iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** XII **Month of publication:** December 2017

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue XII December 2017- Available at www.ijraset.com

Security Algorithms for User Behavior Analysis in Cloud Environment: A Survey

Thiruchendhil Arasu[1], Dr. E. George Dharma Prakash Raj[2], B. Prashanth [3]
[1]*IT Director* Dell Innovation Technology QE Performance Engg DELL Bangalore
[2] *School of Comp Sci and Engg Bharathidasan University Tiruchirappalli*
[3]*Perf. Engineer Dell Bangalore*

Abstract: Cloud Computing provides on-demand access to affordable hardware and software platforms. The Application Services hosted on Single/Multiple Cloud provider platforms have diverse characteristics that require extensive Security mechanisms to aid in controlling the Quality of Service.
Cloud computing security or, more simply, cloud security refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing. There are significant issues that need to be addressed in order for cloud computing to be adopted as universally as the Internet. Among these issues, the societal and technological issues around security for cloud computing are some of the most important and will act as both drivers and constraints for mass adoption of cloud computing. The societal issues are trust, privacy, and user behavior and how security affects these factors. The technological issues include scalability, reliability, encryption, data rights, and transparency. This paper gives a survey on various existing algorithms that are available on Cloud Computing related to user behavior.
Keywords: Cloud Computing; Data Privacy; Data Protection; Security; Virtualization; Monitoring; Deep Learning; Predictive Analytics.

I. INTRODUCTION

Cloud computing is a model for networking universal, easy and on demand access to a set of computing resources that can be quickly interfering with minimum labor, or require the service provider to be provisioned. One of the issues discussed in cloud computing, is user behavior trust in cloud services. For trusted services and users' satisfaction in the context of cloud computing behavior trust of each user should be assessed. Cloud computing subscribers, including members, local organizations and distributed resources should built trustworthy relationships among entities which are linked together. One of the major concerns of User Behavior in Cloud Computing is Security. A Cloud Secure 360 is is the need today to identify any of the security vulnerabilities at the Internet Service Provider (ISP) level by publishing the behavior pattern of different profiles in a particular area. The behavior pattern of an individual is tracked or monitored continuously based on the different actions he/she does in the internet. This service is expected to provide critical behavior based profile information to the ISP's, threat monitoring tools on the cloud and organizations that do business in the internet etc.
This paper is organized as follows. Section II gives an explanation on the various work done on Cloud Security. This is followed by an analysis of the various existing algorithms in Cloud Computing. Section IV concludes the paper.

II. USER BEHAVIOR ANALYSISALGORITHMS IN CLOUD COMPUTING

There has been good amount of related work done in the area of behavior based user profiling for the cloud security. Few of the methods are given below.

A. Cloud Rank Algorithm

A rank clustering system, Cloud Rank [1], is proposed by Sakyajit et al that takes into account cloud user preference data to characterize cloud user behavior and also identify groups of users with similar behavior in an unsupervised manner. The user groups are determined based on fitting mixture models on the cloud user preference observations. A preference can be anything that a system designer would like to include to characterize high-level user requirements such as demands on performance, cost, security, availability, etc. Cloud Rank can be useful for: (i) cloud providers to target their service offerings according to the user groups through appropriate customization of services pertaining to the user groups typical requirements; (ii) recommendation systems ora

marketplace to determine which offerings best suit certain user groups; and (iii) prediction of any new users behavior based ontheir preference information.

B. Entropy Algorithm

Li-Jun-Jain et. al. in their paper [2] have proposed a Dynamic Trust Evaluate method to deal with cloud user's behavior using Entropy method to reflect the essential regular pattern of user's behavior evidence. Some of the findings of this work are that it 1. Effectively preventing trust fraud problem with "slow rise" principle. 2. Able to timely response to malicious behavior with constantly aggravate punishment strategy ("rapid decrease" principle),effectively prevent malicious behavior and malicious user. 3. Able to actual reflect the recent credibility of the accessing user by expired trust update strategy and most recent trust calculation. 4. Has simple and customizable data structure, simple trust evaluation method, which has good scalability.

C. Anomalous Behavior Detection Algorithm

Xiaoming Ye et. al. proposes an anomalous behavior detection model [3] based on cloud computing. Virtual Machines (VMs) are one of the key components of cloud Infrastructure as a Service (IaaS). The security of such VMs is critical to IaaS security. This research into VM security issues, especially regarding VM network traffic anomalous behavior detection, remains inadequate. This paper proposes a model that uses Software-Defined Networks (SDN) to implement traffic redirection. The model can capture inter-VM traffic, detect known and unknown anomalous network behaviors, adopt hybrid techniques to analyze VM network behaviors, and control network systems. This model gives a basis for increased confidence in the security of running parts of the system in an external cloud-based environment.

