# Multi-Agent Intrusion Detection and Prevention System for Cloud Environment

K.Venkataramana
Research Scholar
Department of Computer Science
S.V.University,Tirupati,A.P India

M.Padmavathamma
Phd,Research SupervisorHead,Department of Computer Science
S.V.University,Tirupati A.P India

## ABSTRACT
Cloud computing is a type of distributed computing approach for IT Sector that leverages in efficient pooling of on-demand, self-managed virtual Infrastructures consuming them as a service by applications/organizations which would save thousands of dollars on CapEx and OpEx. To adopt this new cloud technology main concern for the consumers is the cloud computing security and it is the responsibility for the service providers to secure the cloud make it available at all time without interruption. In cloud computing all resources are virtualized by Hypervisor by creating Virtual machines, but its vulnerabilities raises many questions relating to security due to intrusion of malwares which allows security breaches. In this paper we propose Multi-Agent Intrusion Detection and Prevention System(MA-IDPS) by using Agents which will prevent security breach in Cloud due to attacks from intruder malware programs. Our system will be deployed at every instance of VM as well as at the client node end to detect and prevent intrusions due to malicious programs by an IDPS agents. This MA-IDPS model not only protects the cloud environment but also secures its agents and encrypts data tables that are part of IDPS by placing them in secure environment like Agent Runtime Environment (ARE) and Root VM respectively.MA-IDPS agent reports or prevents any abnormal behavior to Cloud administrator for further action. The proposed model secures the cloud from outside attacks either from client side or by a malware programs created in VM's

## General Terms
Cloud computing, Security, Intrusion Detection and prevention System, Agent based technology.

## Keywords
Intrusion Detection, Agents, cloud computing, Hypervisor, Modified BM algorithm, DLP, Smart Agent, User behavior.

## 1. INTRODUCTION
Cloud computing has evolved one of novel computing paradigm which enables IT managers to provision services to users in less time in a cost-effective way. Cloud is a significant step in the evolution of computing paradigms and a revolution in delivering IT services. Virtualization plays a vital role in creating cloud applications which can dynamically consumes resources when required for providing services such as SaaS, PaaS ,IaaS. Commonly used Virtualization technologies are from VMWare, the open source community (Xen, Virtualbox), Citrix, and Microsoft. Despite concerns from many security professionals, cloud computing isn't innately more or less secure. But the cloud model does force a movement toward a more robust and capable foundation of security services. Excitement of using new technology should not lead to overlook the gaps and issues that may lead to breach of security regarding data and applications running in environment. Main security is the concerns because of their operational models, the enabling technologies, and their distributed nature, clouds are easy targets for intruders. While intrusions can be handled by an Intrusion Detection System (IDS) [1], current IDSs have many deficiencies which hinder their adoption in a cloud environment. As the Internet forms the basic requirement for Cloud Computing, existing technologies can be imbibed into cloud computing to find remedies for some of the security threats.

The existing agent based technology is already using in distributed applications that runs on internet has prompted us for this work. In agent based technology an agent is defined as a computer system or a software program that is capable of performing autonomous (independent) actions, that will, decide for itself and figuring out what needs to be done to satisfy its design objectives [2]. A multiagent system consists of a number of agents, which interact with one another to complete a task [2]. To successfully interact, agents require the ability to cooperate, coordinate, and negotiate with each other. Cooperation is the process when several agents work together and draw on the broad collection of their knowledge and capabilities to achieve a common goal[3]. Multi-agent Systems are increasingly becoming popular in carrying valuable and secured data over the network. Because of the open and dynamic nature, cloud computing can leverage from using MAS[4] in various ways as one of its way can be in security which we used in developing MA-IDPS.

