IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-6, Issue-4 E-ISSN: 2347-2693

Proposing Cloud Based Intrusion Detection System for Tracing Intruder Attacks

A. K. Chaturvedi[1*], F.A. Lone[2]

[1]MCA Dept., Govt. Engineering College, Ajmer, India|
[2]CS Dept., Mewar University, Chittorgarh, Rajasthan, India

*Corresponding Author: amit0581@gmail.com

Available online at: www.ijcseonline.org

Received: 13/Mar/2018, Revised: 21/Mar/2018, Accepted: 04/Apr/2018, Published: 30/Apr/2018

***Abstract* —** Before proposing a new model and implementing it in the Intrusion Detection Systems, First find out how intrusion detection is performed on Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) offerings, along with the available host, network and hypervisor-based intrusion detection options. The ability to perform intrusion detection in the cloud is heavily dependent on the model of cloud computing. In cloud computing, most of the attacks till today traced are the remote attacks. In this paper, we are proposing a model for Cloud Based Intruder Detection System [CBIDS]. This model is created for tracing the attacks on the online storage at SaaS and PaaS layer of cloud computing and appropriately the recommended action will be taken to protect the stored data and executing the handler accordingly. Further modifications in this model will be done on the basis of obtaining requirements and gaps in tracing the attacks.

***Keywords*—**Cloud, Intruder, IDS, Intrusion Detection System, HIDS, NIDS, Attack.

I. INTRODUCTION

Introduction: The use of online services either in banking, entertainment, social networking, education, marketing etc is very much popular now. As the number of internet users increases the online data increases rapidly than before. Every day millions of images, videos, and business data uploaded or added and downloaded to the online storage.

Before proposing new and implementing it in the Intrusion Detection Systems in a cloud computing environment. First find out how intrusion detection is performed on Software as a Service, Platform as a Service and Infrastructure as a Service offerings, along with the available host, network and hypervisor-based intrusion detection options. Attacks on systems and data are a reality in the world we live in. Detecting and responding to those attacks has become the norm and is considered due diligence when it comes to security. As a matter of fact, most of the standards and regulations applied in the technology space today have explicit instructions regarding the need for monitoring and alerting, or intrusion detection.

The ability to perform intrusion detection (ID) in the cloud is heavily dependent on the model of cloud computing you are using:

Software as a Service (SaaS): The reality is that SaaS users must rely almost exclusively on their providers to perform intrusion detection (ID). You may have the option of getting some logs and deploying a custom monitoring and alerting on that information, but most intrusion detection (ID) will be done by the provider.

Platform as a Service (PaaS): Like SaaS, most of the intrusion detection (ID) for this level of service will be done by the provider. Since intrusion detection systems (IDS) are typically outside the application, you must rely on your provider to deploy IDS in a PaaS. You can, however, configure your applications and platforms to log onto a central location where you can then set up monitoring and alerting (i.e., where you can perform ID).

Infrastructure as a Service (IaaS): This is your most flexible model for intrusion detection (ID) deployment. Unlike the other two, IaaS gives you more options as a consumer. This is where we will spend most of this article.

In IaaS the intrusion detection can be performed at four primary spots : (1) in the virtual machine itself, (2) In the hypervisor or host system, (3) in the virtual network, and (4) in the tradition network. In the virtual machine it allows to monitor the activity of the system and detect and alert on issues that may arise. In hypervisor or host system, it allows

to monitor the hypervisor and anything happened between VMs and the hypervisor. In the virtual network, it allows to monitor the network traffic between the VMs on the host and the traffic between the VMs and the host. In the traditional network, it allows you to monitor, detect, and alert on traffic that passes over the network infrastructure.

So, Intrusion detection can be performed in the cloud in three possible ways. The first option is the traditional host intrusion detection system (HIDS). You can use a HIDS on the VM, as well as the host/hypervisor. The HIDS on the VM would be deployed, managed and monitored by you. The HIDS on the hypervisor would be the responsibility of your provider. If you desire to incorporate any of the hypervisor ID information in your IDS, then you would have to coordinate with your provider. In reality, it is likely that you will not get that information, so the contract with your provider will need to ensure that they are performing adequate monitoring and alerting. Deploying and managing a HIDS on the VM would be the customer's responsibility, while HIDS on the hypervisor would fall under the responsibility of the provider.