D. Random Petri Network Algorithm

The paper from Xin Lu et. al. addresses the issue of credibility authentication of user behaviors in the cloud computing environment. The Paper proposes a user behavior credibility authentication model [4] built on the characteristic-based random Petri network to assess the behavior contract credibility of the users accessing the cloud service resources. This model first makes dimensional normalization of the behavioral residue data of the users and uses the decision tree ID3 algorithm to characterize the behavior a residue data of the users to check such data against the behavior authentication sets, so as to determine the credibility of the compliance of the user behaviors with the contract. User behaviors are dynamic and random, so this paper proposes the status deduction function of the random Petri network to analyze the credibility of the compliance of user behaviors with the contract. Then the credible degree is calculated to make quantitative assessment of the user behaviors' credibility. This model is able to reliably assess user behaviors' credibility in the cloud computing environment and is a certain improvement in terms of accuracy and efficiency of credibility authentication compared with the traditional models.

E. Key Stroke Dynamics Algorithm

Insider attack is the most devastating threat due to the familiarity of the underlying system to the insiders. The proposed approach by Mahesh Babuet. al. mitigates this threat by a host based user profiling technique [5] where a key stroke dynamics is used for analyzing the user behavior and a retraining approach his also proposed as the imposter patterns are absent at the time of registration. One observation made in cloud is that most of the administration work involves command line interface rather than graphical user interface. Since the command line inter face requires a lot of key strokes, the proposed approach is well suitable for this environment. If the abnormality in the user behavior is detected, the system is locked so that a malicious masquerader cannot do any modification in the name of others.

F. Rule Learning Algorithm

Insider threats still remain as one of the major concerns. Threats from malicious insiders are often listed as dangerous threats by many researchers. However, this threat has not received the attention it deserves because many organizations turn out to be extra care full about external threats than insider threats. Lucky Nkosiet. Al discusses an approach that can help in identifying insiders behaving in a malicious way, which may lead to an attack. A rule learning algorithm [6] was used in learning the behavior pattern of users, in order to build user profiles. A Matching algorithm was then used to match the historical behavior of the user with the current behavior, in order to identify users that masquerade in the system as normal users.

III. ANALYSIS OF DIFFERENT USER BEHAVIOR SECURITY ALGORITHMS IN CLOUD COMPUTING

This Section gives an analysis of the different User Behavior Security Algorithms in Cloud Computing with respect to its Pros and Cons.

