Exploratory Security Analysis of Intrusion Detection System Strategies

Dr.R.Sundar Raj [1] Mr.P.Ilayaragu [2] Mr.S.Sivaraja [3]

[1,2,3]Assistant Professors, Department of Computer Science,
Kongu Arts and Science College (Autonomous), Erode-638 107, Tamilnadu, India

ABSTRACT

Cloud computing in these days creating a great impact in various fields with impeccable pros of it. It has gained the hope of many small and medium level business people to step in to the new dimension of technology to some extent, but not in a satisfactory level. This happens due to some kind of mysterious fear, thinking that what if their data that are at sensitive level gets attacked or misused. The world is very competitive and the peer business organizations or attackers who are against the societal benefits may intrude in to the well-managed deck of cloud data. These kind of threats should be identified and should be protected with a massive shield in such a way that no enterprises or individuals may lose the data they keep as precious legacy. Many ideas regarding the detection of intruders have been proposed by many other works by various researchers, but still the problem arises. In order to identify them with clear root causes, this work thinks of the exploratory analysis presently followed intrusion detection systems in cloud.

Keywords: IDS, Physical Machines, Virtual Machines, Virtualization.

1. INTRODUCTION

Cloud Computing, which is a newly emerging technology which is a set of IT services that are provided to a customer over a network on a leased basis and with the ability to scale up or down their service requirement. It is a promising computing paradigm which recently has drawn the extensive attention from both academia, industry and other kind of business. Usually cloud computing services are delivered by a third party provider who owns the infrastructure. Its advantage to mention are vast but a few include scalability, resilience, flexibility, efficiency and outsourcing non-core activities [1,2,3]. Cloud Computing offers an innovative business model for organizations to adopt IT services without upfront investment.

In recent years, Cloud Computing is an area that is visited and adapted by almost all the categories of the concerns. They may range like academic, industry, communication, health, research etc., The usage is becoming wider, but the depth of its root path is limited. This is due to the hesitation that lies in some of the willing minds regarding the security inurement approach in the cloud technology. This technology acts as a pool area of computing resources that are to be virtualized.

2. CLOUD SECURITY

Security is a two-sided coin in the world of Cloud computing with its own pros and cons. It has some contentious issues in it, especially in the area of data confidentiality and protection[4,5,6]. If safety of data in cloud becomes questionable, its worst-case scenario will teach us the lessons of security and the ransom cannot be claimed in any means. Thus, security plays a very vital role.

The main situation in which the cloud network becomes insecure is when the intrusion happens. To thwart the adversaries and to mitigate the vulnerabilities, introducing an efficient Intrusion Detection System is an essential factor. This paper introduces an innovative approach of seeking the support of string matching algorithms for the detection of intrusions in an another alternative, but an efficient route to meet out the needs of dealing the intrusions in a better way [7,8,9]. The current part of Intrusion Detection System (IDS) in cloud computing may be replaced with this idea, to take out better results. Instead of just proposing an alternative approach, a weaker point of the existing method is identified and corrected and has also been proven well.

2.1 Role of Virtualization

Cloud Computing has been used in most of the diversified fields, and merging Virtualization with cloud provides a good support to achieve the aim of Cloud Computing to its fullest. Virtualization is the key enabler technology of a converged infrastructure and to deal with the essential requirements of cloud. The features such as, on demand sharing of resources, security by isolation, etc., are made possible through the concept of Virtualization [10,11,12].

Virtualizing a data center's IT resources can have certain consequences related to the physical infrastructure. If these impacts and consequences are ignored, the broad benefits of Virtualization and Cloud Computing can be limited or compromised, and in some cases it may experience severity. Virtualization brings many advantages on the manufacturing system reliability, by allowing full system backups and quick recovery in case of failures, as well as providing built-in redundancy. Virtualization software enables to break the single application server into fractional replicas called VMs.

2.2 Virtual Machines

Virtual Machines (VMs) are used to run multiple core machines independently with the property of isolation among the applications [13]. These machines create an illusion among the users that they are using the systems with a whole sole access. They are also essentially needed for applying this concept of Virtualization.

2.3 Migration of Virtual Machine

Migration of VMs is a process that is carried out within two or more servers deployed either over a Local Area Network (LAN) or Wide Area Network (WAN) in which a VM is moved from one machine to another. With day to day advancements and arising need for the huge data storage in the processing and networking of applications, VMs and their migrations are becoming major needs of any business of present state [14,15,16]. Hence, VM Migration becomes an essential factor when there is a need to share the resources among other users.