IDPS technologies commonly uses signature-based, anomaly-based or stateful protocol analysis based methodologies to detect the incidents. On the way IDPSs are deployed they are classified as: (1) Host-based IDS (HIDS) detect an intrusion at a single host by monitoring network traffic (only for that host), system logs, running processes, application activity, file access and modification etc., .(2) Network-based IDS (NIDS), monitors network traffic for particular network segments or devices and analyzes the network and application protocol activity to identify suspicious activity and informs to firewalls at the network boundaries.(3) Distributed IDS (DIDS) which integrates both types of sensors. DIDS can be categorized as Mobile Agent IDS (MAIDS), Grid based IDS (GIDS), and recently Cloud based IDS.

Traditional NIDS and HIDS cannot identify suspicious activities in a cloud environment due to its dynamic nature. So in this paper we have proposed Multi-Agent Intrusion Detection and Prevention System which uses signature- based, Anomaly-behavior based methodologies for a Cloud to deal with attacks like: (1) Masquerade attacks: where threats impersonate legitimate users, (2) Host-based attacks: these

can be a consequence of masquerade attacks and generally result in an observable user behavior anomaly and (3) Network-based attacks with intruders trying to penetrate into network. MA-IDPS is a agent based system than can be distributed across nodes in cloud for better performance than other IDPS systems. The remainder of this paper is organized as follows. Section 2 presents our brief literature survey done for proposing our model. In Section 3 we have specified architecture of MA-IDPS, Section 4 gives working of our model, Section 5 specifies working of MA-IDPS when deployed in cloud, Section-6 gives brief security analysis and in Section 7 we have summarized our proposed model and the future work.

## 2. RELATED WORK

In the research paper by XueJing and Ziang jian-jun[5] has given comprehensive survey about cloud security issues and their implication at various levels. The study about various vulnerabilities and defects in current security controls in cloud computing is discussed in paper by Grobauer, B.et al.[6] give us the information regarding some of vulnerabilities for IAAA service. In a recent research paper by, Rocha and Correia [7] showed how malicious insiders can steal confidential data. They demonstrated a set of attacks with attack videos, showing how easily an insider can obtain passwords, cryptographic keys and files etc.

In their paper by Anup gosh and chris greamo[8] has focused on how malware effect cloud computing environment, how they can be minimized by using sandboxing at client side at browser level. In the article A multi-agent based system for intrusion detection by Islam M.Hegazy et al [9] has described a framework for intrusion detection using agent based technology. Due to dynamic nature of agents and similar characteristics of cloud makes possible to use agents for IDPS in our model. In research article by Hisham A.Kholidy et.al[10] has proposed a framework for Intrusion Detection in cloud systems where IDS is deployed at all the nodes including database which should also be secured. In paper an autonomous agent based incident detection system for cloud environments[11] has proposed agent based model with sensors by monitoring business flows customer behavior can be predicted can determine DoS attacks. By considering above study we have proposed this model Multi-Agent Intrusion and Detection System(MA-IDPS) using agents for cloud which will minimize and prevent attacks from intruders. We proposed this model at Infrastructure level which forms the basis for PaaS and SaaS.

## 3.ARCHITECTURE OF MA-IDPS

In cloud computing both service providers and clients should secure the resources from malicious attacks by unauthorized elements. As it is a requirement for Cloud Computing environment to have Intrusion Detection and Prevention System to detect attacks on their services, we are proposing this IDPS using Multiple Agents to overcome attacks.

Our MA-IDPS Model consist of Software agents running in Agent Runtime Environment (ARE). ARE is part of IDPS which will create, destroy and allow agents to run securely thus protecting it from outside attacks. ARE will allow execution of agents that is part of IDPS. The Communication between agents in IDPS is done by IDMEF (Intrusion Detection Message exchange Format) message which is based on XML schema provided by RFC[12]. At client side it is Client Agent Runtime Environment (CARE) that acts as sandbox which allows execution of Smart Agent securely.

The proposed MA-IDPS is shown in figure-1 contains following agents and components

1.Knowledge Data Table(KDT): KDT contains data regarding malware signature patterns learned. It is be updated by UA after detecting of abnormal behavior or new signature by an analyzer agent (AA) by using MBM algorithm.