TABLE I

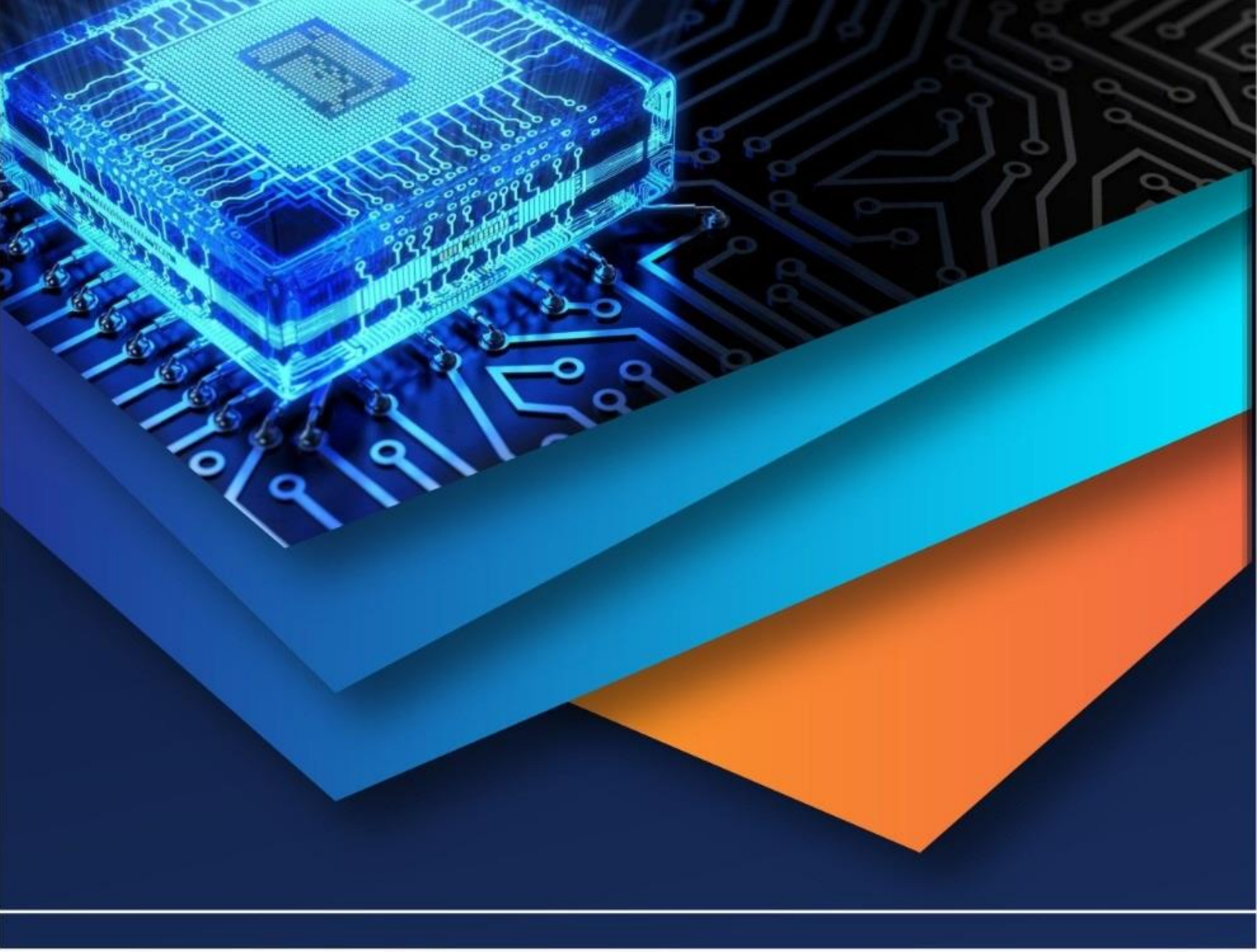
No	Algorithm	Pros	Cons
1	Cloud Rank Algorithm	Takes into account cloud user preference data to characterize cloud user behavior and also identify groups of users with similar behavior in an unsupervised manner	Misses the outside vulnerability or early detection
2	Entropy Algorithm	Dynamic trust evaluate method can effectively distinguish user's abnormal behavior.	Misses the outside vulnerability or early detection
3	Anomalous Behavior Detection Algorithm	Inter VM network behavior or anomalies. Effectiveness is greater than 90%	Misses the outside vulnerability or early detection
4	Random Petri Network Algorithm	User credibility authentication based on the contract. Based on decision tree ID3 algorithm	Misses the outside vulnerability or early detection
5	Key Stroke Dynamics Algorithm	Insider threats can be avoided; it is again through user behavior through key strokes	Misses the outside vulnerability or early detection
6	Rule Learning Algorithm	Identifies insider threat through user behavior& rule learning algorithm	Misses the outside vulnerability or early detection

IV. CONCLUSION

From this Survey paper, it can be found that there are various algorithms related to Security based on User Behavior in Cloud Computing. This paper has explained six existing algorithms which deal with Security and User Behavior Analysis in Cloud Environment. An analysis of these six algorithms show that all the methods misses the outside vulnerability or early detection. Through this paper, it can be said that Security and User Behavior Analysis in Cloud Environment with respect to outside vulnerability or early detection is a good area of research.

REFERENCES

[1] Sakyajit Bhattacharya, Tridib Mukherjee, and KoustuvDasgupta, "CloudRank: A Statistical Modelling Framework for characterizing user behavior towards targeted Cloud Management" IEEE Network Operations and Management Symposium, 201
[2] LI Jun-Jian, Li-Qin, "User's Behavior Trust Evaluate Algorithm Based OnCloud Model" IEEE Fifth International Conference on Instrumentation and Measurement, Computer, Communication and Control, 201
[3] Xiaoming Ye, Xingshu Chen, Haizhou Wang, XuemeiZeng, Guolin Shao, Xueyuan Yin, and Chun Xu, "An Anomalous Behavior Detection Model in Cloud Computing"Special Issue On Information Security ,Volume 21, Number 3, June 201
[4] Xin Lu, Cheng du, China; Yue Xu, Cheng du, China "An User Behavior Credibility Authentication Modelin Cloud Computing Environment". IEEE International Conference on Information Technology and Electronic Commerce, 2014.
[5] Mahesh Babu, Mary SairaBhanu, "Analyzing User Behavior Using KeyStrokeDynamicsto Protect Cloud from Malicious Insiders" IEEE International Conference on Cloud Computing in Emerging Markets, 2014
[6] Lucky Nkosi, Paul TarwireyiMathew O Adigun, "Detecting a Malicious Insider in the CloudEnvironment Using Sequential Rule Mining", IEEE International Conference on Adaptive Science and Technology, 2014



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY