Journal of Computer Engineering
ISSN 10003428

Original Research Article
Vol 9, Issue 5, 2020 | ISSN: 1000-3428

Threat Analysis and Counteractive Strategies for Cloud-Based Services Under Advanced Attacks

Aisha J. Khan, Rami A. Mansour, Noura M. Elgohary

School of Computer Science, University of Birmingham, UK; Department of Information Technology, King Fahd University of Petroleum and Minerals, Dhahran, Saudi Arabia; Faculty of Engineering, Cairo University, Egypt

***Abstract*—**Cloud computing provides infrastructure to the enterprise through the Internet allowing access to cloud services at anytime and anywhere. This pervasive aspect of the services, the distributed nature of data and the wide use of information make cloud computing vulnerable to intrusions that violate the security of the cloud. This requires the use of security mechanisms to detect malicious behavior in network communications and hosts such as intrusion detection systems (IDS). In this article, we focus on the detection of intrusion into the cloud sing IDSs. We base ourselves on client authentication in the computing cloud. This technique allows to detect the abnormal use of ubiquitous service and prevents the intrusion of cloud computing. This is an approach based on client authentication data. Our IDS provides intrusion detection inside and outside cloud computing network. It is a double protection approach: The security user node and the global security cloud computing.

I. Introduction

THE emergence and use of new technology solutions such as cloud computing is due to the rapid evolution of business processes, the need for data storage, sharing services and to disregard/substitution of machinery and work/ calculation tools.

The cloud allows storing information and focuses on data independently their support [1]. The Internet allows the cloud to provide services at any time and in anywhere, which allows to have ubiquitous services [2], [3]. The advantages of cloud computing; namely: The supply of infrastructure services, data and insurance services availability, rapid scalability and accessibility [4], [5]; exposing the network to malicious activities.

To stop malicious activities, it is necessary to implement IDS [6], [7]. IDSs detect and respond (react) to attacks occurring in the network by implementing new security policies [8]. To solve the problems in intrusion networks, IDSs have been widely applied [1]. This paper includes and focuses on the ubiquitous service aspect of cloud computing [9].

In this article, we present an IDS that aims to overcome the problems of network intrusions in cloud computing. The remainder of this paper is divided into five sections. Section II presents the paradigm of cloud computing and how it relates to related work on intrusion detection in cloud computing, is introduced. Section III details our proposal, while Section IV exposes advantages and privileges of the proposed solution. Section V describes a test of our approach in virtual environment and Section VI presents the conclusion and directions for further work.

II. Background and Related Work

A.Cloud Computing

In [10], [11], National Institute of Standards and Technology (NIST) has given the definition of Cloud Computing as: Cloud computing is a model for enabling ubiquitous, provides on-line computer services or applications, accessible to anywhere, anytime, and by any device (smartphone, desktop, laptop and tablet). Cloud computing allows sharing an infrastructure, an application solution or a platform to any user on-demand it via a simple self-service website (also called a portal) [12].

Among the services provided by cloud computing, we have infrastructure, storage, development platforms, and web applications through the cloud (Internet). Cloud computing is composed of the special characteristics that are the distributed and open structure of cloud computing and services become, shared resources, node mobility, services availability assurance, rapid accessibility, scalability, and availability of service and information, etc. [11], [13].

B.Intrusion Detection System (IDS)

The IDS are implemented in order to detect any attempted violation of the security mechanisms, this is permanent or regular monitoring systems.

Intrusion detection is the discovery or identification of the use of a computer system for purposes other than those intended [14]. They identify abuse of computer systems, by unauthorized users, detect attack on computing resources, and also deal with misuse of the Internet system [15], [16].

Intrusion detection is to scrutinize network traffic, collect all events, analyze them and generate alarms in case of identification of malicious attempts. Optionally, IDS can react against these malicious behaviors and take measures against [17].

