International Journal of Science and Research (IJSR)
ISSN: 2319-7064
Impact Factor (2018): 7.426

Secure: Self-Protection Approach in Cloud Resource Management

Sangeetha G M[1], Lavanya S[2], Prashanth[3]

[1, 2]Department of CSE, Dr.AIT, Bangalore, India

[3]Department of CSE, Veerappa Nisty Engineering College, Shorapur, Yadgiri, India

Abstract: ***Cloud computing is a modern technology that increase application potentialities in terms of functioning, elastic resource management and collaborative execution approach. Cloud resource management requires complex policies and decisions for multi-objective optimization. It is challenging - the complexity of the system makes it impossible to have accurate global state information. Affected by unpredictable interactions with the environment, e.g., system failures, attacks. Cloud service providers are faced with large fluctuating loads which challenge the claim of cloud elasticity. This paper focuses on a self-protecting mechanism i.e., the property of autonomic computing was proposed to make the cloud self-protected without human intervention from intrusions and attacks. The architecture of self-protecting of cloud was presented and describes the basic interaction and functionality of each component of architecture. Self-protection is the ability of a computing system to defend itself against threats and intrusions. A self-protection component aids in distinguishing and recognizing intimidating behaviour and reacts autonomously to protect itself against malicious attacks. This paper proposes a Self-protection approach in cloud Resource management (SECURE) approach for dealing with security attacks. SECURE can create new signatures automatically and provide security against DDoS, Probing, U2R, R2L and DoS security attacks. SECURE continuously monitors security attacks during the execution of workloads, performs analysis to understand alerts in the case of security attacks, makes a plan to perform required actions to manage threats, and executes the action. Security agents (sensors) are created on SVM as an anomaly detector. SECURE increases the security of cloud-based services and increases intrusion detection rate if the same threat arrives again.***

Keywords: security attacks, cloud, resource management, zero-day attack, self-protection approach

1. Introduction

Cloud data centers are beginning to be used for a range of always-on services across private, public and commercial domains. These need to be secure and resilient in the face of challenges that include cyber-attacks as well as component failures and mis-configurations. However, clouds have characteristics and intrinsic internal operational structures that impair the use of traditional detection systems. In particular, the range of beneficial properties offered by the cloud, such as service transparency and elasticity, introduce a number of vulnerabilities which are the outcome of its underlying virtualised nature. Moreover, an indirect problem lies with the cloud's external dependency on IP networks, where their resilience and security has been extensively studied, but nevertheless remains an issue.

The approach taken in this paper relies on the principles and guidelines provided by an existing resilience framework. The underlying assumption is that in the near future, cloud infrastructures will be increasingly subjected to novel attacks and other anomalies, for which conventional signature based detection systems will be insufficiently equipped and therefore ineffective. Moreover, the majority of current signature-based schemes employ resource intensive deep packet inspection (DPI) that relies heavily on payload information where in many cases this payload can be encrypted, thus extra decryption cost is incurred. Our proposed scheme goes beyond these limitations since its operation does not depend on a-priori attack signatures and it does not consider payload information, but rather depends on per-flow meta-statistics as derived from packet header and volumetric information (i.e. counts of packets, bytes, etc.). Nonetheless, we argue that our scheme can synergistically operate with signature-based approaches on an online basis in scenarios were decryption is feasible and cost-effective. Overall, it is our goal to develop detection techniques that are specifically targeted at the cloud and integrate with the infrastructure itself in order to, not only detect, but also provide resilience through remediation.

At the infrastructure level we consider: the elements that make up a cloud datacentre, i.e. cloud nodes, which are hardware servers that run a hypervisor in order to host a number of Virtual Machines (VMs); and network infrastructure elements that provide the connectivity within the cloud and connectivity to external service users.

A cloud service is provided through one or more interconnected VMs that offer access to the outside world. Cloud services can be divided into three categories based on the amount of control retained by the cloud providers. Software as a Service (SaaS) retains the most control and allows customers to access software functionality on demand, but little else. Platform as a Service (PaaS) provides customers with a choice of execution environment, development tools, etc., but not the ability to administer their own Operating System (OS). Infrastructure as a Service (IaaS) relinquishes the most control by providing customers with the ability to install and administer their own choice of OS and install and run anything on the provided virtualised hardware; as such, IaaS clouds present the most challenges in terms of maintaining a properly functioning system. Such a system would ideally be free from malware and from vulnerabilities that could lead to an attack.

2. Problem Statement & Related Work

The intrinsic properties of virtualised infrastructures (such as elasticity, dynamic resource allocation, service co-hosting and migration) make clouds attractive as service platforms. Though, at the same time they create a new set of security challenges. These have to be understood in order to better protect such systems and make them more secure. A number of studies have addressed aspects of cloud security from different viewpoints (e.g. the network, hypervisor, guest VM and Operating System (OS)) under various approaches derived either from traditional rule-based Intrusion Detection Systems (IDSs) or statistical anomaly detection models. This paper presents a cloud security solution derived from a sub-domain of anomaly detection, viz. novelty detection. In this section we firstly review the challenges arising from the virtualisation embedded within cloud technologies and further discuss background and related work with respect to anomaly detection in cloud environments. We also present the architectural context, within which the research presented in this paper is carried out.

