMs (migration requests), migration problem is studied in this work and for solving the same, an efficient algorithm called Enhanced Artificial Neural Network (EANN) and IDS based on fuzzy is introduced.

In this method, migration request is included with correlations between VMs and these correlated VMs are treated integrally rather than separate treatment. Migration request is remapped using EANN algorithm at first stage and migration paths are computed and from source server, for migrating virtual machines, bandwidth resources are allocated to destination ones. An extended system model is considered, where F-IDS is equipped in cloud

3.1 Cloud System Model

Cloud is assumed as a physical machines set in this model and from various users, number of VMs can be hosted by every machine. Placement strategy is used by cloud provider for assigning VMs to physical machines in initial condition. Analysis is not affected by placement strategy details and there is no control of adversary over it.

Assumption is made that, collocation with set of victim VMs is a major interest of adversary on same physical machines [22]. Through a game-theoretic framework, interaction between adversary and cloud provider who is a defender is studied in this work, where, rewards are time-dependent.

For defending against collocation attacks, VMs are reassigned to different machines, at the time selected by defender's strategy. On other side, attack rate is selected by adversary for launching more VMs for increasing their chances for prolonged collocation with her victims. For the game, three possible placement scenarios are illustrated in figure 1.

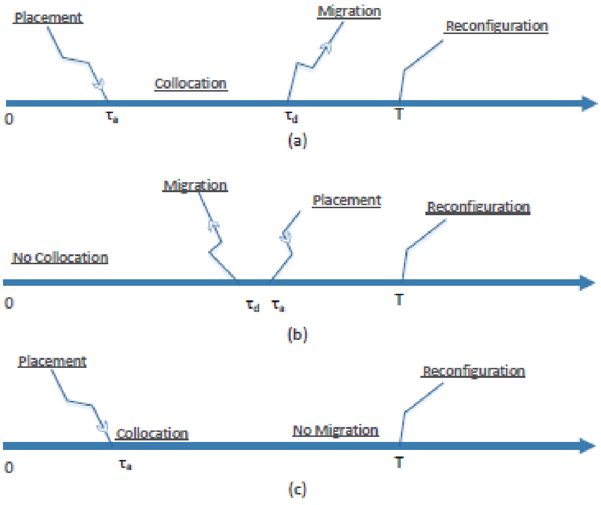


Figure. 1 Three possible placement scenarios for stackelberg game model [22]

In plot (a), at time τ_d, before target VM is migrated to another node, at time τ_a, attacker's VM is successfully collocated with target VM on same hypervisor. A successful collocation event is represented by this scenario and information leakage is produced because of this.

In plot (b), before placing malicious VM on hypervisor, target VM is migrated and so, collocation event will not occur.

At last, no-migration policy is illustrated in plot (c), where, maximization of collocation time happens.

3.2 Stackelberg game theory steps

Stackelberg game model based mitigation timing problem is presented in this section. In this game, for security sensitive resource, fight is happens between two players. Attack-defence condition is described by this presented model [24]. Two types of players are incorporated in this game, they are competing against each other and termed as attacker and defender. Defender tends to product the resource and attacker tends to comprise the resource. Detailed discussion about, game model's every element is presented below, A tuple $\Gamma(\rho, \mathrm{A}, u)$, is used for defining a game, where

- Players set is represented as ρ. Here, $\rho = \{1,2\}$,player 1represents defender and player 2 represents adversary.
- For adversary and defender action space is given by $= A_d \times A_a$.
- $u = u_d, u_a$represents reward function, $u: A \to \mathbb{R}^2$.

a) Defender's action space

Re-allocation period is controlled by cloud provider, who is termed as system defender as stated from timing factor investigation. Assume, time constant as $\tau_d \epsilon A_d$, where defender migrates a running VM to a new physical node, so that $A_d = [\tau_{min}, T]$. In this, system parameter is represented as T, where reset of credential is alloed and smallest reconfiguration time is represented as τ_{min}. At time T assume a leakage model, where reset of credential happens and fromside-channel attack, no benefit is given to attacker.