How to cite: Aisha J. Khan, Rami A. Mansour, Noura M. Elgohary (2020). Threat Analysis and Counteractive Strategies for Cloud-Based Services Under Advanced Attacks. Journal of Computer Engineering, 9(5), 8–15. DOI: https://doi.org/10.5281/zenodo.19341656

With the goal of classifying IDS, two approaches have been proposed; the behavioral approach (anomaly detection) [18] and the scenario approach (misuse detection or knowledge based detection) [19], [20].

The first is based on a model describing the normal exploitation of the system (normal behavior) by classifying as intrusive any significant deviation from this model [21].

The second is based on patterns or a sequence of events representing attack signatures by classifying as intrusive (attacks) all comportment authentic to these patterns [21].

C.IDS in Cloud Computing

Many efforts have been taken in the area of cloud computing and IDS to overcome the current security threats in the cloud computing. Nikolai et al. [22] were interested in the users of the virtual machine resource, by implementing an IDS cloud environment which is responsible for monitoring users using data from virtual machines monitors. This allows to control operation outside of the virtual machines so the attacker cannot modify the system in the case of tenant's instance is violated.

A way to see the security of cloud computing is to be interested in privacy in the environment of cloud computing [23]. In this approach, the authors have presented most attacks and threats cons cloud computing with explanation of the latest solutions and their limitations. Another way to see the security of cloud computing is to ensure the integrity and accuracy of user's data in the cloud. For this, Wang et al. [24] have proposed a system against malicious attacks attempting to modify data, and collusion server attacks. It is an effective and resilient system.

To detect intrusion in cloud applications, Dastjerdi et al. [25] proposed a scalable, flexible and cost effective method using mobile agents. This method is used for protecting Virtual Machines (VMs) that are outside an organization. Evidences of an attack from all the attacked VMs are collected by a Mobile agent. Further analysis and auditing are applied on this evidence.

IDS architecture of cloud computing is presented in [26]. IDS provides services and storage services supported by each node of the Cloud environment. IDS service system is composed of two components: Analyzer and Alert System. Data from various resources is captured by the event auditor. The IDS service system receives data from the event auditor. This data is used for detecting intrusion by using a behaviorbased or knowledge-based technique. In this approach, artificial neural network (ANN) [27] is used for detecting unknown attacks. Alert system informs other nodes when any attack or intrusion is detected.

III. PROPOSITION

In this paper, we develop an IDS for detecting and correcting anomalies and intrusions occurring in cloud computing environments. We focused on ubiquitous aspect of services offered by cloud computing, because users are accessing these services in real time. We propose a rational implementation of IDS over cloud computing services.

A.Proposal Description

The architecture of our contribution is composed of (cf. Fig. 1):

(1) An IDS controller that is responsible for archiving all protective objects (analysis, detection and correction).
(2) Cloud server provider that handles user's services.
(3) A database which contains the list of legitimate users with their authentication.
(4) User who is a Customer (applicant) service.
(5) Mobile Agent allows the analysis and the detection of any intrusion on user node.

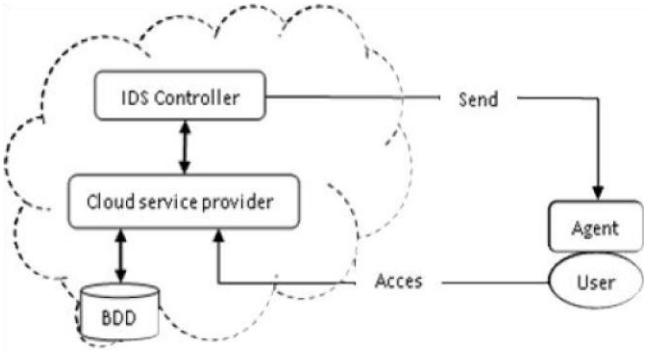

Fig. 1 Architecture of proposal

For every user access to cloud services provider, IDS controller sends a mobile agent to the user node. The mission of the mobile agent is to deploy an instance of IDS at the node level, which allows the analysis and the detection of any intrusion. This analysis and detection is based on the user behavior.

Fig. 2 shows the framework of IDS activity. However, the main task of IDS is defending a computer system by detecting an attack and possibly repealing it.

To procure services, the user (customer) made an authentication access to the provider level cloud service provider. To ensure the identity and legitimacy of the applicant (customer), verification is made based on authentication data. The profile user is created on the authentication database (inputs received from the user). Then the behavior of the node (user) is constructed from the data stream. The actual behavior with the normal profile is compared to detect anomalies in the behavior of nodes (users). When an abnormality is detected, an alarm is sent to the node provider of cloud services to help solve this problem.

B.Normal Profile

An authentication confirmation is performed at each access of a user to a cloud services provider. This authentication limit access to information and services offered by cloud computing. The normal user profile is created based on the legitimate user data and represents a typical behavior of a user. This profile consists of authorization (permission) and restriction; it is represented as a feature vector. Let Vi (0) be the feature vector of node i of size n. Such that: Vi(0) = (vi1, vi2, vi3, ..., vin)^T, and n is the number of characteristics of the node i.

C.Intrusion Detection

The detection phase identifies abnormal vectors. To solve the problem of the attacks at the cloud computing our contribution evolves according to two phases: security user nodes and global security cloud environment.

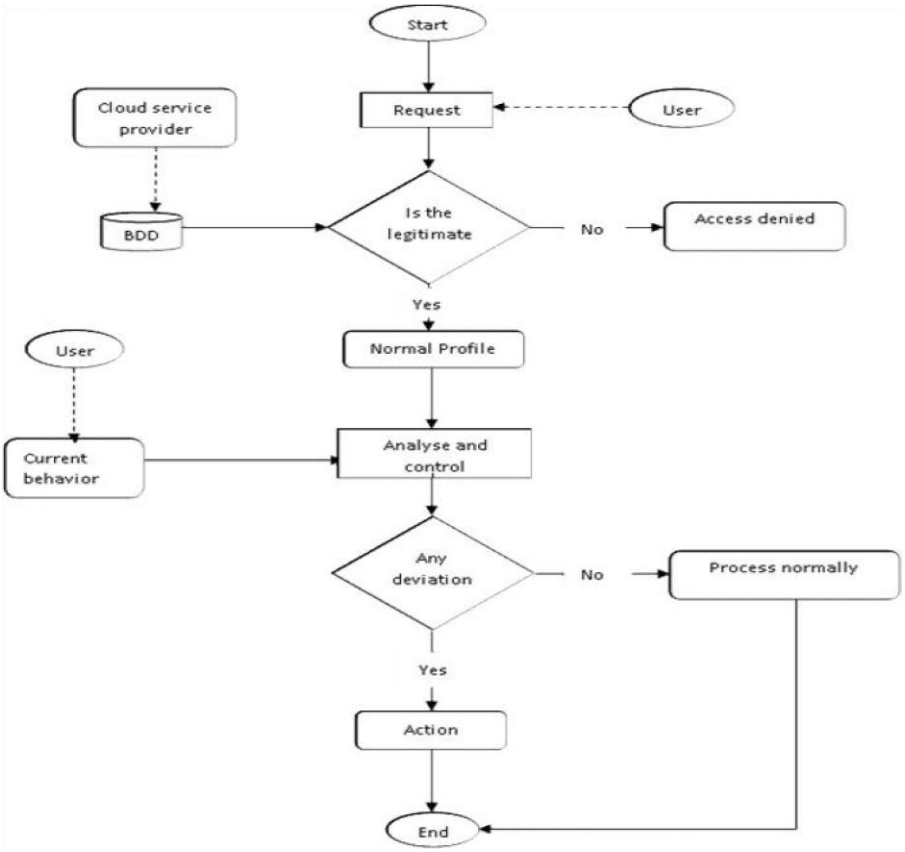

Fig. 2 IDS-activity framework

1) *Security User Nodes*: A data collection is performed at the node; these data are represented as feature vector v. This collection is done in a time interval t. The vector represents the behavior of a user node in this time period.