2. Behavioral Data Table(BDT): BDT contains data regarding rules ,Behavioral patterns learned and updated by UA during training period for matching and detection of abnormal behavior using fuzzy logic ART algorithm.

3.Smart Agent (SA): SA is an intelligent agent present at client node or in a node which is part of Cloud. SA will probe user behavior and abnormal activities in Node by examining OS logs etc., and sends it to IDPS for verification. SA will act like a mobile agent it will be returned upon client exit or node exit.

4. Verifier Agent(VA): VA will verify the identity of SA before the data is sent to IDPS in VM from node in a cloud to avoid intrusion of unauthorized agent.

5. Update Agent(UA): UA agent will update KDT and BDT in IDPS database for new malware signatures or behavior patterns from other resources or training data sets.

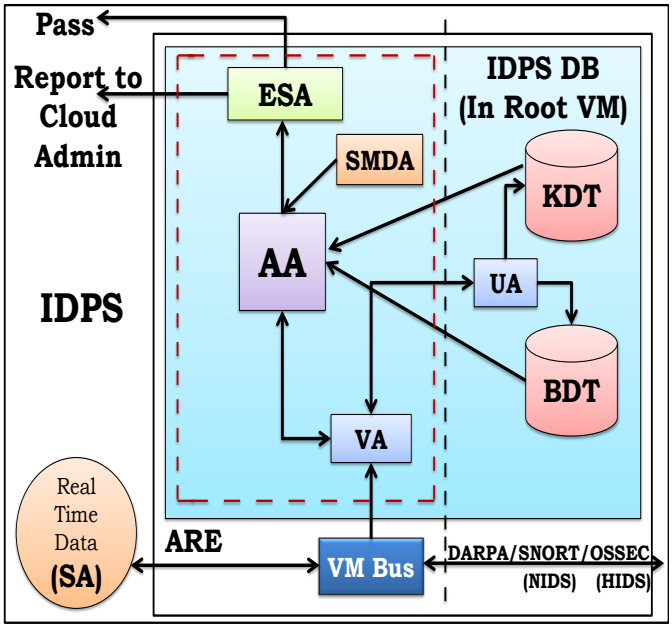


**Fig. 1:Proposed Model for MA-IDPS**

6.Analyzer Agent(AA): AA will accept each packet or data to detect attack or to find abnormal behaviour pattern which may cause security breach by comparing the data in KDT and BDT. AA will raise an event to ESA or allows to perform action based on result of comparison. AA uses Pattern matching and Fuzzy logic inference techniques to detect and prevent possible intrusions.

7.Event Signaling Agent(ESA): ESA receives event from AA either to allow the process for execution or report to Cloud admin about the severity of attack and course of action to be taken.

8. Smart Malware Detection Agent(SMDA): SMDA is a daemon agent which runs in regular intervals in system hosting IDPS which will find out any malware process or action attacking the IDPS and transfers the actions to AA which will in turn do the necessary action to prevent attack.

In MA-IDPS agents are created, destroyed and executed securely in Agent Runtime Environment. ARE is created for every instance of IDPS in cloud. Agents are communicated through VMBus between VM's and Hypervisor.

**Table-1 Notations used in IDPS model**

| Notation | Description |
|---|---|
| MA | Multi Agent |
| ARE | Agent Runtime Environment |
| CARE | Client Side ARE |
| KDT | Knowledge Data table |
| BDT | Behavior Data Table |
| AgId | Agent ID |
| Agtable | Agent table in memory which store ids for agents created |
| UA | Update Agent |
| VA | Verifier Agent |
| AA | Analyzer Agent |
| SMDA | Smart Malware Detection Agent |
| SA | Smart Agent |

# 4. WORKING OF MA-IDPS

Multi-Agent Intrusion Detection and Prevention System when deployed ARE is created for each instance in VM which in turns creates multiple autonomous software agents that can interact together to learn or to exchange experiences. ARE acts as a Sand Box which allows only agents of IDPS will be executed with special Id code. Agents are created dynamically and their ids are stored in Agent table(Agtable) which are indexed by using hash function. As we modeled IDPS to be used in Cloud/Grid Computing Environments which contains various nodes or client applications running on different Virtual Machines or any devices which access services. Our Proposed IDPS has two parts First Part contains ARE part which contains various agents discussed in above section such as Smart Agent(SA),Verifier Agent(VA), Update Agent (UA), Analyzer Agent(AA), Event Signaling Agent(ESA),Smart Malware Detection Agent (SMDA) which will prevent Intrusion and prevent attacks in node where IDPS is deployed and Second part contains Database part which contains Tables KDT and BDT for storing signatures, rules ,policies.

Initially IDPS will be in Learning state in which Knowledge Data Table (KDT) and Behaviour Data Table (BDT) will be updated with datasets by Update Agent(UA) by the data available from existing SNORT/OSSEC or by DARPA which obtained data from IDSs submitted by six research groups in 1998[13].Both KDT and BDT are part of IDPS database which are secured by Encryption mechanism. UA uses Adaptive Resonance Theory (ART)[14] neural network classifier (developed by Grossberg [15,16] to group presented patterns into categories without human supervision. ART is one type of an unsupervised neural network that uses competitive learning. A pattern that does not closely match any of the known categories causes the network to add a new category during the learning phase.UA converts patterns into fuzzy rules add it to BDT. Each rule in are expressed as a logic implication p-> q where p is called the antecedent of the rule and q is called the consequence of the rule. The rule structures are based on Zadeh[17].

When IDPS deployed Agents are created and executed in ARE. While at client node it is known as Client Agent Runtime Environment(CARE) which runs Smart Agent (SA) upon client login or node usage. SA is a Mobile agent which collect user behaviour data like sequences of striking the keyboard , user trying to logging into system with different passwords and data from log files from host OS return back to IDPS system at regular intervals to detect malicious user.

When ARE creates an agent it computes AgID as given in algorithm and it is stored Hashed indexed table known as Agent table (Agtable) at index given by hash value of agent code. Agtable is accessible by all the agents of that IDPS instance. SA is verified by VA with SA ID-code with the values in Agtable which is stored in encrypted format.

## 4.1 Verifier Agent Algorithm

This algorithm is used by Verifier Agent for verifying / authenticating id of each agent transferring data into IDPS in VM so that outsider agent is avoided to enter into the system.

1. Begin

[AgentId Gen Phase]

2. VA computes AgId= $g^{k1}*g^{k2}$ mod p where p is a large prime, and $g^{k1}$, $g^{k2}$ are primitive roots in $Z_p^*$.
3. ID for each Smart Agent is computed as SgID= $g^{k2}$ mod p and added to it for verification.
4. Compute indx=H(SgId) where SgID is ID given to smart agent or any agent code in ASCII value and H is a hash function.
5. Agtable[indx,0]=AgId, Agtable[indx,1]=g, Agtable[indx,2]=k1,Agtable[indx,3]=p

[ Agent Verification Phase]

6. When SA return with data from node it is verified as indx=H(SgId)
7. Compute tid= $g^{k1}$ mod p by retrieving from Agtable[indx]
8. If( Agtable[indx,0]<>tid*SgID) then
9. SA is a foreign Agent it is destroyed or killed and event is logged into logfile about incident
   Else
10. SA 's data is passed to Analyzer agent(AA) for further introspection.
11. End.

Analyzer agent analyses the incoming packets data or a pattern from SA for malware signatures or for any abnormal behaviour by client by comparing it with data in KDT or BDT. AA uses modified version of BM algorithm[13] for pattern matching and AI technique ART for behaviour goal matching using heuristics.

## 4.2 MBM Algorithm

This algorithm is used by AA to matches input with the malwares or virus patterns stored in KDT against the packet or data to be examined when it is sent into IDPS by agents.

Input : A packet/Message from SA to be processed by VM in cloud.

Result: AA will drops packet or message if it matches with the pattern n KDT by applying MBM .

**MBM algorithm** used by AA is based on

a) Looking-glass heuristic: Compare ***P*** with a subsequence of ***T*** moving backwards

b)Character-jump heuristic: When a mismatch occurs at ***T***[***i***] = ***c***,

If ***P*** contains ***c***, shift ***P*** to align **P[**0] with next position to the last occurrence of ***c*** in ***P*** with ***T***[***i***]

Else

shift ***P*** to align ***P***[0] with ***T***[***i*** + 1].

*MBMPatternMatchAlgorithm(T,P)*
T: Represents a record in KDT which contains known malware patterns to be compared with Pattern P contained in Packet received by AA from client/application.

```
1.begin
2. L=LastFindFunction (p), returns index of last
   occurrence of P
3.Initialize si=m-1
4. pl=m-1, where m is the length of Pattern to matched with T.
5.Set Flag=false
6. while not EOF( KDT) and flag=false
7. Read T from KDT
8. Repeat steps 9 to 17 until (si>m-1)
9. If(T[si]=P[pl]) then
10.                 If (pl=0) then
11                          flag=true
12                          break;
                    Else
13                          si=si-1
14                          pl=pl-1
                    Endif
    Else
15.         l=L[T[si]]
16.         si=si+1-min(pl,l)
17.         pl=m-1
    Endif
    EndRepeat
    EndWhile
18 . If (flag=true) then
19  AA raises alert to ESA and ESA reports packet
      as Malicious to Cloud Admin, adds activity to
      Log and drops packet.
      else
20.     Packet is Passed for processing in VM.
    Endif
21. end.
```

Analyzer agent works as a fuzzy controller [17] to make decisions and possibly take action based on anomalous behavior. AA agent sends reports of security incidents, including the severity of the event to ESA. ESA uses various incident characteristics like severity of event, attack time, user behaviour to make a decision to take some action, such as terminate a process, or do nothing, based on the AA input and reports to Cloud administrator for some action. AA also inspects protocol packet headers (e.g., TCP, UDP, or ICMP) to detect anomalies. Every network protocol can be modeled as a sequence of finite state transitions that defines its normal behavior. Thus any break in the rules of the state machine is considered as malicious behavior.
IDPS uses the SMDA to check VM's memory for any malware or virus and reports to AA for further action. If VM having IDPS is attacked by intruder SMDA will check the Memory usage statistics , log files, SLA for any deviation will signal AA for self-destruction of VM. SMDA will close the ports after scanning ports in VM which are idle for over a period of time and avoid intrusion by a malwares in cloud domain.

## 5. DEPLOYMENT OF MA-IDPS IN CLOUD

In this paper we have taken Microsoft Hyper-V architecture[18][19] for modeling and using Multi Agent Intrusion Detection and prevention system, but it can be used in VMWare architecture also with slight modifications. Our model of MA-IDPS can be used in any cloud model as given in Fig-2 when deployed. Hyper-V supports isolation in terms of a partition. A partition is a logical unit of isolation, supported by the hypervisor, in which operating systems execute. The Microsoft hypervisor must have at least one parent, or root, partition, running Windows Server 2008 64-bit Edition.

The virtualization stack runs in the parent partition and has direct access to the hardware devices. The root partition then creates the child partitions which host the guest operating systems. A root partition creates child partitions using the hypercall application programming interface (API)[18].
MA-IDPS will be deployed in Hyper-V architecture as given in Fig-2, where the IDPS database present in Root Partition which will be updated by UA running in ARE from other agents through VMBus which acts as main communication channel between VM's and Root VM.
In Hyper-V Root VM will control other VM's. IDPS is deployed in all guest VM's running client applications or VM's having domains running client applications except the IDPS DB is present in Root VM thus protecting it from external attacks. The communication between VM's in Hyper-V architecture is done through VMBUS. The agents in Hypervisor also uses the same VMBus for communication.

