Journal of Engineering and Applied Sciences 12 (22): 5939-5943, 2017
ISSN: 1816-949X

A Review: Analysis and Comparison of Different Detection Techniques of IDPS

Navjot Kamboj, Simar Saggu, Aditya Lamba and Meeta Singh
Faculty of Engineering and Technology, Manav Rachna International University,
Faridabad, Haryana, India

Abstract: In today's world, many enterprises are moving towards the cloud computing systems as it will provide an attractive and cheap service for users to store their data and run applications along with the accessibility and reliability options. This study discusses cloud services, trends, security and threats present at each service model along with the challenges faced in addition to intrusion detection and prevention system used for securing the cloud infrastructure. This study also compares different techniques of detecting the security threats in Intrusion Detection and Prevention System (IDPS) and provides the solutions to deal with the detected threats.

Key words: Cloud, security, intrusion detection, prevention, threats, solution

INTRODUCTION

Throughout the history of computer science mainframe computers were predicted to be the future of computing. A number of attempts have been made since 1960's which was an era of time sharing utilities, network computer and later grid computing to disengage the users from increased hardware needs (Zissis and Lekkas, 2012). This abstraction is slowly becoming a reality as it is moving to smaller and affordable PCs and servers which together construct the so called cloud computing system also called cloud.

Cloud computing reduces the hardware needs and overall complexity as everything is done on the server side. It is a technology in which data storage, computation and management takes place on multiple servers which can be accessed through internet at any time any anyplace. A berkeley view of cloud computing defined cloud to be services executed in data centres by using hardware and software (Armbrust *et al.*, 2009). Whereas according to National Institute of Standards and Technology (NIST., 2007) definition, cloud model is composed of five essential characteristics; on demand self service, measured service, broad network access, rapid elasticity and resource pooling, three service models; Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and four deployment models; Public cloud, community cloud, private cloud and hybrid cloud (Mell and Grance, 2009).

Literature review: The cloud computing is seen as an important change of information industry and will make more impact on the development of information technology for the society. The majority of cloud computing infrastructure consists of reliable services delivered through data centre. These services are built on servers with different levels of virtualization technologies which are accessible anywhere in the world. The data can be stored in the cloud system and the user can use the data in any time and in anywhere and pay per use policy. Many companies provide the cloud computing platform such as Google, IBM, Microsoft, Amazon, VMware and EMC (Liu, 2012).

As cloud computing made data access easier and quicker but on the other hand storing of data on multiple servers focuses on one important question that is its security. For many business-critical computations, today's cloud computing appears inadvisable due to issues such as service availability, data confidentiality and others (Chen *et al.*, 2010). In cloud systems different parts of an application can be stored at different locations that can have an adverse impact on the performance of the application. Therefore, it is quite natural that monitoring and maintenance is not as simple a task. In addition to this the cloud customers always have a fear of losing data by having them locked into proprietary formats. They may lose control over their data, since the tools for monitoring are not always provided to the customers. Hence, data loss is a potentially real risk in some specific deployments. The biggest challenges of cloud security are separation of data part and access control. Based on cloud infrastructure, tenants should be separated from each other and different users from one tenant should be separated from each other with the

Corresponding Author: Navjot Kamboj, Faculty of Engineering and Technology, Manav Rachna International University, Faridabad, Haryana, India

limitations of security policies (Ma *et al*., 2016). As data is stored at different location there is no control of customer over the infrastructure in which data is stored. Intrusion detection and prevention system here plays a significant role by protecting the infrastructure in which data is stored. Using IDPS, attacks can be identified and notified to the administrator immediately or can be prevented from causing more harm to the system.

In the fight of securing data stored in various servers spread across the globe, various models and systems have been proposed. Ateniese *et al*. (2007) initially proposed a Provable Data Possession (PDP) Model which gave permission to client whose date is stored with untrusted servers to view and verify the original data stored on servers. Juels and Kaliski (2007) proposed a technique called "Proof of Retrievability" (PoR) which included spot-checking and error-correcting algorithms for ensuring ownership and retrievability of data stored on servers. Subashini and Kavitha (2011) studied security issues in cloud delivery models and analyzed causes of every security issue. Intrusion Detection and Prevention System (IDPS) is a very efficient method for securing cloud and can act as an indispensable tool. IDPS has a goal of detecting destructive activities and preventing serious damage to the system (Shabtai *et al*., 2010).