In order to minimize information leakage chances, value of $\tau_d$is optimized by defender and it avoids system over loading with unnecessary migrations. Between stability and security, tradeoff optimization is a amjor goal of defender. In specific, high security of system is indicated by small value of τ_d. This because of small co-residency times between any two VMs. But, between physical nodes, VMs, frequent migration increases the overhead of the system.

The VM live migration overhead depends on workload of VM. Speed of network, memeory size of VM are major factors affecting overhead of VM migration as shown in this work. More stable system is required with high value of τ_d. On same node, between VMs, coresidency time is large and it makes system highly susceptible to a data breach through collocation attacks.

b) Attacker's action space

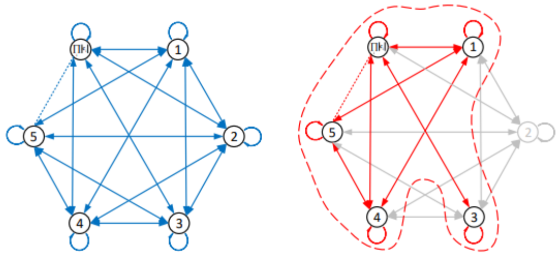
Here, assumption is made that, system placement algorithms are not known to attacker and so, it tries to increase request count submitted to provider of cloud for increasing its coredidency chances. Assume $\lambda_a \epsilon A_a$ represents request rate submitted to cloud, where, non-negative attack rates interval is represented as $A_a = [\lambda_{min}, \lambda_{max}]$. At time t=0, game is assumed to start and actual time is represented as τ_a, where, attacker successfully collocates with her targeted victim.

Hence, non-negative random variable is given by $\tau_a > 0$ with probability density function (pdf) $f_a(\tau_a:, \lambda_a)$ which is parametrized byλ_a. For every submitted job, cost is paid by attacker, so it needs optimization over attack rate λ_a. So, tradeoff of attacker can be summarized as, Probability of collocation with victim by attacker is less if λ_a is very smallλ_a is very small and any information is stealed before migration of VMs. At high attack cost expense, successful chance of collocation is increased by attackers if λ_a is very large. So, for yielding early collocation's higher probability than $f_a(\tau_a; \lambda_{a2})$, pdf f_a should be $f_a(\tau_a; \lambda_{a1})$ and $\lambda_{a1} > \lambda_{a2}$.

c) A Graphical View:

In this model, state switches and states sets are represented as a directed graph. For instance, fully connected graph is shown in figure 2a, with links as state switches and nodes as states set. Figure 2b is obatined by eliminating some invalid switches and states. At game's beginning, one node is selected as initial state s_0 by defender. In every turn, one node a_t is selected as target by attacker. Self loop is contained by evvry valid state, which means that no switch is always one option for defender.

From a node, outgoing links count is assigned as node outdegree of degree for short, or in equivalent, states count that are switched from state. $N(s) = \{s' \in V_{|css'} \neq \infty\}, \forall_s \in V$ is defined as a neighbor state and $|N(s)|$corresponds to node's degree.



(a) A fully connected graph

(b) A subgraph after elimination of invalid states and valid links

Figure. 2 All possible switch pairs model [22]

d) Attacker's Strategy

In this subsection, payoff and strategy of attacker are defined. For deciding formation of prior belief $q_t = \{q_s \,|\, s \in V\}$ by attacker regarding states probability distribution based on feedback received in previous action and in game. For simplicity, for all states, identical cost of attacking is assumed and attack is always benefitted by this. SO, at turn t, attacker always selects $a_t = argmax_{s \in V} q_s$.

e) Defender's Strategy and Cost

Between switching states cost and attack loss, balanced is strike by defender, which is an objective of it. To this end, before start of game, strategy is committed by defender and the same is declared to attacker. Randomized strategy should be adopted by defender as in Stackelberg games, for accounting attacker's possible response.