To determine abnormalities, we calculate the distance between $v_i(0)$ and v_i (t). We class $v_i(t)$ abnormal, if the projection distance calculated exceeds a predefined threshold:

$$\begin{cases} d\square vi(0),vi(t)\square\square o: \text{Normal} \\ \square\square\square\, d\square vi(0),vi(t)\square\square o: \text{Anomaly} \end{cases}$$

2) *Security Global Cloud Environment*: After detection at the user node, the mobile agent manages the result of the detection in case of an attack and passes the results to the controller IDS to contribute to a comprehensive and cooperative detection of intrusion.

D.Behavior in the Case of Attack

In the event of a possible intrusion (attack) is detected, the proposed system can further stop the attack itself, system is capable of : (1) Terminate the user session that is being used for the attack that will be removed from the cloud, (2) Block access to the target (or possibly other likely targets) from the offending user account, IP address, or other attacker attribute, (3) Block all access to the targeted host, service, application, or other resource, (4) A track on the intruder (and the intrusion) is kept to prevent the defective node from attempting to join the cloud (network) any other time, (5) Inform other users and VMs in the cloud of the intruder.

IV. Advantages of Proposed Model

IDSs proposed in related work have the problems: [22] has two problems cannot detect such as accessing the account of authorized users and false positive, [23] cannot detect new types of attacks or create signature base, [24] produce network load with an increase of VMs attached on a Mobile Agent, and [25] cannot detect any insider intrusion running on VMs and requires more training time and samples for detecting accuracy.

In the related work section, building the normal profile is based on a learning phase [8].

In comparison with the IDSs proposed in the related work, the proposed model has advantages in the cloud environment which are: (1) no need to update database of the normal profile, (2) it can detect new type of intrusion, (3) it can detect any insider intrusion, and (4) it can detect outsider intrusion.

In our solution, it is not necessary to update the normal profile because access to the information and services provided by the cloud service provider is done through authentication (through permissions and restrictions) [8].

If a host becomes the victim of the attacker, the new behavior of the host is detected, analyzed by comparing it to its normal profile, hence the intrusion is stopped.

If the attack comes from outside of the network, in such a case, the authentication of the intruder does not exist in the authentication database, where the host is not allowed to join the cloud, the intrusion is stopped.

Our proposal is based on a controller IDS, which lies in the cloud, allows for the concurrent processing of data analysis, monitoring and distributed sensing, which is an efficient approach.

For the positioning of IDS, our approach is installed on each node, on VM of cloud, and on the entire cloud computing, when other approaches are installed either on each node or on each VM.

V. Implementation of Proposed Model

The Proof-of-Concept is implemented as a first step in the direction of a mature IDS. All components are implemented in a local test environment to evaluate the concept of the proposed model.

We conducted a simulation using VirtualBox under a Windows environment. A system with a processor 3.0 GHz and 4 GB of RAM was used to conduct the simulation. To develop the function of IDS for the proposed model, we create a VM under VirtualBox; the VM has a network. We have an authentication database that has all the identity of the node (host) connected and certified by the cloud. We installed our controller IDS which is responsible for intrusion detection. To implement our IDS, we use Voyager [28] as the mobile agent platform.

At first, we launched the system with random access to the VM; an access request is made by the nodes, once authentication is verified through the database, the normal profile of the nodes is built on the basis of authentication, the current behavior of the nodes is collected by agent Mobile detection. The mobile agent is started by the IDS controller, comparing the current behavior with the normal profile is realized. In case of deviation (changing) of the behavior of the node, the measure against the intrusion is started.

To elaborate the function of our IDS model in cloud, we carried out a number of intrusion attacks like denial-of-service (DoS) attack on target machine. In DoS attacks, the intruder sends multiple pings with a very short duration of time to consume network bandwidth. DoS attacks cause a flood of traffic to the network, which leads to the denial of user services. This attack reduces network performance and increases the bandwidth [29]. For testing purposes, bad packets along with legitimate data packets were sent to the simulated system. During the test phase it was observed that the analysis module efficiently identified and discarded bad data packets.