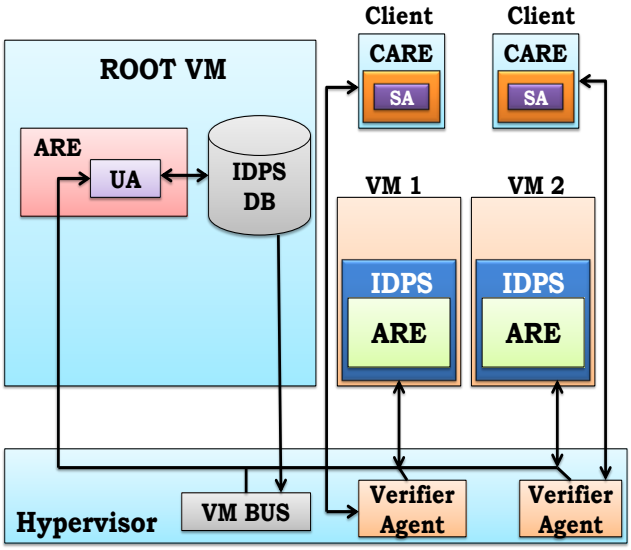


**Fig. 2: MA-IDPS Deployed in Cloud**

Verifier agents (VA) running in Hypervisor will perform required verification and authentication of agents carrying data into IDPS to prevent intrusion by an malware program from guest VM's or from client nodes.
At the clients nodes IDPS deploys Smart Agent (SA) which will run in Client Agent Runtime Environment (CARE) which acts like a Sand box for protecting itself from attack and scans the node for possible malware programs or abnormal user behavior and is reported to AA in domain in which client is related to.

## 6. SECURITY ANALYSIS

In the proposed MA-IDPS model we have addressed the two issues of security relating to agents and database in IDPS which are not properly discussed in previous works. The first issue relating to agent security in the existing works, they have focused on securing the deployed system but not the agents itself that are part of IDPS. There is possibility that agent can be modified or new agent can be introduced by an intruder into the system which will destroy entire IDPS or its

main aim of protection. So in our model we have secured agent verifying it by using Verifier Agent and also agents are secured by running them in Secure runtime environment like ARE,CARE. IDPS allow execution of agents created in secure environment and every agent will be given an agent id which will be verified by VA in hypervisor or in root VM. All the process in VM's are executed only after authenticated by AA.
The Second issue is database that compromises the IDPS which should be secure and correct to identify the threats or intruders, so in our model we have positioned the database at root VM which is highly protected and also data in it is encrypted. Database is accessed only by agents in IDPS not by any program or process, where as in other works discussed earlier the database is positioned at every node which may rise many security problems.
MA-IDPS model for cloud computing environment is resilience to following attacks like
a)Malware Attacks: it is prevented by SMDA which will check memory of VM against any malware signature by checking its memory attributes and handed it over to AA which will kill the malware process by checking it against the signature in KDB. Even at client side also SA will prevent malware attacks as it checks and verifies every process.
b) DOS Attacks: as the verifier agent receives packet only from authenticated agent it will not allow unauthorized requests and it will be denied by VA itself and hence this type of attacks will be minimized.
c) Port Open attacks: Whenever opened ports are in idle state there is a possibility that intruder can attack the VM, so as to overcome this attack we have SMDA running in VM which will scan all the open ports in VM and the ports are forced to close which are idle for over a period of time without a request due to various reasons at client side or due to network traffic.
d) Masquerade attacks is not possible as the every request is through SA in client node which will be authenticated by VA.
d)Root-Kit attacks: this type of attacks are eliminated as the SMDA will scan entire OS memory for any presence rootkit malware unauthorized process and report it to Analyzer agent for action.
SA at client will reports abnormal behavior of attacker or trying to known password of genuine user to IDPS in VM to which client belongs thus reducing intrusion by illegitimate user.