The problem definition of this system is to detect malware entities in public cloud infrastructures and providing secure features. The main objective is to demonstrate the methodology to detect malware entities in public cloud infrastructures maintaining the data highly secure and maintaining the data integrity and data security at cloud using encryption technique.

3. Literature Survey

A survey of literature has been carried out in ordr to identify the research problem, formulate the objectives, and determine the methodology to evaluate the proposed solution for this project.

"C. Wang" The paper "**EbAT: online methods for detecting utility cloud anomalies"**, proposes EbAT - Entropy-based Anomaly Testing - offering novel strategies that recognize inconsistencies by breaking down for subjective measurements their dispersions as opposed to singular metric limits. Entropy is utilized as an estimation that catches the level of dispersal or convergence of such circulations, amassing crude metric information over the cloud stack to frame entropy time arrangement. For adaptability, such time arrangement would then be able to be joined progressively and over different cloud subsystems. At long last, online instruments - time arrangement investigation, flag preparing or subspace strategy - are utilized to recognize oddities in entropy time arrangement (grids) in every subsystem or at each level of chain of command. The result is our capacity to 'zoom in' to the parts and measurements where peculiarities might be starting.

Disadvantages: Accuracy to be increased. Performance to be maximized. Not robust

"Y. Guan and J. Bao"The paper "A cp intrusion detection strategy on cloud computing", propose a framework for the construction of a CP intrusion detection system in E-Government. The idea can help people construct a flexible security system based on a well-organized strategy and statistical model.

Disadvantages: Security to be increased. Performance to be increased

"J.-H. Lee, M.-W. Park, J.-H. Eom, and T.-M. Chung" Distributed computing framework needs to contain some Intrusion Detection Systems (IDSs) for ensuring each Virtual Machine (VM) against dangers. There exists an exchange off between the security level of the IDS and the framework execution. In the event that the IDS give more grounded security benefit utilizing more standards or examples, at that point it needs substantially more processing assets in extent to the quality of security. So the measure of assets distributing for clients diminishes. Another issue in Cloud Computing is that, enormous measure of logs makes framework directors difficult to break down them. In this way, the paper "Multi-level interruption recognition framework and log administration in distributed computing", propose Multi-level IDS and log administration technique in light of purchaser conduct for applying IDS viably to Cloud Computing framework.

Disadvantages: Security to be increased. Lack of scalability since it requires increasingly more resources under high system workload. Performance efficiency to be increased

"A. Marnerides, S. Malinowski, R. Morla, and H. Kim."The paper "Fault diagnosis in {DSL} networks using support vector machines", display an on a very basic level new approach for ordering known DSL-level (Digital Subscriber Line) oddities by misusing the properties of curiosity recognition by means of the work of one-class Support Vector Machines (SVMs). By goodness of the lop-sidedness dwelling in the preparation tests that thus prompt tricky forecast results when utilized inside two-class plans, we receive the properties of one-class grouping and build models for freely recognizing and ordering a solitary sort of a DSL-level peculiarity. Further, use as deduction arrangements the models determined by the one-class SVM details worked by the referred to marks as hailed by the substantially more modest number of accurately designed DSLAMs in a similar system with a specific end goal to help the grouping perspective against the checked unlabelled occasions.

Disadvantages: Need to increase the efficiency and scalability.Need to increase fault tolerance and performance. Cost to be decreased.

"C. Wang, V. Talwar, K. Schwan, and P. Ranganathan" The paper "Online detection of utility cloud anomalies using metric distributions", proposes EbAT – Entropy-based Anomaly Testing – offering novel techniques that identify peculiarities by examining for subjective measurements their circulations instead of individual metric limits. Entropy is utilized as an estimation that catches the level of dispersal or convergence of such appropriations, conglomerating crude metric information over the cloud stack to shape entropy time arrangement. For adaptability, such time arrangement would then be able to be joined progressively and over various cloud subsystems.

Disadvantages: Need to increase the efficiency and scalability. Response time and cost to be decreased. Performance to be maximized.

"Q. Guan, S. Fu, N. DeBardeleben, and S. Blanchard" The paper "Exploring Time and Frequency Domains for Accurate and Automated Anomaly Detection in Cloud Computing Systems", introduce a wavelet-based multi-scale peculiarity ID system, that can examine profiled cloud execution measurements in both time and recurrence areas and recognize strange cloud practices. Learning advancements are misused to adjust the choice of mother wavelets and a sliding recognition window is utilized to deal with cloud dynamicity and enhance irregularity location precision. We have actualized a model of the oddity recognizable proof framework and led probes an on-grounds distributed computing condition.