A second option is a traditional network intrusion detection system (NIDS). This type of deployment is useful in detecting some attacks on the VMs and hypervisor. It does, however, have several limitations. The first is that it cannot help when it comes to attacks within a virtual network that runs entirely within the hypervisor. Second, it has very limited visibility into the host itself. Lastly, if the network traffic is encrypted, there is really no effective way for the NIDS to decrypt the traffic for analysis. In the cloud, NIDS falls completely in the realm of the provider to deploy and manage.

The third option would be the use of an intrusion detection system that runs at the hypervisor layer but is not strictly a HIDS for the hypervisor. One of the promising technologies in this area is the use of VM introspection. This type of IDS allows you to monitor and analyze communications between VMs, between hypervisor and VM and within the hypervisor based virtual network. The advantage of hypervisor-based ID is the availability of information, as it can see basically everything. The disadvantage is that the technology is new and you really need to know what you are looking for. As with NIDS, this falls completely within the scope of the provider to deploy and manage.

In reality, intrusion detection in the cloud is best performed by the provider. They have the hooks where the important stuff happens. ID based on VM introspection is probably the most promising technology on the horizon in terms of an instruction detection system for the cloud.

The security of data or privacy preserving is the basic necessity in cloud computing. To understand the security requirements in cloud computing, one should understand about the vulnerability, attacks, mapping of attackers, and available tools to secure it. Intruder Detection System uses mobile agent sand using three types of honeypots in order to detect attacks, behaviour of attackers, increase the added value of honeypot and IDS based mobile agents, solve systems limitations of intrusion detection, improve knowledge bases IDS thus increase the detection rate in our cloud environment [2]. IaaS providers offer their customers variety of services like continuous network access, storage. A registration process is coupled with network access to setup authentication to use the cloud services. But Spammers, malicious code authors and other criminals do their activities by playing with anonymity behind the registration process and usage models. PaaS providers have traditionally suffered most from such attacks and recent studies shows that hackers have begun targeting IaaS providers as well. Future areas of concern include password and key cracking, DDoS, launching dynamic attack points, hosting malicious data and botnet command and control. The SaaS providers expose a set of APIs and software interfaces that customers use to manage and interact with cloud services computing which allows for exactly the methods used by hackers to compromise systems with clouds, their motivations and attitudes to the compromised machine [3]. There are three important forms of the cloud: (1) The public cloud is the first to appear, its principle is to host Web applications on a shared environment with an unlimited number of users (e.g. Amazon, Google, etc.)[4]. The private cloud is an environment deployed within a company. Implement a private cloud means the transformation of the internal infrastructure using technologies such as virtualization to deliver on-demand services in a simple and fast way [3]. The hybrid cloud allows the coexistence and communication between a private cloud and a public cloud in an organization sharing data and applications [5].

The contribution of IAAS infrastructure as a service of private cloud OpenStack which combines the Intrusion Detection System (IDS) based on mobile agent with three basic types of honeypots: honeyd, honeycomb and Honeywall. The purpose of this paper is to combine the different security challenges in a cloud environment by using: - IDS based on mobile agent that combines two types of intrusion detection "Behavioral and scenarios" in one IDS [4]; - Honeyd to attract all types of hackers to our work environment [6]; - The Honeywall which has several features at the same time to facilitate the detection of several types of intrusion in our system [3]; - The honeycomb in order to generate new signatures [7].

II. Related Work

S. Khan, K. A. Shakil and M. Alam, presented a survey of current research and future directions on cloud-based big data analytics. They discussed that the advent of the digital age has led to a rise in different types of data with every passing day. In fact, it is expected that half of the total data will be on the cloud by 2016. This data is complex and needs to be stored, processed and analyzed for information that can be used by organizations. Cloud computing provides an apt platform for big data analytics in view of the storage and computing requirements of the latter. This makes cloud-based analytics a viable research field. However, several issues need to be addressed and risks need to be mitigated before practical applications of this synergistic model can be popularly used. This paper explores the existing research, challenges, open issues and future research direction for this field of study.