Transition probabilities set $P = \{p_{ss}'\}|V| \times |V|$ is used for defining strategy of defender in this work, where, resource switching probability from current state s to s' is expressed as p_{ss}'. In beginning, an optimal P is committed by defender and based on P, in every turn, states are sampled. If $c_{ss}' = \infty$, we need $p_{ss}' = 0$ and $\sum_{s'} \in V p_{ss}' = 1, \forall_s \in V$. Cost of defender at turn t for a specified states pair $s_t, s_{t+1}$is defined as,

$$c(s_t, s_{t+1}) = 1_{\{a_t = s_{t+1}\}} + c_{s_t, s_{t+1}} \quad (1)$$

Loss due to attack is represented in first term of expression (1) [22], where, if $a_t = s_{t+1}$, then $1_{\{a_t = s_{t+1}\}} = 1$ else 0. Cost of switching is represented by second term.

f) Feedback During the Game

Information asymmetry reversing is a major purpose of Migration Timing Problem (MTP). So, game's information structure definition is a critical one. Assumption is made that, before the start of game, all resource information and strategy of defender is known to both players. But, during the game, player may have various feedback.

Defender: To public, initial state $s_0$and strategy P of defender is declared as Stackelberg game leader. During the game, P is not changed by defender. In every turn, success or failure of attack by an attacker is known to defender.

Attacker: Value of s_0 and P are known to attacker as Stackelberg game's follower. At any turn t, success or failure of an attack is known to attacker after attacking. In case of successful attack, s_t is known to attacker immediately. Else, this turn will be used for learning s_t by attacker and at this turns end, it knows s_t. In both cases, $q_t = p_{st}$, where, in P, s_t-th row is represented by p_{st}. Form defender's perspective, it is a worst-case scenario. Case is leaved and no feedback or partial feedback is received by attacker for future work.

g) Defender's Optimal Strategy and Cost

Under various conditions, optimum cost and optimum strategy of defender are solved in this. From any initial state, minimization cost, as expressed in (2) [22] is a major problem of defender. With an initial state, defender's optimal cost is represented as$C^*(s)$, where,

$$C^*(s) = {}^{min}_{p}\, C_p(s) \quad (2)$$

Based on MTP theory, computation of optimal strategy P^* is possible and for any initial state $s \in V$, cost can be optimized simultaneously by this.

$$P^* = argmin_P C_P(s), \forall_s \in V \quad (3)$$

For a defined feedback structure, at any t, have $a_t = argmax_{s \in V} p_{s_t s}$. So, at turn t, expected loss of defender is given by,

$$E\left[1_{\{a_t = s_{t+1}\}}\right] = E[1_{\{s_{t+1} = argmax_{s \in} p_{s_t s}\}}] = maxp_{s_t} \quad (4)$$

At turn t, for a specified P and s_t, expected loss of defender is given by

$$c_p(s_t) \triangleq E_{s_{t+1}}[c(s_{t,} s_{t+1})] \quad (5)$$

$$= maxp_{st} + \sum_{s_{t+1} \in N(s_t)} p_{s_t s_{t+1}} c_{s_t s_{t+1}} \quad (6)$$

3.3 Cost Function calculation by Enhanced Artificial Neural Networks (EANNs)

Minimization of longterm discounted cost is the objective of defender in this work and it is expressed as $\sum_{t=0}^{\infty} \alpha^t c(s_t)$,where, discounted factor is represented as $\alpha \in (0, 1)$. As defender is not sure about attacker, it tend to minimize the cost function in current turn itself rather than in next turn, as interpreted from α. Highly patients of defender is indicated by high value of discount factor.

Based on Markov chain, resource state is involved for specified initial state s_0 and P with V as its state space and transition probability as P. So, discounted problem is corresponds to problem of defender, where, coincide occurs between transition probabilities and strategy of defender. With initial statess_0 = s, long-term cost of defender can be rewritten as,

$$C_P(s) = \sum_{t=0}^{\infty} c_p(s_t) \quad (7)$$

$$= C_p(s) + \alpha \sum_{s' \epsilon N(s)} pss' E\left[\sum_{t=0}^{\infty} \alpha^t \left(s_{t+1,} s_{t+2,}\right) | s_1 = s'\right] \quad (8)$$

$$= C_p(s) + \alpha \sum_{s' \epsilon N(s)} pss' C_P[s'] \quad (9)$$

- **Enhanced Artificial Neural Network (EANN)**

A way of reasoning is An artificial neural network (ANN), where central nervous system neurons principles influences it [25]. There are three layers in this neural network, called, input, hidden and output layer and there exist, some artificial neurons called nodes in every layer with output vector, bias of neuron and weight matrix.

From beyond the network, neurons layer, which receives inputs directly as called as input layer, layer which produces network's outcome is termed as output layer and hidden layer corresponds to the one between input and output layers. Between input and output parameters, linear and nonlinear associations can be learned by network by using nonlinear transfer functions of various neuron layers. Weights are multiplied with individual inputs in feed-forward systems and summing function is give with these weighted values and with neurons bias, it is summed. Figure 3 shows the proposed back propagation neural network. Feed Forward NN is similar to back propagation neural network, except that, error's back propagation.

Neural network is used for initially training the data in cloud. Consider $a_m = data_1, data_2, \dots \dots data_m$ as data. Hidden layers are given with this data. Following shows the process done in hidden layer,

$$H_l = \left[\sum_{m=1}^{M} weight_{lm} \times a_m\right] + Bias_l \quad (10)$$

Where,

atl^th node, hidden layer is represented as H_l,

atl^th node, input vector a_m's interconnection weight is represented as $weight_{lm}$,

at lth node, bias is represented as $Bias_l$,
elements count is represented as M,

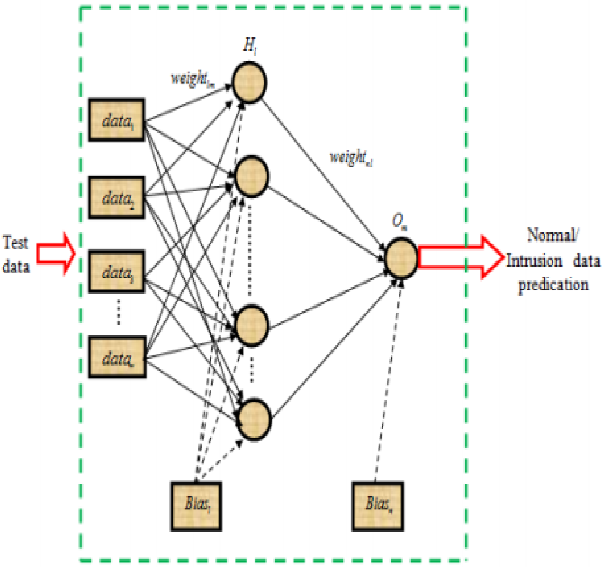


Figure.3. EANN Architecture

Input's transfer function is taken at hidden layer for generating output. Activation function used here is tan sigmoid function, which is a most commonly used one and it is expressed as,

$$\phi(H_l) = \frac{e^{H_l - e^{-H_l}}}{e^{H_l + e^{-H_l}}} \qquad (11)$$

At lthnode, output is given by expression (11), next layer is given with this output. For every hidden neurons, this process is done and forward the results to output layer. In output layer, through activation function, bias function and hidden layer output' weighted sum are passed and it is given by,

$$O_m = \phi[(\sum_{l=1}^{L} weight_{nl} \times \phi(H_l))Bias_n] (12)$$

Where,
hidden vector's interconnection weight is represented as $weight_{nl}$
elements count is given by L,

Error between estimated outcome and target is computed at last. Between predicted and target outcome, Mean Square Error (MSE) computed for achieving the same. Computation of error is expressed as,

$$MSE = \frac{1}{Q}\sum_{q=1}^{Q}(O_{target,q} - O_{predicted,q})^2 \qquad (13)$$

$$MSE = \frac{1}{M_C}\frac{1}{Q}\sum_{q=1}^{Q}(O_{target,q} - O_{predicted,q})^2 \qquad (14)$$

Technique used to select first hidden layer's nodes count is adaptively selected based on mean square error in this proposed work. This is done for dynamic training of learning rate L_r, manual setting blindness is avoided using this with the momentum factor M_c's assistance . A novel neural network model termed as Enhanced Artificial Neural Network (EANN) is constructed according to adaptively selected first hidden layer's nodes count, momentum factor and learning rate, which is selected dynamically.