TABLE I
Detection Result

Normal data size (KB)	24	50	100	200
Intrusion data size (KB)	10	30	99	100
Normal behavior	24	50	100	200
Intrusion detection	100%	100%	100%	99.83%
False positive	0.40%	0.58%	5.00%	6.00%

Table I shows the result of anomaly detection for the proposed model. The table shows the normal behavior (NB), intrusion detection (ID), and false alarm (FA) rates. The rate of user's normal behavior equals 100%, the ID rate is very high, and our approach detects all intrusions. The FA rate is very small because the type of these attacks is similar to normal behaviors. As the table shows, our model proposed gives good results; it detects any new attacks, detects intruders not identified by the authentication basis that originate from outside the network, detect any intruders identified by the authentication base and trying to affect proper network. Our approach is effective because it attained a 100% detection rate, with the exception of a false positive rate is very low due to the types of attacks that are still poorly detected, it is very similar to normal behavior.

VI. Conclusion and Future Work

Cloud computing is increasingly sought by clients seeking loans infrastructure, effective management of resources, and services that have a ubiquitous appearance.

However, the cloud is facing a security problem that must be solved. The IDSs provide a mechanism of protection against intrusions.

In this paper, we develop an intruder detection system based on the authentication usage of customers, checks the use of cloud by customers, reports, and prevents intruders to realize the intrusion. This is the solution for insider attack, attack flooding outsider attack, and attack on the VM.

The model proposed implements a double protection of user nodes and ensures the security of cloud environment and VM of cloud.

For future research work, we suggest to implement the proposed IDS approach in a real cloud computing environment to verify the envisioned outcome. Also, it is suggested to focus on the problem of how services are made available ubiquitously to the user (customer), and reduce the threats that weigh on cloud environments by increasing the level of security in the cloud computing environment.

REFERENCES

[1] T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, “Hey, you, get off of my cloud,”exploring information leakage in third-party compute clouds, In: CCS’09, Proceedings of the 16th ACM conference on Computer and communications security, New York: USA, 2009, pp. 199 – 212.

[2] R. Wu, G.-joon Ahnl, and H. Hul, “Information Flow Control in Cloud Computing,” IEEE Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom), 2010, pp. 1 – 7.

[3] A.E. Youssef, “Exploring Cloud Computing Services and Applications,” Journal of Emerging Trends in Computing and Information Sciences, Vol. 3, No. 6, 2012.

[4] A.E. Youssef, and M. Alageel, “A Framwork. For Secure Cloud Computing,” IJCSI International Journal of Computer Science Issues. Vol. 9. Issue 4. No. 3, 2012.

[5] Z. Mahmood, “Cloud Computing: Characteristics and Deployment Approaches,” 11th IEEE International Conference on Computer and Information Technology, 2011, pp. 121 – 126.

[6] R. Bace, and P. Mell, “NIST Special Publication on Intrusion Detection Systems,” National Institute of Standards and Technology, 2001.

[7] K. Sellami, R. Chelouah, L. Sellami, and M. Ahmed-Nacer, M, “Intrusion Detection Based on Swarm Intelligence using mobile agent,” International Conference on Swarm Intelligence: Theoretical advances and real world applications (ICSI 2011). Cergy: France; June, 2011, pp. 1 – 3.

[8] L. Sellami, D. Idoughi, and A. Baadache, “Intrusions Detection System Based on Ubiquitous Network Nodes,” INFOCOMP 2014. The Fourth
International Conference on Advanced Communications and Computation. Paris, 2014, ISBN. 978-1-61208-365-0, pp. 138 – 143

[9] J. Mchugh, A. Christie,and A. Allen, “Defending Yourself: The Role of Intrusion Detection Systems,” IEEE Software, 17(5) , 2000, pp. 42 – 51.

[10] F. Liu, J. Tong, J. Mao, R. Bohn, J. Messina, L. Badger, and D. Leaf, “NIST Cloud Computing Reference Architecture‖ (NIST SP 500-292),” National Institute of Standards and technology, Departement of commerce. U.S, 2011.

[11] P. Mell, and T. Grance, “The NIST Definition of Cloud Computing,” Recommendation of NIST. Special Publication 800-145, 2011.