U. Sivarajah, M. M. Kamal, Z. Irani, V. Weerakkody, explained the Critical analysis of Big Data challenges and analytical methods. Big Data (BD), with their potential to ascertain valued insights for enhanced decision-making process, have recently attracted substantial interest from both academics and practitioners. Big Data Analytics (BDA) is increasingly becoming a trending practice that many organizations are adopting with the purpose of constructing valuable information from BD. The analytics process, including the deployment and use of BDA tools, is seen by organizations as a tool to improve operational efficiency though it has strategic potential, drive new revenue streams and gain competitive advantages over business rivals. However, there are different types of analytic applications to consider. Therefore, prior to hasty use and buying costly BD tools, there is a need for organizations to first understand the BDA landscape.Given the significant nature of the BDand BDA, this paper presents a state-of-the-art review that presents a holistic view of the BD challenges and BDA methods theorized/proposed/employed by organizations to help others understand this landscape with the objective of making robust investment decisions. In doing so, systematically analysing and synthesizing the extant research published on BD and BDA area. More specifically, the authors seek to answer the following two principal questions: Q1 –What are the different types of BD challenges theorized/proposed/confronted by organizations? and Q2 – What are the different types of BDA methods theorized/proposed/employed to overcome BD challenges?. This systematic literature review (SLR) is carried out through observing and understanding the past trends and extant patterns/themes in the BDA research area, evaluating contributions, summarizing knowledge, thereby identifying limitations, implications and potential further research avenues to support the academic community in exploring research themes/patterns. Thus, to trace the implementation of BD strategies, a profiling method is employed to analyze articles (published in English-speaking peer-reviewed journals between 1996 and 2015) extracted from the Scopus database. The analysis presented in this paper has identified relevant BD research studies that have contributed both conceptually and empirically to the expansion and accrual of intellectual wealth to the BDA in technology and organizational resource management discipline.

Y.Mehmood, U. Habiba, M.A.Shibli, R. Masood, presented a study on "Intrusion Detection System in Cloud Computing: Challenges and Opportunities". Today, Cloud Computing is the preferred choice of every IT organization since it provides flexible and pay-per-use based services to its users. However, the security and privacy is a major hurdle in its success because of its open and distributed architecture that is vulnerable to intruders. Intrusion Detection System (IDS) is the most commonly used mechanism to detect attacks on cloud. This paper provides an overview of different intrusions in cloud. Then, we analyze some existing cloud based intrusion detection systems (IDS) with respect to their type, positioning, detection time, detection technique, data source and attacks they can detect. The analysis also provides limitations of each technique to evaluate whether they fulfill the security requirements of cloud computing environment or not. We emphasize the deployment of IDS that uses multiple detection methods to cope with security challenges in cloud.

Z. Tan, X. He, P. Nanda, J. Hu proposed enhancing Big Data Security with Collaborative Intrusion Detection. They presented that a collaborative intrusion detection system (CIDS) plays an important role in providing comprehensive security for data residing on cloud networks, from attack prevention to attack detection. To ensure that the CIDS is resistant to compromise, we use authentication and encryption as well as an integrity check. Because the CIDS works 24/7, energy-efficient group key distribution schemes are preferable for secure key distribution and node authentication. These schemes provide a strong, secure mechanism for updating group keys when nodes join in or leave the network or a node is being compromised. They're also resilient to collusion attacks, in which multiple nodes are compromised and coordinated for attack. Finally, a backup central coordinator runs alongside the main coordinator to prevent a single point of failure. The coordinators' roles can be exchanged depending on actual requirements and network conditions.

Future studies will explore the framework's implementation and application on different cloud computing systems. Focuses of our future studies will be casted on algorithms for distributed and parallel data summarization on cloud computing, and their implementation on the MapReduce framework, as well as new detection approaches for HIDSs.