## 7. CONCLUSION

Even though this new cloud computing technology reduces the expenditure for IT-Industry there main concerns are regarding with cloud Security. To make consumers to use this technology it is the responsibility for the service providers to ensure that cloud environment is secure and available at all time without interruption that may cause due to threats. So by analyzing various models of IDPS we have proposed this MA-IDPS by using agents for cloud environment at Infrastructure level which forms base for cloud applications. Our proposed Agents in IDPS are intelligent enough to avoid attacks and secure cloud from various attacks. MA-IDPS can be deployed in all cloud models as the problem of security has same impact. In our future extension to this work we will try to practically deploy this IPDS model in cloud nodes by using open cloud resources.

## 8.ACKNOWLEDGMENTS

My sincere thanks to my research supervisor Dr.M.Padmavathamma who have helped with her valuable suggestions and contributed towards the development of this IDPS model.

## 9.REFERENCES

[1] Karen Scarfone and Peter Mell, 800-94, Feb. 2007 "Guide to Intrusion Detection and Prevention Systems (IDPS)",National Institute of Standards and Technology(NIST),Special Publication.

[2] M.Wooldridge, 2009 , "An Introduction to Multi-Agent Systems", second ed., JohnWiley & Sons Ltd,Chichester, England

[3] [3] Kwang Mong Sim Senior Member, p78-81,March/April 2012,"Agent-Based Cloud Computing, IEEE
Computing", IEEE Transactions On Services Computing,2011

[4] Domenico Talia, "Clouds Meet Agents",2012 IEEE Internet Computing

[5] XueJing,Zhang Jian-jun, P 475-478,2010,"A Brief Survey on the Security model of cloud Computing, International symposium on Distributed computing and applications to business IEEE computer society

[6] Grobauer.B Walloschek.T. Stocker.E,2011,"understanding Cloud Computing Vulnerabilities",Security & Privacy, Volume:9 Issue:2,IEEE

[7] F.Rocha,M. Correia,2011,Lucy in the sky without diamonds: Stealing confidential data in the cloud.

[8] Anup ghosh, Chrish greamo, page 79-82, 2011, "Sandboxing and Virtualization", Security and privacy,IEEE.

[9] Islam M. Hegazy, Taha Al-Arif, Zaki.,T. Fayed, and Hossam M. Faheem ,Oct-Nov 2003,"Multi-agent based system for intrusion Detection" ,Conference Proceedings of ISDA03, IEEE.

[10] Hisham A. Kholidy, Fabrizio Baiardi, 2012 CIDS: "A Framework for Intrusion and Detection in cloud Systems", 9th International Conference on Inform-ation Technology- New Generations,IEEE.

[11] Frank Doelitzscher∗, Christoph Reich∗, MartinKnahl and Nathan Clarke, p197-204, 2011,"An autonomous agent based incident detection system for cloud environments", 3rd IEEE International Conference on Cloud Computing Technology and Science

[12] H.Debar,D. Curry, 2007, Network WorkingGroup Secure Works, Inc.http://www.ietf.org/rfc/rfc4765.txt

[13] Feng Du, 2012, "An Effective pattern matching algorithm for Intrusion Detection", International conference on Computer sciences and Electronic Engineering, IEEE.

[14] Dipankar Dasgupta and Hal Brian, "Mobile Security Agents for Network Traffic Analysis", Intelligent Security Systems Research Group

[15] D. Saha and A. Mukherjee, 2003 "Pervasive Computing: A Paradigm for the 21st Century Computer, vol. 36, pp. 25-31

[16] Grossberg, S., ed.,1988 Neural Networks and Natural Intelligence, MIT Press, Cambridge,Massachusetts.

[17] Zadeh, L.,1994 Fuzzy Logic, Neural Networks and Soft Computing, Communications of the ACM, Vol. 37, No. 3, pp.77-84, 1994.

[18] Brendon Baker ,"Windows Server Virtualization & The windows Hypervisor", http://www.blackhat.com/presentations/bhusa07/Baker/Presentation/BH07_Baker_WSV_Hypervisor_Achitecture.pdf

[19] Microsoft Hyper-V Architecture, referred at http://en.wikipedia.org/wiki/Hyper-V