MATERIALS AND METHODS

Intrusion detection and prevention system: Earlier only intrusion detection system was used which just detected intrusions. Later intrusion prevention system was added to IDS that detected as well as prevented intrusions by altering attackers content or alters the security environment (Scarfone and Mell, 2007). IPS can sometimes detects non-intrusive activity as destructive activity due to high false alarm rates (Patel *et al*., 2010). IDS is software that enabled intrusion detection and prevention process. There are particularly two types of attack in a system-internal and external. Internal attacks occur when internal users try to gain unauthorized access. External attacks occur due to unauthorized access by external origins. A traditional IDPS monitored data, perform analysis, detect malicious activities and then generate alarms and preventive response was given. Traditional IDPS generated alarm for every attack irrespective of the severity of the threat. Some attacks called as incidents looked malicious but actually were not. These false alarms impacted the systems which sometimes caused unavailability of data. To overcome this problem, various advanced IDPS were developed.

IDPS is basically divided into two layers

Functional layer: This is the layer where all four basic functions of monitoring, detection, alert generation and reaction take place.

Structural layer: This layer is also known as infrastructural layer. The structure of an IDPS is based on two types: individual or collaborative. An individual arrangement of IDPS is achieved by physically integrating it within a firewall. A collaborative IDPS consists of multiple IDPSs over a large network where each one communicates with each other.

Intrusion detection and prevention system consists of two components detecting elements and correlation handlers. IDPS can be run on individual systems and on different systems that communicate with one another, this kind of IDPS structure is called as collaborative IDPS. These can be divided into 3 types:

Central: This collaborative IDPS contains a central server to which several nodes are connected via medium. Each node has its own IDPS which has only the role of detecting intrusions locally and sending reports to the central server. The central server acts as a correlation handler that examines all of these detected intrusions and takes an accurate detection decision. Breaking down of central unit disrupts entire process of correlation handling.

Hierarchical: The system is divided into many subgroups on basis of same kind of features like location, same platform. A hierarchy is formed; lowest level systems have IDPS that just detect intrusions while higher level system has IDPS with both detecting elements and handlers. Better than centralized approach but lags as higher level system cannot detect intrusions properly due to abstraction.

Fully distributed: All the nodes perform both the functions, detecting and correlation handling and communication with one another. The main advantage of this method is design is scalable as no central authority is there. But this method also has some disadvantages like lack of accuracy in detection decision due to unavailability of all alerts, lack of alert information which insufficient for detecting large scale intrusions (Zhou *et al*., 2010).

Detecting techniques: If intrusions are detected properly by IDPS, then prevention becomes easy. Following are different techniques for detection of intrusions:

Signature based: This method finds known malicious patterns in network traffic. Signatures for known attacks are developed and stored. Its response type towards attacks of intrusions is of passive and has a collaborative structure. Example, sending mail bugs through internet Worm attack (Spafford, 1990).

Table 1: Various works on IDPS detecting techniques

Researchers name	IDPS technique	Algorithm used	Applications	Objective	Results
Marc Norton (2004)	Signature Detection	Aho-Corasik	Implemented in SNORT for multi-pattern searching	To improve performance on large pattern grounds	Memory needed for matching is reduced pattern
Jabez and Muthu kumar (2015)	Anomaly based	Outlier detection approach	Many big datasets like KDD are used to train IDS initially at distributed storage environment	To enhance the detection precision for low frequent attacks and detection stability	Proposed IDS identifies all types of attacks such as probe, DoS, U2R, R2L
Tian *et al*. (2008)	Hybrid detection	Support vector Machine	It correlates processes and allows for handling training information (attack data) online, rather than in batch	Preventing, detecting and reacting to intrusions without disturbing the of existing systems	Lowers the false alarm rate and provide real-time the intrusion detection

Table 2: Summary on IDPS detecting techniques along with its advantages and disadvantages