2.5 Approaches Of Virtualization

Generally, in an environment that supports traditional methods, the concept of physical switch is used along, by connecting with the physical servers. The organizations that use it can receive details about the traffic that goes between the servers and the connected switch. In VMs, the virtual switch has links from the physical switch through the physical NIC [17,18]. The eye is kept away from this and may cause some lag related to the safeguard measures and efficiency in performance. Thus it is essential to keep track on the major approaches related to the Virtualization. The popular approaches are shown as follows: (i) Hypervisor Based Virtualization; (ii) Application Based Virtualization; (iii) Operating System Based Virtualization.

3. SETBACKS AT INTRUSION LEVEL

The intrusion is common in all the fields, but more in cloud area. These intrusions are detected well in the present level to some extent and is running on an average throughput production as a corrective measure. The main area that is left out in this is the outcome of the conversion of intrusion data packets [19,20]. They are traditionally captured and used, but all the approaches are having its own cons. The automated nature of IDS is in the semi-automated state. Thus, deepening the roots of intrusion conversion and matching it for the Intrusion Prevention System are the needs of the hour.

3.1 Signalling Outputs

The intrusion detection is a serious need and usually this supplies signalling outputs. They are generally four in number, which are as follows:

- First is True Positive in which the intrusion is found to a malicious and is identified in correct way,
- Second one is True Negative in which, the intrusion is found to be a valid event and is rejected.
- Third is False Positive in which the intrusion is found to be a malicious one, but identified in an incorrect way.
- In fourth case of False negative, the intrusion is not at all found but by considering the malicious intrusion as a normal entry.

True signalling refers to the correct identification of item and the False signalling refers to the missing or left out rejection of item incorrectly. Positive signalling refers to the correct action is taken and the Negative signalling refers to the incorrect action imposed upon them. For a good Intrusion Detection System, the first two categories of signalling (False Positive and Negative) should be in lower rate and the next two categories of signalling (True Positive and Negative) should be in higher rate. From the proposed work of it is evident that the occurrence of False Negative is greater, and that too especially towards the attacks that are more in the sense of their age, than the occurrence of False Positives, that focusses on managerial aspects than that of to the security issues.

3.2 Gathering Intrusion Data

The data is a very important aspect in any kind of analysis. In the existent form of collecting data, data about the intrusions are gathered in the two ways [21,22], say

(i) Centralized, in which the information flows from a merged pool of data source

(ii) Distributed, in which the information flows from the data sources scattered in different physical locations.

These data would definitely fall in any one of the category types, according to their functionalities. The data type may be in the form of audit log, to which, all the transactions of a particular record are verified thoroughly for the security reasoning; Traffic mode, in which all the details regarding the methodology found towards the mode of travel of data is stored; Network log, to which the details regarding the data packets transferred, route chosen for the transfer, the nature of connections that are established are kept stored; Application audit, by which all the running and ready applications are verified and the relevant information is stored. The time is yet another very important aspect that are considered in Intrusions. If the recovery step of detect or to block an anomaly within the specific time, then that may cause serious adversaries.

3.3 Time Factors

As a time view point, the attacks caused may also be referred as Time granularity, which may have three forms in chief, they are batch-wise, in which the time constraints are shifted into batches; periodic, in which the time granularity is intermittent; continuous, which is mechanically opposite to the periodic sector. The time of detection of intrusion may be bi-categorized as real time, the appropriate time in which the anomaly has to be detected. The intrusion has to be dealt and is otherwise termed as on-line time; non-real time, the most in-appropriate and useless time in which the anomaly may not be detected and the intrusion may not be dealt and is otherwise termed as off-line time. The response of the intrusion detection system, may be active, through which the system is taking counter measuring acts and by not giving just the recovery seeking alarms; or passive, through which the system by not taking counter measuring acts and by simply giving the recovery seeking alarms [23].