Back propagation computed error to hidden layer is done next. In order to reduce error value, adjusted the interconnection weight accordingly. Until making zero or less than 0.0001 as error value, this process is continued. This corresponds to training process and for new data, testing process is done. Within neural network, data within cloud are trained. Generate training weight and for anomaly data testing, this is set as testing weight.
With trained data, anomaly data is checked. In cloud data is updated, if test score is greater 5, else data is added in queue. For grouping possibility, again checked the data addition into queue, if there are ten data entries in queue. These data are corresponds to intrusion data. For future analysis, data detected as intrusion data are not considered, else they will be stored separately.

3.4. Game model with Fuzzy based Intrusion Detection System

Goal of attacker in aforementioned model is to collocate with her victim immediately after migration of victims happens. Until τ_d, attacker will reside there, after collocating with her victim as shown evidently because, there is no detection technique for urging her to evade [22]. Existing system is extended in this section and considered that cloud data centre is equipped with an IDS.

After a sufficient time period δ, suspicious activities and any user's malicious behaviour are captured by IDS. Time period is a random variable having distribution$y(\delta), \delta \in [0, T]$. $\delta < \tau_d$is maintained for useful detection. So, collocation attacks needs to be stopped by attacker before being detected. Another control variable s is introduced, which needs to be optimized by attacker. This parameter indicates, time duration that she should continue to carry on attack after collocating successfully.

Between extreme of a fully degenerate distribution where δ is exactly known by players and extreme of an uninformative prior (a uniform distribution) where useful information about time-to-detection δ is not known to player, entire range of priors are accounted by distribution $y(\delta)$. For latter case, attacker is choose to stop after a duration δ from onset of successful collocation, i.e., right before $\tau_a + \delta$.

For accounting detection probability, attacker's payoff function u_a is modified next. A cost D is incurred by attacker in detection event as this user will be black listed, but, its gain equals amount of data read out until detection. Over collocation time τ_d, and time to- detection δ, attacker's expected reward is averaged for redefining it.

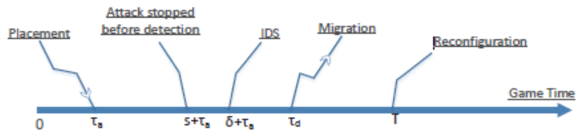


Figure.4. Attacker evades IDS by early stopping of malicious activity.

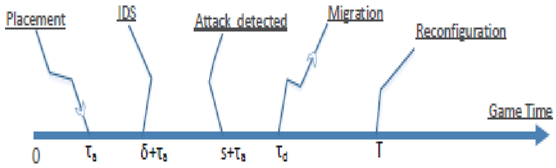


Figure.5. Attacker detected by Fuzzy based Intrusion Detection System(F-IDS) [22].

In no detection event as attacker stopped malicious activities before IDS alarm, attacker's expected payoff is accounted by first term [22], i.e., $s < \delta$. Figure 4 illustrates the same. Detection event is represented by second term, so at $\tau_a + \delta$, collation ends., i.e., after a collocation duration $\delta < s$, figure 5 shows the same. So, detection loss D is incurred by an attacker. No detection event because of migration mechanism is accounted by third and fourth terms. It can also be stated as, attacker is not identified because $\tau_d - \tau_a < \min(\delta, s)$.

Attack launching cost is accounted by last term. After reaching maximum generations count, iteration is stopped. After suitable process, for further processing, select a best rule and give it to FLS and normal or abnormal condition data under test is decided then. Fuzzy system are aligned after generating optimum rule. Fuzzy rule base and fuzzy membership function (MF) definition are the major steps of fuzzy system design.

- **Membership function**

Following describes the expressions used for computing membership values. Mapping of membership value or membership degree with every point of input space among 0 and 1is evaluated by a curve called MF. Proper MF is selected for aligning MF[26]. For obtaining fuzzified value by changing input is data is done by selecting triangular MF.