U. Oktay and O.K. Sahingoz, presented Attack Types and Intrusion Detection Systems in Cloud Computing. In recent years, lots of organizations have adopted their systems for enabling cloud based computing to provide scalable, virtualized on-demand access to a shared pool of computing resources such as networks, servers, storage, applications and services. Mainly cloud computing technology enables users/enterprises to eliminate the requirements for setting up of expensive computing infrastructure and reduces systems' operating costs. As a result, this technology is used by an increasing number of end users. On the other hand, existing security deficiencies and vulnerabilities of underlying technologies can leave an open door for intrusions. Therefore, cloud computing providers need to protect their users' sensitive data from insider or outsider attacks by installing an intrusion detection and prevention system. In this paper, it is aimed to define different attack types, which affect the availability, confidentiality and integrity of resources and services in cloud computing environment. Additionally, the paper also introduces related intrusion detection models to identify and prevent these types of attacks.

Neha, Mandeep Kaur, proposed an Enhanced Security using Hybrid Encryption Algorithm. Information Security plays a major role in today's scenario. Cloud computing is a technology that provides access to information and computing resources from anywhere that a network is available. There is a need to secure the data stored on cloud. The main goal behind the design of encryption algorithm must be security against unauthorized attacks. However, for all cloud computing applications, performance and cost of implementation are also major concerns. Encryption algorithm would not be of much use if it is very much secure but slow in performance. The security and performance of encryption algorithms must be balanced. In this paper, encryption algorithms (AES, Blowfish, Twofish) has been discussed to analyze the performance level of each algorithm.

C. Ambikavathi and S. K. Srivatsa, discussed Integrated Intrusion Detection Approach for Cloud Computing. Intrusion Detection System (IDS) models and methods are integrated for better detection of intruders and mitigation of false alarms. Integrated IDS is proposed to provide security in a cloud environment. The distributed and dynamic nature built-in of cloud environment leads to critical issues like huge log analysis, heterogeneous traffic aggregation and scalability, etc. Intrusion specific data classification and false alarms degrades performance. This integrated model integrates both IDS models and IDS methodologies. Host-based IDS (H-IDS) model integrates with network-based IDS (N-IDS) model, as well as signature and anomaly based IDS methods are integrated to get the best of each. Whenever a Virtual Machine (VM) is created, H-IDS is in-built into its operating system to monitor the activities within that VM. N-IDS is deployed at strategic locations within the cloud network to monitor the traffic between the virtual machines and from the outside environment. Any malicious activity initiated by a cloud user using their virtual machine is detected by H-IDS. The packets flowing through the cloud network are captured and analyzed by N-IDS to detect infected packets send by hackers. The weakness of one methodology is compromised by the other during integration, but if the methods are used separately they are ineffective. Known attacks can be detected by signature based IDS and the new/unknown attack patterns are identified by anomaly based IDS. The major drawback of anomaly based IDS is high false alarm rate. It can be overcome by signature based IDS. This proposed work is implemented using Opennebula, for constructing a cloud environment and tested with IDS tools. This integration leads to improve cloud security and trust among consumers. IDS specific issues are also rectified such as false alarms, heterogeneity etc.

Akash G Mohod1, Satish J Alaspurkar, presented an analysis of IDS for Cloud Computing. This seminar works on approach for obtaining optimal number of features to build an efficient model for intrusion detection system (IDS). Most Intrusion Detection Systems (IDSs) are designed to handle specific types of attacks. It is evident that no single technique can guarantee protection against future attacks. To handle large scale network access traffic and administrative control of data and application in cloud, a new multi-threaded distributed cloud IDS model has been proposed. Facing new application scenarios in cloud computing, the IDS approaches yield several problems since the operator of the IDS should be the user, not the administrator of the cloud infrastructure. Extensibility, efficient management, and compatibility to virtualization-based context need to be introduced into many existing IDS implementations.

S.N. Dhage, B.B. Meshram, discussed Intrusion detection system in cloud computing environment. In recent years, with the growing popularity of cloud computing, security in cloud has become an important issue. As 'prevention is better than cure', detecting and blocking an attack is better than responding to an attack after a system has been compromised. This paper proposes architecture capable of detecting intrusions, in a distributed cloud computing environment, and safeguarding it from possible security breaches. It deploys a separate instance of IDS for each user and uses a separate controller to manage the instances. IDS in this architecture can be signature-based as well as learning-based method.