4. CLASSIFICATION OF BASED ON THE IDS STRATEGY

Based on the approaches of detecting the anomalies, they are categorized into five major categories. They are as follows:

4.1 Signature based Detection of intrusions

Signatures are nothing but the attack patterns that are known and configured priory, to the level of data or network communication. This is a very simple kind of detection approach that is followed in many of the Intrusion Detection Systems that is based on matching the newly occurring intrusion to the signatures of the expected set of intrusions, that is already provided by the cloud providers to the customers in advance. When the new intrusion has found a match with the existing pool of intrusion signatures, then automatically the alert signal with less False Positives is emerged and the intrusion is blocked to enter into the system and is protected not to make any kind of changes to the system. This kind of intrusion detection method is alternatively termed as Rule based Intrusion Detection Systems

4.2 Anomaly based Detection of intrusions

In Anomaly based intrusion detection, the network traffic is constantly monitored and if any unfamiliar change occurs in the network, immediately that is reported to the agent of the network where a human interaction is necessary. The features of the system are completely recorded and kept as a reference. The rule sets are stored in to it according to the properties of the system, from the agent or the administrator of the network.

This works like an Expert system, which is very similar to the operations of Artificial Intelligence. This keeps track of all the layers of the network.

4.3 Heuristic based Detection of intrusions

Heuristic based detection of anomalies are nothing but analysing the attack behaviour that is known and configured priory, to the level of data or network communication. The new and unfamiliar behaviour, if found then immediately reported to the cloud system, advancing and overcoming the limitations of signature based detection systems. For doing this, a baseline of normal traffic and a recent abnormal or unusual behaviour should be frequently compared. The logs of behaviours should be seriously taken in to consideration.

4.4 Statistical based Detection of intrusions

Statistical based detection takes a set of action events and network area as a non-malicious sector, also considering all the remaining events or network as malicious. In this method, the statistical based algorithmic approach is followed that does complex computations making the agent to reside in the network and to monitor the malicious nature in a consistent manner. The expected normal value of the anomaly is calculated priory. Comparing the expected result, if the concentricity of the anomaly of a cloud network gets increased, then the subsequent alerts are informed with duly suggested actions. The expected normal value of the anomaly in this sense is termed as an anomaly score.

4.5 Hybrid based Detection of intrusions

The Hybrid based methodology is not an individual type as like the previous ones. It is a proportionate mix-up of the remaining approaches, seeking the combined dealings of functionalities. These kind of Hybrid methodologies remains successful only when the proper needs are compensated with each other. This is a useful approach, which when formulated on proper ratio, by identifying the cons of one method matching the pros of another method.

5. SETBACKS FOUND ON THE IDS STRATEGY

Based on the classification of approaches of detecting the anomalies, their setback areas are spotted. They are presented in Table 5.1:

5.1 Setbacks observed in Signature based detection

- The generation of signature set is an area that needs an eye of stare, which is very tough to be done.
- The new signature set are not constantly updated both in the providers' end and receivers' end of the cloud service. This happens due to the lack of interest or awareness of the cloud service receiver or due to the demand of extra costs posed by the providers for these kind of updates that are to be concentrated frequently. Mechanism for the efficient signature updation is lacking.
- The network traffic of the one-to-one (Sender-Receiver) system is considered. The reference of threats should be in a global view. That is found missing with the present form of Signature based intrusion detection.

5.2 Setbacks observed in Anomaly based detection

- Not all the changes in the network are malicious, but this approach records all the changes as attacking ones and would generate more number of False positives, which is difficult to manage
- Defining and generating rule sets are really difficult
- Detailed network nature identification is demanded

5.3 Setbacks observed in Heuristic based detection

- Dealing with behavioral approaches, that are really a tedious kind of job that are to be handled in routine of dynamically changing environment.
- False positives are reported in a higher rate and is very difficult to deal with them.

Table 5.1 Difficulties Observed In The Existing IDS Approaches

APPROACH	SETBACKS
Signature Based Intrusion Detection	The new signature sets are not constantly updated both in the providers' end and receivers' end of the cloud service. This happens due to the lack of interest or awareness of the cloud service receiver or due to the demand of extra costs posed by the providers for these kind of updates that are to be concentrated frequently. Mechanism for the efficient signature updation is lacking.
	The network traffic of the one-to-one (Sender-Receiver) system is considered. The reference of threats is not in a global view.
	Efficient mechanism for monitoring the signatures is found to be scarce.
Anomaly Based Intrusion Detection	Not all the changes in the network are malicious, but this approach records all the changes as attacking ones and generates more number of False positives, which is difficult to manage.
	Defining and generating rule sets are really difficult.
	Detailed network nature identification is demanded.
Heuristic Based Intrusion Detection	Dealing with behavioral approaches, are really a tedious kind of job that are to be handled in routine of dynamically changing environment.
	False positives are reported in a higher rate and is very difficult to deal with.
Statistical Based Intrusion Detection	The generation of search set is an area that is very complex in real time scenarios that has to be done in a regular basis.
	The compatibility of protocols is another problem since in a cloud network, many protocols involved in to it.
	The implementation of these kind of systems need an extreme care and consideration in algorithmic computations.
Hybrid Based Intrusion Detection	The mixture of methodologies should be compatible to each other, which is not always possible.
	The methodologies, if not in a proper proportion may cause serious and adverse effects.
	The need arises to have a detailed understanding of all kinds of system methods, so that the idea can be cultured properly, which is very tedious.