In a fuzzy set A, there are three vertices *a*, *b*, and *c* of *f*(*x*) in triangular MF, where, lower boundary is represented by a, upper boundary is represented by c with 0 as a membership degree and centre value is represented as b with 1 as membership degree. Estimation of fuzzy MFs, is a key issue in all fuzzy sets.

1. Fuzzy set is evaluated fully by MF.
2. A MF renders and an element similarity degree measured to a fuzzy set
3. Any form can be taken by MFs, but in real applications, there exist some usual examples.

Following describes the formula used for computing membership values.

$$f(x) = \begin{Bmatrix} 0 & if\ x \le a \\ \frac{x-a}{b-a} & if\ a \le x \le b \\ \frac{c-x}{c-b} & if\ b \le x \le c \\ 0 & if\ x \ge c \end{Bmatrix} \tag{15}$$

Fuzzy logic afforded with these rules. There are fuzzy rules set in rule base in medium, high and low distance value form. Incoming data is tested after completion of training process. Data is uploaded to CSP by cloud user in testing process. The CSP is not aware of incoming data, so, it checks the normal or intruded condition of incoming data in this stage. Data is tested by trained FLS structure. Score value is obtained at last. Condition specified in expression (16), will be satisfied by obtained value of score.

$$result = \begin{cases} T_h \ge score; & data\ are\ normal \\ T_h \le score; & data\ are\ intrued \end{cases} \tag{16}$$

Intrusion of specified data is checked by using its score value. One threshold T_h is fixed according to score value in this. Data with computed score value greater than threshold T_h is intruded. Other data are corresponds to normal one.

4. Results and Discussion

Extensive simulations are conducted for evaluating the proposed algorithm's performance. For experimentation, CloudSim framework is adapted in cloud simulation environment. With respect to evaluation metrics such as average attack duration, average migration time and detection accuracy, promising results are produced by proposed algorithm as shown in results of simulation.

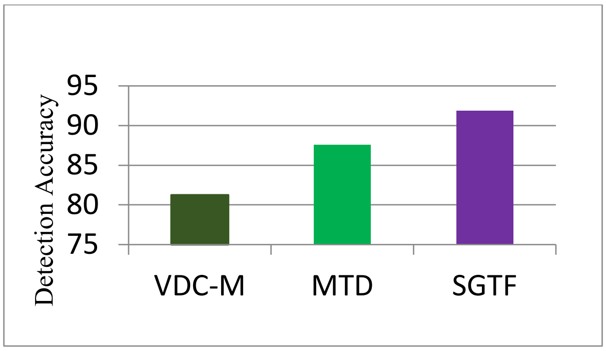


Figure.6. Performance comparison of detection accuracy between proposed and existing techniques

Detection accuracy performance comparison of existing and proposed methods are shown in figure 6. Around 91.87% of accurate results are produced by proposed SGTF technique, which is a highest one, whereas, 87.56% of accurate results are produced by MTD technique and 81.24% of accurate results are produced by VDC-M technique.

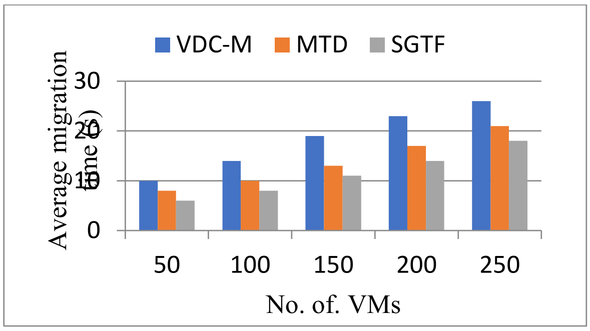


Figure.7. Performance comparison of total completion time against number of virtual machines

If there is an increase in PMs count, then there will be an increase in migration time gap between 250 VMs and 200 VMs as shown in figure 7. This is because, for a specified 250 VMs input, with small PMs count, majority of VMs cannot be accepted in actual situations. So, there is no huge difference between 200 VMs input and 250 VMs. But, VMs accepted by cloud system can be increased by increasing PM host count and resources. It leads to an increase of total migration time