T. Kuldeep, Tyagi S.S and Agrawal R., discussed the overview of Snort Intrusion Detection System in Cloud Environment. Now a day's cloud computing has become

very popular since it reduces infrastructure cost. Hence, the level of security measures also has to be increased. Intrusions Detection Systems (IDSs) are designed to handle attacks but many intrusion detection system (IDS) are designed for specific attack/attacks. It is evident that no single technique can guarantee protection against future attacks. To handle large scale network access traffic and administrative control of data and application in cloud, we have to develop a new cloud IDS model that can assure maximum security in cloud. In this paper we will talk about the snort IDS on Linux which ensure enough security, efficient management into virtualization based system.

A. Kaur, S. Singh, proposed an efficient data storage security algorithm using RSA algorithm. This paper gives a brief introduction about cloud computing by giving its definition, characteristics of cloud computing, components, types, categorization of cloud services which described Platform as a Service, Infrastructure as a Service and Software as a Service. By having a look at this paper, an individual surely will have a clear idea about the basics of cloud computing. Cloud computing is an emerging computing paradigm in which resources of the computing infrastructure are provided as services of the internet. Cloud computing allows consumers and businesses to use applications without installation and access their personal files at any computer with internet access. This paper explores various security methods such as Access Control, Telecommunications and Network Security, Information security governance and risk management, Application Security, Security Architecture and Design. An RSA system generally belongs to the category of PKCS. RSA encryption is one of the public-key methods that have been popular in last decade. In particular, the RSA algorithm is used in many applications. Although the security of RSA is beyond doubt, the evolution in computing power has caused a growth in the necessary key length. The performance characteristics of RSA are observed by implementing the algorithms for computation. In this paper, RSA was implemented through an encryption and decryption procedures over different key sizes.

A. Bhardwaj, GVB Subrahmanyam, V. Avasthi, H. Sastry, discussed Security Algorithms for Cloud Computing. With growing awareness and concerns regards to Cloud Computing and Information Security, there is growing awareness and usage of Security Algorithms into data systems and processes. This paper presents a brief overview and comparison of Cryptographic algorithms, with an emphasis on Symmetric algorithms which should be used for Cloud based applications and services that require data and link encryption. In this paper we review Symmetric and Asymmetric algorithms with emphasis on Symmetric Algorithms for security consideration on which one should be used for Cloud based applications and services that require data and link encryption.

J. Khan, H. Abbasa, J. Al-Muhtadia, presented Survey on Mobile User's Data Privacy Threats and Defense Mechanisms. Nowadays, mobile devices have become an integral part of our daily life. These have proven to be an advantageous scientific invention that fills personal and business needs in a very efficient manner. In this era, the availability of mobile services has significantly increased because of the rich variety of mobile devices and essential applications provided by mobile device manufacturers. At the same time, numerous mobile security issues and data privacy threats are challenging both manufacturers and users. Therefore, mobile devices are an ideal target for various security issues and data privacy threats in a mobile ecosystem. In this paper, we provide a brief survey of the security challenges, threats, and vulnerabilities of a mobile ecosystem. Furthermore, we discussed some key points required to ensure mobile security and defend against data privacy threats. The emphasis of the discussion is, strong protection and the restriction of malicious activity at the application developer end, application stores end, and operating system and mobile device manufactures end by preventing the user from using non-recommended applications (which may be malicious) and considering biometric features for the authentication of real users in the mobile devices. Also briefly discussing the defense mechanisms that are considered to be a relatively better approach for securing personal and business related data or information in the mobile devices.

Shuying Li, Ya Pan, presented a study on secure data storage based on cloud computing. With the advance of cloud computing technology, more economic benefits have been brought to users. While satisfying the needs of users, cloud computing brings its advantages-low costs, rapid deployment and flexible scale adjustment into full play. Increasing number of data is stored in all kinds of networks with more and more companies and people using cloud computing service, thus put severe challenge on users data security and availability. Under these circumstances, the study analyzed data security of users, and found out that data storage security attracts attentions both from private users and business users. The security challenges cloud computing has brought to us are how to prevent users' data from leaking, how to guarantee users obtain data efficiently and accurately. It introduced the research status of secure data storage under the circumstance of cloud computing. Surveys showed that experts and scholars have attached great attention to data security under this circumstance. Strategies on secure data transmission and storage based on cloud computing, including encryption and decryption processing, were also introduces in this paper. To protect user data security, structure model has been built and secure data storage system under cloud computing has also been introduced.