5.4 Setbacks observed in Statistical based detection

- The generation of signature set is an area that is very complex in real time scenarios that has to be done in a regular basis.
- The compatibility of protocols is another problem in this, since in a cloud network many protocols involved in to it.
- The implementation of these kind of systems need an extreme care and consideration in algorithmic computations.

5.5 Setbacks observed in Hybrid based detection

- They do not have an individuality and robustness.
- The mixture of methodologies should be compatible to each other, which is not always possible.
- The methodologies, if not in a proper proportion may cause serious and adverse effects.
- The need arises to have a detailed understanding of all kinds of system methods, so that the idea can be cultured properly, which is very tedious.

Parameter setting for the analysis is listed in the Table 5.2 as follows:

Table 5.2 Parameter Setting – SBIDS

Parameter	Value Range
No. of Test Servers	250 - 1000
No. of random key pairs	2n
Threshold Metric value	0 to 1
Attack Classes	8 to Cl(UA)
Vector Normality	0
Vector Abnormality	1
No. of String Pattern Match (Average)	98.5
Failure Function range	0 to maxLen(Str)
ST Update rate	0.99

6. CONCLUSION

The main objective of this analysis is to overcome the cons of the existing intrusion detection methods to carry out resource management in a better way of security and by adapting new policies of security. Various kind of threats are identified and has paved way in protecting with a shield in such a way that no enterprises or individuals would lose the data they keep as precious legacy. The root causes are clearly identified through this analysis work that has thought of the exploratory analysis of presently followed intrusion detection systems in cloud.

REFERENCES

1. Anup H. Gade. (2013). A Survey paper on Cloud Computing and its effective utilization with virtualization. *International Journal of Scientific and Engineering Research*, 4(12), 357-363.
2. Asaju La'aro Bolaji, Ahamad Tajudin Khader, Mohammed Azmi Al-Betar Mohammed A. Awadallah. (2013). Artificial Bee Colony Algorithm, its Variants and Applications: A Survey. *Journal of Theoretical and Applied Information Technology,* 47(2), 434 - 459.
3. Ashish Prosad Gope and Rabi Narayan Behera. (2014). A Novel Pattern Matching Algorithm in Genome Sequence Analysis. *International Journal of Computer Science and Information Technologies,* 5(4), 5450-5457.
4. Brototi Mondal, Kousik Dasgupta, Paramartha Dutta, Kalyani and Visva. (2012). Load balancing in Cloud Computing using Stochastic Hill Climbing-A Soft computing approach. *Elsevier, Science Direct- Procedia Technology, Bharati University,* 4(1), 783-789.
5. B Rahul. Diwate and Satish J. Alaspurkar. (2013). Study of Different Algorithms for Pattern Matching. *International Journal of Advanced Research in Computer Science and Software Engineering,* 3(3).