[12] “Cloud Computing,” NIST Cloud Computing Program Draft Documents, Information Techology Laboratory, https://www.nist.gov/programs-projects/cloud-computing, Created November 15, 2010, Updated November 17, 2016 (accessed November 2016).

[13] L. Sellami, D. Idoughi and P.F. Tiako, "An Intrusion Detection System Based on Nodes in Cloud Computing Environments", in Proceedings of Fourth International Conference on Parallel, Distributed, Grid and Cloud Computing for Engineering, P. Iványi, B.H.V. Topping, (Editors), CivilComp Press, Stirlingshire, United Kingdom, paper 22, Croatia 2015, doi:10.4203/ccp.101.22, ISSN 1759-3433, pp. 1-10.

[14] L. Mé, and C. Michel, “La détection d’intrusion : bref aperçu et derniers développements,” 1999.

[15] B. Philippe, “Architecture expérimentale pour la détection d’intrusions dans un système informatique,” 2001.

[16] J. Lancia, “Infrastructure orientée service pour le développement d’application ubiquitaire,” These. N_d’ordre : 3745, 2008.

[17] K.V.S.N.R. Rao, A. Pal, and M.R. Patra, “A Service Oriented Architectural Design for Building Intrusion Detection Systems,” International Journal of Recent Trends in Engineering. 1(2) , 2009, pp. 11 – 14.

[18] E. Cooke, “Examination of a HIDS (SNORT + ADS),” Available at: cs.columbusstate.edu/cae-ia/studentpapers/cooke.edgar.pdf.

[19] H. Zhengbing, L. Zhitang, and W. Junqi, “Novel Network Intrusion Detection System (NIDS) Based on Signatures Search of Data Mining‖,” First International Workshop on Knowledge Discovery and Data Mining, 2008, pp. 10 – 16.

[20] K. Hwang, M. Cai, and Y. Chen, S. Member, M. Qin, “Hybrid Intrusion Detection with Weighted Signature Generation over Anomalous Internet Episodes,” IEEE Transactions on Dependable and Secure Computing. 4(1), 2007, pp. 1 – 15.

[21] A. Saxena, A. K. Sharma, "An Agent based Distributed Security System for Intrusion Detection," in Computer NetworksInternational Journal of Computer Applications (0975 – 8887), Vol 12– No.3, November 2010, pp. 18-27.https://pdfs.semanticscholar.org/
1b99/3f06a4c3fa7df5d68d7562f64a74b11b9ed1.pdf,
(accessed November 2016)

[22] J. Nikolai, “Detecting Unauthorized usage in a cloud using Tenant. Network Security” pp. 7 – 10, 2010.

[23] R. Bhadauria, R. Chaki, N. Chaki, and S. Sanyal, “A Survey on Security Issues in Cloud Computing,” The IEEE Communications Surveys and Tutorials, 2011.

[24] C. Wang, Q. Wang, K. Ren, and W. Lou, “Ensuring Data Storage Security in Cloud Computing,” 17th International Workshop on Quality of Service: (IWQoS'09), 2009, pp. 1 – 9.

[25] KABAV. Dastjerdi, SGH. Tabatabaei, Distributed intrusion detection in clouds using mobile agents. In: Third International Conference on Advanced Engineering Computing and Applications in Sciences: ADVCOMP ’09, 2009, pp. 175 – 180.

[26] K. Vieira, A. Schulter, C. Westphall, C. Westphall, “Intrusion detection techniques in grid and cloud computing environment,” IEEE IT Professional Magazine, 2010, pp.38 – 43.

[27] K.S. Narenda, and K. Parthasarathy, “Identification and control of dynamical systems using neural networks. IEEE Transaction on Neural Networks. vo. 1, no. 1, 1990, pp. 4 – 27.

[28] Recursion Software Inc, Voyager ORB Developer's Guide. www.objectspace.com, (accessed November 2016).

[29] O. Saud,” cloud intrusion detection and prevention systems taxonomy (CIDPS),”

http://www.slideshare.net/OhudSaud/cloud-intrusiondetection-and-prevention-systems-taxonomy, (accessed November 2016).