Researchers name	Aim	IDPS category	Type or approach	Technique	Signature detection and prevention	Anomaly detection and prevention	Advantages	Disadvantages
Janakiraman *et al*. (2003)	To provide an IDPS that uses peer to peer approach for the network security in a distributed environment	HIDPS and NIDPS	Peer to peer	Signature based and anomaly based	Yes	Yes	Reliability	Difficult to implement, memory issues
Harley Kozushko	To define the difference between host based and network based IDPS	HIDPS and NIDPS	Sequence matching and malicious matching	Signature based	Yes	No	Automated response to malicious threats	Unable to detect and prevent anomaly behaviour
Guimaraes and Murray (2008)	To find if SNORT and source fire are the best IPSs	NIDPS	OS and application level	Signature based	Yes	No	Allows self configuration	Unable to detect and prevent anomaly behaviour
Shibli and Muftic (2008)	To provide a secure mobile agent IDPS for	HIDPS	Secure mobile mobile agent	Signature based and anomaly based	Yes	Yes	Less human effort, real time response	Need to find better techniques

Anomaly based: Anomaly detection is a technique of detecting threats which performs activities that are not normal according to defined system behaviour (Brown *et al*., 2002). Whenever such anomaly occurs an alarm is generated to the administrators that define the presence of an unidentified behavior in the system, this makes a acceptable possibility that the events are caused by either malicious or disturbing activities, this technique identifies intrusions by classifying activities as either abnormal or normal.

Hybrid based: It is a mixture of both signature and anomaly detection method in order to improve the capabilities of IDPS. The various works done in IDPS detecting techniques are summarized in Table 1 and 2.

RESULTS AND DISCUSSION

Intrusion prevention system: Intrusion prevention system is an approach of detecting and preventing known and unknown threats attacking the networking systems. The function of IPS is to detect malicious activity, log data regarding this activity, report it by generating alarms and try to block or stop it. IPS is installed at various locations in a network or in host systems. Earlier only firewalls were used to protect a network. Firewalls are software or hardware which examines the incoming packets and outgoing packet. It has set of rules defined in the software or hardware. IPS can also be divided into following types:

Host based: The IPS is installed on the host computers and protects the host system and application from attacks. These IPS help in protecting servers and workstations. HIPS can prevent both encrypted and unencrypted attacks as they analyse the packet once the packet is decrypted by host computer. They are called as last line of defence. They use system's memory and processor for intrusion prevention.

Network-based: IPs is installed on a network. This IPS monitors and examines inbound and outbound packets from the wires while it is travelling to a host and blocks malicious packets. They help in defending the critical infrastructure. They are also called as first line of defence as they are the first IPS that receives the packet and examines it. They use their own memory and processor.

Network Behavior Analysis (NBA): Analyzes traffic on a network and detects threats that produce unusual traffic flow, e.g., Distributed Denial of Service (DDoS) attacks or some malware.

Wireless Intrusion Prevention Systems (WIPS): Theseare deployed in a wireless network for monitoring the traffic by analyzing wireless network protocols. These mostly used for monitoring and analyzing the Wireless LANs.

Summary on IDPS detecting techniques along with its advantages and disadvantages is shown in Table 2.

CONCLUSION

In cloud computing, the data is stored and managed at different locations so, the users were not sure about safety of their data which was the biggest challenge. To overcome this challenge, intrusion detection and prevention system comes in picture. IDPS helps in securing the cloud infrastructure and therefore protecting users data from unauthorized access or tampering.

Different techniques of intrusion detection system are signature, anomaly and hybrid. Signature detection method looks for known attacks in the cloud whereas Anomaly detects unknown attacks and hybrid detection method has the capabilities of both signature and anomaly methods. Hybrid can detect both known and unknown attacks in cloud. For prevention of detected attacks content-based IPS is considered as it has an advantage of detecting signature and anomaly attacks and also preventing them.

ACKNOWLEDGEMENTS

Researchers would like to express the gratitude to Dr. Kiran Khatter, research mentor, accendere Knowledge Management Services (Accendere KMS) Pvt. Ltd. and other research mentors from accendere KMS Pvt. Ltd. for their comments on earlier versions of the manuscript. Although, any errors are our own and should not tarnish the reputations of these esteemed persons.

REFERENCES

Armbrust, M., A.D. Joseph, R.H. Katz and D.A. Patterson, 2009. Above the clouds: A Berkeley view of cloud computing. MCs Thesis, EECS Department, University of California, Berkeley, California.

Ateniese, G., R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson and D. Song, 2007. Provable data possession at untrusted stores. Proceedings of the 14th ACM Conference on Computer and Communications Security, October 29, 2007, Alexandria, Virginia, USA., pp: 598-609.