6. Chirag Modi, Dhiren Patel, Bhavesh Borisaniya, Hiren Patel, Avi Patel and Muttukrishnan Rajarajan. (2013). A survey of intrusion detection techniques in cloud, *Elsevier, Journal of Network and Computer Applications,* 36(1), 42-57.
7. Dervis Karaboga and Bahriye Akay. (2009). A comparative study of Artificial Bee Colony algorithm. *Elsevier, Journal of Applied Mathematics and Computation,* 214(1), 108-132.
8. Dhinesh Babu L. D and P. Venkata Krishna. (2013). Honey bee behavior inspired load balancing of tasks in cloud computing environments. *Elsevier, Applied Soft Computing,* 13(1), 2292-2303.
9. Fouad Bahrpeyma, Ali Zakerolhoseini, Hassan Haghighi and Shahid Beheshti. (2014). Using IDS fitted Q to develop a real-time adaptive controller for dynamic resource provisioning in Cloud's virtualized environment. *Elsevier, Applied Soft Computing,* 26(1), 285-298.
10. Junaid Arshad, Paul Townend and Jie Xu. (2013). A novel intrusion severity analysis approach for clouds. *Elsevier, Future Generation Computer Systems,* 29(1), 416-428.
11. Raj, R Sundar; Bhaskaran, Dr. V Murali. (2014). Technical Guidance to Overcome the Issues on Cloud Computing. *Journal of NanoScience and NanoTechnology,* 2(6), 725-727.
12. Raj, R Sundar; Bhaskaran, Dr. V Murali. (2015). A Roadmap to Virtualization Approach in Cloud Computing. *International Journal of Advanced Research in Data mining and Cloud Computing,* 3(1), 33-37.
13. Raj, R Sundar; Bhaskaran, Dr. V Murali. (2015). An Empirical study on revolutionizing approach in Cloud Computing paradigm. *International Journal of Contemporary Research in Computer Science and Technology,* 1(6), 187-198.
14. Raj, R Sundar; Bhaskaran, Dr. V Murali. (2016). Improved Cloud Security Mechanism with a Self-Monitored Intrusion Prevention System. *International Journal of Advance Research in Science and Engineering,* 5(12), 20-32.
15. Raj, R Sundar; Bhaskaran, Dr. V Murali. (2017). Comparative Analysis of Cloud Tools to Implement Automated Resource and Security Management. *Indian Journal of Engineering (An International Journal),* 14(35), 20-32.
16. Raj, R Sundar; Bhaskaran, Dr. V Murali. (2017). Securing cloud environment using a string based intrusion detection system. *Advanced Computing and Communication Systems (ICACCS), 20174th International Conference on*, 1-13.
17. Raj, R Sundar; Bhaskaran, Dr. V Murali. (2018). Security Intelligence in Cloud with Intrusion Detection and Prevention Enhancements. *International Journal of Advance Research in Science and Engineering,* 7(2), 454-467.
18. Raj, Dr.R Sundar. (2018). Suitability of Virtualization and ABC Algorithm in the SEAFORM Approach. *International Journal of Management, Technology And Engineering,* 8(XII), 1843-1854.
19. Rodrigo N. Calheiros, Rajiv Ranjan, Anton Beloglazov, C´esar A. F. De Rose and Rajkumar Buyya. (2010). CloudSim: a toolkit for modeling and simulation of cloud computing environments and evaluation of resource provisioning algorithms. *CLOUDS Laboratory,* 41(1),.23–50.
20. Suraj Pandey, LinlinWu, Siddeswara Mayura Guru and Rajkumar Buyya. (2008). A Particle Swarm Optimization-based Heuristic for Scheduling Workflow Applications in Cloud Computing Environments. *The University of Melbourne, Australia*.

21. Weiwei Kong, Yang Lei and Jing Ma. (2016). Virtual machine resource scheduling algorithm for cloud computing based on auction mechanism. *Elsevier, Journal of Optik,* 127(1), 5099–5104.
22. UCI Repository – https://archive.ics.uci.edu/ml/support/Cloud
23. European Union Open Data Portal
    - https://data.europa.eu/euodp/en/data/dataset/yUBHDpCh8MDqL9Gub8Qmq

AUTHORS' BIOGRAPHY

Dr.R.Sundar Raj, Assistant Professor in Computer Science of Kongu Arts and Science College (Autonomous), Erode, Tamilnadu, India has received his B.Sc. in Computer Science and M.C.A degree from Bharathiar University and has secured University I Rank in both the degrees. He has also published research papers in International journals. He has secured Highly Commended in his Ph.D. programme from Bharathiar University with his area of research as Cloud Computing. He has six years of teaching experience and has received Best Teacher awards twice.

Mr.P.Ilayaragu, Assistant Professor in Computer Science of Kongu Arts and Science College (Autonomous), Erode, Tamilnadu, India has received his B.Sc. and M.Sc. degrees in Computer Science from Bharathiar University. He has received M.Phil. from Periyar University. He has also published research papers in International journals with his area of research as Web Mining. He has fifteen years of teaching experience.

Mr.S.Sivaraja, Assistant Professor in Computer Science of Kongu Arts and Science College (Autonomous), Erode, Tamilnadu, India has received his B.Sc. in Computer Science from Bharathiar University and M.Sc. in Computer Science from Periyar University. He has received M.Phil. from Bharathidasan University. He has also published research papers in International journals with his area of research as Data Mining. He has sixteen years of teaching experience.