III. PROPOSED MODEL

In the Cloud computing environment, the deployment of already available Intrusion Detection and Prevention Systems (ID/PS) can't achieve the desired level of security and performance since architecture of cloud computing paradigm is different from existing computing methods like Grid computing. The rapidly growing demand of cloud resources by its users urges the need of some efficient mechanism for secure provisioning of its resources since intruders may compromise the cloud resources and can cause damages to users' data stored there. The effectiveness of IDS depends on aspects like the detection method, location of IDS in network, and its configuration [16].

In this paper, we are proposing a model for Cloud Based Intruder Detection System [CBIDS] as shown in Figure 1. According to this model, when a user interact with the system, first a connection or session is created, then the system asks for some registration information to the user. Then the system uses this registration information to sense the type of user, authentication status, and the authorization permitting in the system. If the user is authentic and authorize for accessing the modules he/she wants to access then it is allowed for that. But if the authenticity is obtained from different means i.e. cracking the security, then it is a serious issue and should be traced out.

Filtering and Analysis of Attacks process will filter out such cases, and if it predicted that this may be an attack. Then this attack will be detected by already created scenarios. There are already defined many type of common attacks called as Known Attacks. If the present attack comes in this category of attacks then it will be mapped into the database and the already decided action will be done and the predefined response will be send back to the user. But if the attack is now known i.e. Unknown attack, then the attack is analyzed by its behavior. After Evaluation, it is observed that the attack is Normal or Abnormal. If it is normal attack then the system will execute the handler for such attacks already decided and designed, and send the response to the user. If the attack is abnormal i.e. the behavior is not stable and varying for interacting the system or hitting the system with multiple registration information etc. Then evaluate such attacks by using association rule from the existing knowledge. If the system satisfies then add such attack to the database for future use and mark it. If not satisfied then send such attack calls to the Manager, it will then handle it appropriately.

IV. CONCLUSION

Mapping or tracing Intruder attacks is an important phase in IDS [Intruder Detection System]. In Cloud Based Intrusion Detection System [CBIDS], we have created a system for tracing attacks on the online storage at SaaS and PaaS Layer of cloud computing. The connection/session creation, collection of registration information, Listening / sensing for authentication comes under the SaaS. The rest of the part of CBIDS comes in the PaaS and IaaS layers of cloud computing. The proposed system is well designed and defined to trace the intruder attacks, mapping the its type, if a unknown attack encounter, it will be handled properly and marked it for the future. Whenever an unknown attack encountered, which is not in the log and already defined handler is not in the record, appropriate action will be taken by the Manager. Hence, CBIDS is a good model of handling intruder attacks.