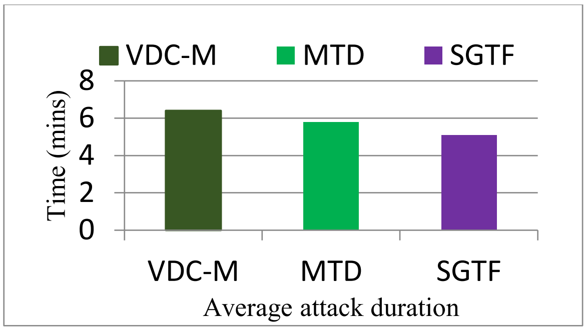


Figure.8. Average attack duration comparison between proposed and existing techniques

Comparison of average attack duration between existing and proposed methods are shown in figure 8. When compared with existing VDC-M and MTD methods, effective detection of attacks is achieved in proposed framework, as shown in experimental results.

5. Conclusion

Confidentiality with high security should be provided by cloud to end user while accessing data from it. Stackelberg Game Theory Framework (SGTF) is used in proposed security model for enhancing data's confidentiality level and over cloud environment, it enhances data security too. For multiple correlated VMs (migration requests), migration problem is studied in this work and for solving the same, an efficient algorithm called Enhanced Artificial Neural Network (EANN) and IDS based on fuzzy is introduced.

In this method, migration request is included with correlations between VMs and these correlated VMs are treated integrally rather than separate treatment. Migration request is remapped using EANN algorithm at first stage and migration paths are computed and from source server, for migrating virtual machines, bandwidth resources are allocated to destination ones. An extended system model is considered, where F-IDS is equipped in cloud.

The F-IDS is a type of reactive defence technique, which is combined to proactive VM migration defence technique for enhancing security of cloud against side channel attacks. For migration timing problem, when compared with existing algorithm, better performance is exhibited by proposed technique as shown in results of experimentation and with respect to data security and level of confidentiality, better enhancement is shown by it. Future research include studying VM allocation dynamics and jointly optimizing timing and allocation policies in stochastic game model formulations

References

[1] Majhi, S. K., & Dhal, S. K. (2016). A Study on Security Vulnerability on Cloud Platforms. *Procedia Computer Science*, *78*(C), 55-60.

[2] Mastelic, T., Oleksiak, A., Claussen, H., Brandic, I., Pierson, J. M., &Vasilakos, A. V. (2014). Cloud computing: Survey on energy efficiency. *Acm computing surveys (csur)*, *47*(2), 1-36.

[3] Almorsy, M., Grundy, J., & Müller, I. (2016). An analysis of the cloud computing security problem. *arXiv preprint arXiv:1609.01107*.

[4] Mollah, M. B., Azad, M. A. K., &Vasilakos, A. (2017). Security and privacy challenges in mobile cloud computing: Survey and way ahead. *Journal of Network and Computer Applications*, *84*, 38-54.

[5] Boutaba, R., Zhang, Q., &Zhani, M. F. (2014). Virtual machine migration in cloud computing environments: Benefits, challenges, and approaches. In *Communication Infrastructures for Cloud Computing* (pp. 383-408). IGI Global.

[6] Fischer, A., Fessi, A., Carle, G., & De Meer, H. (2011, October). Wide-area virtual machine migration as resilience mechanism. In *2011 IEEE 30th Symposium on Reliable Distributed Systems Workshops* (pp. 72-77). IEEE.

[7] Sun, Q., Shen, Q., Li, C., & Wu, Z. (2016, August). Selance: Secure load balancing of virtual machines in cloud. In *2016 IEEE Trustcom/BigDataSE/ISPA* (pp. 662-669). IEEE.

[8] Zhang, W., Han, S., He, H., & Chen, H. (2017). Network-aware virtual machine migration in an overcommitted cloud. *Future Generation Computer Systems*, *76*, 428-442.

[9] Zhao, M., &Figueiredo, R. J. (2007, November). Experimental study of virtual machine migration in support of reservation of cluster resources. In *Proceedings of the 2nd international workshop on Virtualization technology in distributed computing (VTDC'07)* (pp. 1-8). IEEE.