Brown, D.J., B. Suckow and T. Wang, 2002. A survey of intrusion detection systems. Ph.D Thesis, Department of Computer Science, University of California, San Diego, California.

Chen, Y., V. Paxson and R.H. Katz, 2010. What's new about cloud computing security. Master Thesis, University of California, Berkeley Berkeley, California.

Guimaraes, M. and M. Murray, 2008. Overview of intrusion detection and intrusion prevention. Proceedings of the 5th Annual Conference on Information Security Curriculum Development, September 26-27, 2008, ACM, New York, USA., ISBN:978-1-60558-333-4, pp: 44-46.

Jabez, J. and B. Muthukumar, 2015. Intrusion Detection System (IDS): Anomaly detection using outlier detection approach. Procedia Comput. Sci., 48: 338-346.

Janakiraman, R., M. Waldvogel and Q. Zhang, 2003. Indra: A peer-to-peer approach to network intrusion detection and prevention. Proceedings of the 12th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, June 11-11, 2003, IEEE, Washington, USA., ISBN:0-7695-1963-6, pp: 226-231.

Juels, A. and B.S. Kaliski Jr, 2007. PORs: Proofs of retrievability for large files. Proceedings of the 14th ACM Conference on Computer and Communications Security, October 29-November 02, 2007, ACM, New York, USA, ISBN: 978-1-59593-703-2, pp: 584-597.

Liu, W., 2012. Research on cloud computing security problem and strategy. Proceedings of the International Conference on 2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet), April 21-23, 2012, IEEE, Wuhan, China, ISBN:978-1-4577-1415-3, pp: 1216-1219.

Ma, W., Z. Han, X. Li and J. Liu, 2016. A multi-level authorization based tenant separation mechanism in cloud computing environment. China Commun., 13: 162-171.

Mell, P. and T. Grance, 2009. The NIST definition of cloud computing. National Inst. Standards Technol., 53: 20-50.

NIST., 2007. Guide to Intrusion Detection and Prevention Systems (IDPS). National Institute of Standards and Technology, Gaithersburg, Maryland, USA.

Norton, M., 2004. Optimizing Pattern Matching for Intrusion Detection. Sourcefire Publisher, Columbia, Maryland,.

Patel, A., Q. Qassim and C. Wills, 2010. A survey of intrusion detection and prevention systems. Inf. Manage. Comput. Secur., 18: 277-290.

Scarfone, K. and P. Mell, 2007. Guide to Intrusion Detection and Prevention Systems (IDPS). NIST. Spec. Publ., 800: 94-127.

Sen, J., 2013. Security and Privacy Issues in Cloud Computing. In: Architectures and Protocols for Secure Information Technology Infrastructures, Ruiz-Martinez, A. (Ed.). IGI Global, Dauphin, Pennsylvania, pp: 1-45.

Shabtai, A., Y. Fledel, U. Kanonov, Y. Elovici, S. Dolev and C. Glezer, 2010. Google Android: A comprehensive security assessment. IEEE Security Privacy, 8: 35-44.

Shibli, M.A. and S. Muftic, 2008. Intrusion detection and prevention system using secure mobile agents. Proceedings of the IEEE International Conference on Security and Cryptography, July 26-29, 2008, IEEE, Porto, Portugal, pp: 107-113.

Spafford, E., 1990. The Internet Worm Report. Purdue University, Florida, USA.,.

Subashini, S. and V. Kavitha, 2011. A survey on security issues in service delivery models of cloud computing. J. Network Comput. Appl., 34: 1-11.

Tian, Z., W. Zhang, J. Ye, X. Yu and H. Zhang, 2008. Reduction of false positives in intrusion detection via adaptive alert classifier. Proceedings of the International Conference on Information and Automation, June 20-23, 2008, IEEE, Beijing, China, ISBN:978-1-4244-2183-1, pp: 1599-1602.

Zhou, C.V., C. Leckie and S. Karunasekera, 2010. A survey of coordinated attacks and collaborative intrusion detection. Comp. Security, 29: 124-140.

Zissis, D. and D. Lekkas, 2012. Addressing cloud computing security issues. Future Gener. Comput. Syst., 28: 583-592.