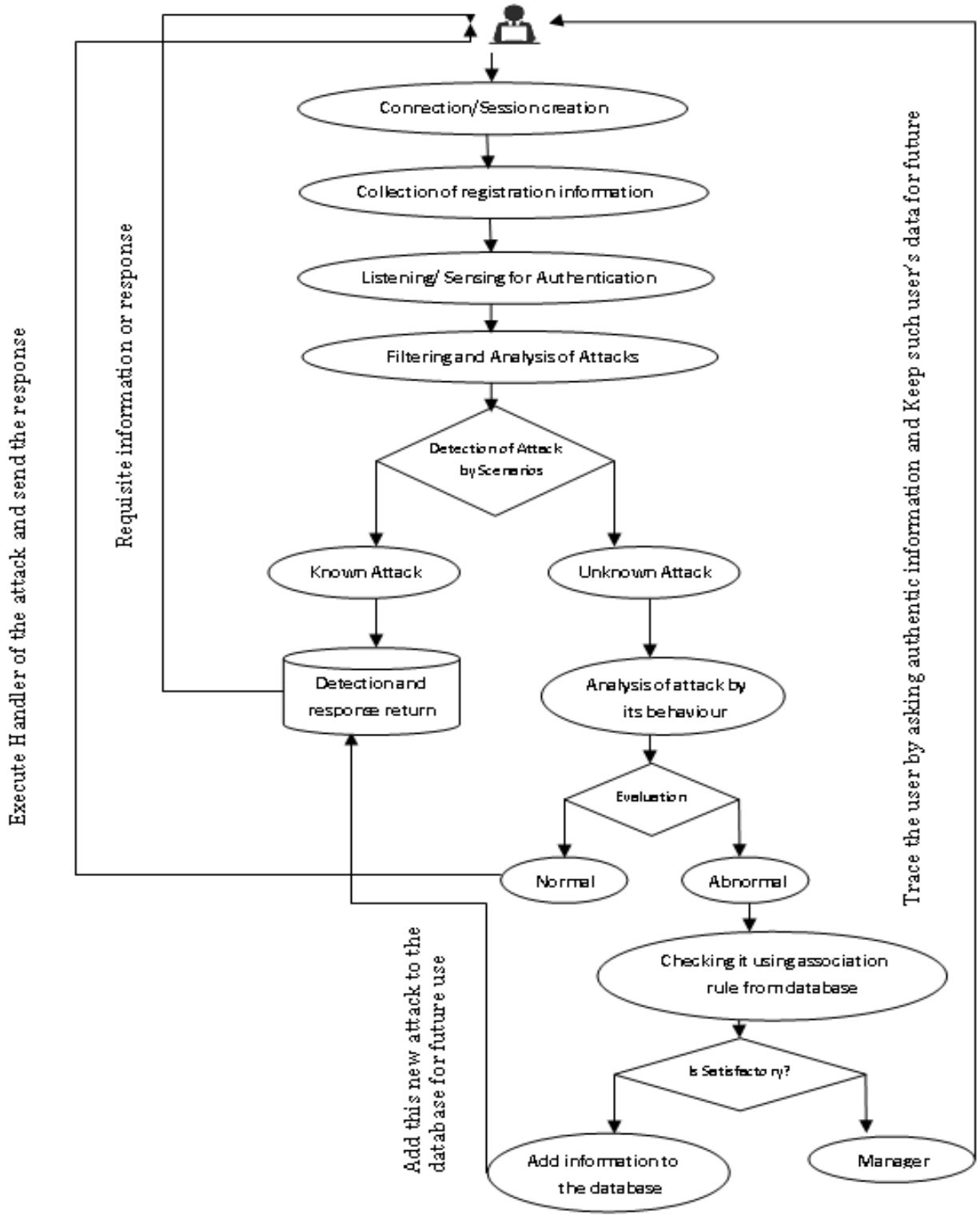

Figure 1 : Model for Cloud Based Intruder Detection System [CBIDS]

REFERENCES

[1] S 1. S. Akter, S.F.Wamba, A. Gunasekaran , R. Dubey, S. J.Childe, "How to improve firm performance using big data analytics capability and business strategy alignment?", Elsevier, Int. J. Production Economics 182 (2016), pp.113–131

[2] 2. C. Saadi, H. Chaoui, "Cloud Computing Security Using IDS-AM-Clust, Honeyd, Honeywall and Honeycomb", International Conference on Computational Modeling and Security (CMS 2016), pp.433-442

[3] 3. Costa DG, Guedes LA (2011) "Exploiting the sensing relevancies of source nodes for optimizations invisual sensor networks." Multimed Tools Appl 55, 2003.

[4] 4. Grance, T., Mell, P.: The nist definition of cloud computing. National Institute of Standards & Technology (NIST) (2009), http://www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf.

[5] 5. Roschke, S., Cheng, F., Meinel, C.: Intrusion detection in the cloud. In: IEEE International Symposium on Dependable, Autonomic and Secure Computing, pp.729-734, 2009.

[6] 6. Ramya. R Securing the system using honeypot in cloud computing environment International Journal of Multidisciplinary Research and Development Volume: 2, Issue: 4, 172-176April 2015.

[7] 7. Y. Sun, Y. Luo, and all, Fast live cloning of virtual machine based on xen. In High Performance Computing and Communications HPCC '09, 11th IEEE International Conference on pages 392-399, June 2009.