[10] Fu, S., Xu, C. Z., Wims, B., &Basharahil, R. (2006). Distributed shared arrays: A distributed virtual machine with mobility support for reconfiguration. *Cluster Computing*, *9*(3), 237-255.

[11] Fan, C. T., Wang, W. J., & Chang, Y. S. (2011, September). Agent-based service migration framework in hybrid cloud. In *2011 IEEE International Conference on High Performance Computing and Communications* (pp. 887-892). IEEE.

[12] Ahmad, R. W., Gani, A., Hamid, S. H. A., Shiraz, M., Yousafzai, A., & Xia, F. (2015). A survey on virtual machine migration and server consolidation frameworks for cloud data centers. *Journal of network and computer applications*, *52*, 11-25.

[13] Wang, G., Wong, T. N., & Wang, X. (2014). A hybrid multi-agent negotiation protocol supporting agent mobility in virtual enterprises. *Information Sciences*, *282*, 1-14.

[14] Aslam, M., Gehrmann, C., &Björkman, M. (2012, June). Security and trust preserving VM migrations in public clouds. In *2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications* (pp. 869-876). IEEE.

[15] Fu, S., & Xu, C. Z. (2004, August). Migration decision for hybrid mobility in reconfigurable distributed virtual machines. In *International Conference on Parallel Processing, 2004. ICPP 2004.* (pp. 335-342). IEEE.

[16] Sammy, K., Shengbing, R., & Wilson, C. (2012). Energy efficient security preserving vm live migration in data centers for cloud computing. *IJCSI International Journal of Computer Science Issues*, *9*(2), 1694-0814.

[17] Tao, F., Li, C., Liao, T. W., &Laili, Y. (2015). BGM-BLA: a new algorithm for dynamic migration of virtual machines in cloud computing. *IEEE Transactions on Services Computing*, *9*(6), 910-925.

[18] Qiu, X., Li, H., Wu, C., Li, Z., & Lau, F. C. (2014). Cost-minimizing dynamic migration of content distribution services into hybrid clouds. *IEEE Transactions on Parallel and Distributed Systems*, *26*(12), 3330-3345.

[19] Wood, T., Ramakrishnan, K. K., Shenoy, P., & Van der Merwe, J. (2011). CloudNet: dynamic pooling of cloud resources by live WAN migration of virtual machines. *ACM Sigplan Notices*, *46*(7), 121-132.

[20] Li, K., Zheng, H., & Wu, J. (2013, November). Migration-based virtual machine placement in cloud systems. In *2013 IEEE 2nd International Conference on Cloud Networking (CloudNet)* (pp. 83-90). IEEE.

[21] Sun, G., Liao, D., Zhao, D., Xu, Z., & Yu, H. (2015). Live migration for multiple correlated virtual machines in cloud-based data centers. *IEEE Transactions on Services Computing*, *11*(2), 279-291.

[22] Anwar, A. H., Atia, G., &Guirguis, M. (2019). A game-theoretic framework for the virtual machines migration timing problem. *IEEE Transactions on Cloud Computing*.

[23] Hong, Z., Juan, W., & HuanGuo, Z. (2013, November). A trusted VM-vTPM live migration protocol in clouds. In *1st International Workshop on Cloud Computing and Information Security*. Atlantis Press.

[24] Wang, X., Chen, X., Wu, W., An, N., & Wang, L. (2015). Cooperative application execution in mobile cloud computing: A Stackelberg game approach. *IEEE Communications Letters*, *20*(5), 946-949.

[25] Minarolli, D., &Freisleben, B. (2014, February). Distributed resource allocation to virtual

machines via artificial neural networks. In *2014 22nd Euromicro International Conference on Parallel, Distributed, and Network-Based Processing* (pp. 490-499). IEEE.

[26] Liu, Z., & Li, H. X. (2005). A probabilistic fuzzy logic system for modeling and control. *IEEE Transactions on Fuzzy Systems*, *13*(6), 848-859.