[8] 8. U. Sivarajah, M. M. Kamal, Z. Irani, V. Weerakkody, "Critical analysis of Big Data challenges and analytical methods", Journal of Business Research (2016), pp. 1-24

[9] 9. Z. Tan, X. He, P. Nanda, J. Hu "Enhancing Big Data Security with Collaborative Intrusion Detection", Article in IEEE Cloud Computing (2014) • January 2015, pp. 34-40.

[10] 10. Neha, Mandeep Kaur, "Enhanced Security using Hybrid Encryption Algorithm", IJIRCCE, ISSN(Online): 2320-9801, Vol. 4, Issue 7, July 2016

[11] 11. A. Kaur, S. Singh, "An Efficient data storage security algorithm using RSA Algorithm", IJAIEM, Volume 2, Issue 3, March 2013, ISSN 2319 – 4847, pp. 536-540.

[12] 12. A. Bhardwaj, GVB Subrahmanyam, V. Avasthi, H. Sastry, "Security Algorithms for Cloud Computing", International Conference on Computational Modeling and Security (CMS 2016), Elsevier, Procedia Computer Science 85 (2016), pp. 535 – 542

[13] 13. J. Khan, H. Abbasa, J. Al-Muhtadia, "Survey on Mobile User's Data Privacy Threats and Defense Mechanisms", International Workshop on Cyber Security and Digital Investigation (CSDI 2015), Elsevier, Procedia Computer Science 56 (2015), pp. 376 – 383

[14] 14. Al Haddad Zayed, H. Mostafa, M. Abdelaziz, B.Youness, "Hybrid Intrusion Detection Systems (HIDS) in Cloud Computing: Challenges and Opportunities", IJEECSE, Volume 3, Issue 3 (June, 2016) | E-ISSN : 2348-2273, pp. 7-13

[15] 15. Shuying Li, Ya Pan, "Study on secure data storage based on cloud computing", Bio Technology - An Indian Journal, BTAIJ, vol. 10, Issue 22, 2014 , ISSN : 0974 – 7435, pp. 13778-13783

[16] 16. U. Oktay, O. K. Sahingoz, "Proxy Network Intrusion Detection System for Cloud Computing", ISBN: 978-1-4673-5613-8, 2013, IEEE, pp. 98-104.

[17] 17. Oktay and O.K. Sahingoz, "Attack Types and Intrusion Detection Systems in Cloud Computing", 6th international information security & cryptology conference, Sep 2013, pp 71-76

[18] 18. C. Ambikavathi and S. K. Srivatsa, "Integrated Intrusion Detection Approach for Cloud Computing", Indian Journal of Science and Technology, Vol 9(22), DOI: 10.17485/ijst/2016/v9i22/95170, June 2016, ISSN (Online) : 0974-5645.

[19] 19. Akash G Mohod, Satish J Alaspurkar, "Analysis of IDS for Cloud Computing", International Journal of Application or Innovation in Engineering & Management (IJAIEM), Volume 2, Issue 3, March 2013 ISSN 2319 – 4847.

[20] 20. S.N. Dhage, B.B. Meshram, "Intrusion detection system in cloud computing environment", Int. J. Cloud Computing, Vol. 1, Nos. 2/3, 2012, pp. 261-282.

[21] 21. T. Kuldeep, Tyagi S.S and Agrawal R., Overview - Snort Intrusion Detection System in Cloud Environment, International Journal of Information and Computation Technology, ISSN 0974-2239 Volume 4, Number 3 (2014), pp. 329-334

Authors Profile

Dr. Amit Chaturvedi obtained the Ph.D. degree in Mar, 2012. He is presently teaching in the Govt. Engineering College, Ajmer. He has 17 years long PG teaching experience. Five doctorate degrees are awarded under his supervision. He has published around 72 research papers in national/international Journals and conference. He has written three text books in the computer science subjects. Presently he is working on the subjects of cloud computing and multicast communication in adhoc networks.

Mr Fayaz Ahmad Lone is a Ph.D. Scholar at Mewar Unviersity in the computer sciece Deptt. He has obtained Masters in Computer Application degree in 2010 from Univesity of Kashmir and M.Phil from Dr. C.V Raman University in 2013. Presently, he is pursuing his Ph.D. under the supervision of Dr. Amit Chaturvedi. He has published two research papers in international Journals.

.