Disadvantages: Performance and efficiency to be increased. Accuracy to be increased.

4. System Design

Framework outline is worried with making another framework in the spot of an old one. This is the most innovative and testing stage and essential as well. A powerful plan enhances procedural subtle elements important furthermore the understanding capacity for executing a shiny new framework.

Preliminary Investigation:
The as a matter of first importance methodology for improvement of a one task begins from those considered perfect planning An mail enabled stage to a little firm done which it may be not difficult what's more helpful of sending furthermore getting messages, there will be an web index ,address book also including A percentage enthralling diversions. When it will be affirmed eventually tom's perusing the association and our undertaking aide those to begin with activity, preliminary examination starts. The movement need three parts:

- "Request Clarification"
- "Feasibility Study"
- "Request Approval"

Request Clarification
Then afterward those support of the request of the acquaintanceship furthermore wander manage, for an examination constantly seen as, those wander request must make broke down choose certainly the thing that the sk obliges. Here our dare is basically inferred to customers inside those association whose frameworks could be interconnectedness by those Local Area Network (LAN). In this it involved timetable mamoncillo require all that ought to on be given on a readymade manner. Thereabouts intuition around of the enormously use of the net done ordinary life, those thinking about headway of the entrance seemed.

Feasibility Study
A crucial effect for preparatory examination may be the certification that the schema request is useful. This may be possible just in the occasion that it is time permits inside confined benefit furthermore occasion when. Those diverse feasibilities that must make broke down are.

- Operational Feasibility
- Economic Feasibility
- Technical Feasibility

Operational Feasibility
Operational possibility manages those examination from claiming prospects of the schema will make transformed. This operationally dispenses for each a standout amongst the weights of the Admin what's more makes him for viably taking after those wander propel. This sort computerization will certainly decrease those the long run Also vitality, which already used done manual fill in. In perspective of the examination, the schema is wound up constantly operationally possible.

Economic Feasibility
Financial Feasibility or Cost-advantage is an examination of the cash related legitimization for a PC based meander. As apparatus was introduced from the earliest starting point organize and for stores of purposes as requirements be the cost on meander of equipment is low. Since the structure is a system based, any number of agents related with the LAN inside that association can utilize this contraption from at whatever point. The Virtual Private Network is to be made utilizing the present assets of the association. So the meander is monetarily possible.

Technical Feasibility
Specialized foul possibility may be the assessment of the particular holdings of the cooperation. Those Acquaintanceship needs IBM flawless machines with a graphical web system connected with those web furthermore intranet. Those schema is made for phase free state. Java server Pages, JavaScript, HTML, SQL server Also WebLogic server are used should develop those schema. The specific plausibility need been completed. Those skeleton is really could be allowed for change and could make made for the present office.

Request Approval
Not every last bit request ventures would charming or achievable. A few companionship gets such an assortment for wander requests starting with client customers that selective couple of for them need aid looked for. For at whatever case, the individual ventures that need aid both conceivable what's more alluring ought to make set under want. Following a wander request may be affirmed, it cost, need, climax run through furthermore staff prerequisite may be assessed what's more utilized with evaluate the place with include it to any wander rundown. Genuinely, the support about the individuals over elements, change meets expectations could be moved.

This system need information screens for each a standout amongst those modules. Screw up messages need aid generated should alert the customer in whatever side of the point he submits a couple missteps also assistants him in the right path so that invalid passages need aid not settled on. Provide for us an opportunity should view profoundly over this under module framework. Illumination setup will be those approach to evolving over the customer committed

commitment should a pc built association. The objective of the data setup may be will make those data acceptably canny what's more free starting with blunders. The screw up is in the majority of the data need aid controlled by the majority of the data framework. Those requisition need been made done straightforward lifestyle. Those structures bring been delineated previously, such a course amid those taking care of the cursor will be set in the position the place must a chance to be entered. The customer will be moreover outfitted with previously, a decision on pick a fitting commitment starting with different decisions recognized for those field over particular instances.

Approvals are needed to each data entered toward whatever side of the point a customer enters a not right information, screw up message will be indicated and the customer could proceed ahead of the ensuing pages in the get for completing each a standout amongst the segments in the introduce page.

Input Design

Enter outline expects an magic a major aspect in the life cycle from claiming modifying advancement, it obliges exceptionally watchful thought from claiming particular architects. The illumination setup may be to sustain data of the requisition as exact as might be required under those condition. With the goal inputs ought to be wanted viably with the goal that the mistakes happening same time during the same chance bolstering need aid restricted. Likewise shown toward programming building concepts, the illumination structures or screens are exceptional to provide for bring a regard control over similarly as a wide margin concerning illustration possible, run also different related approvals.

5. Page Style

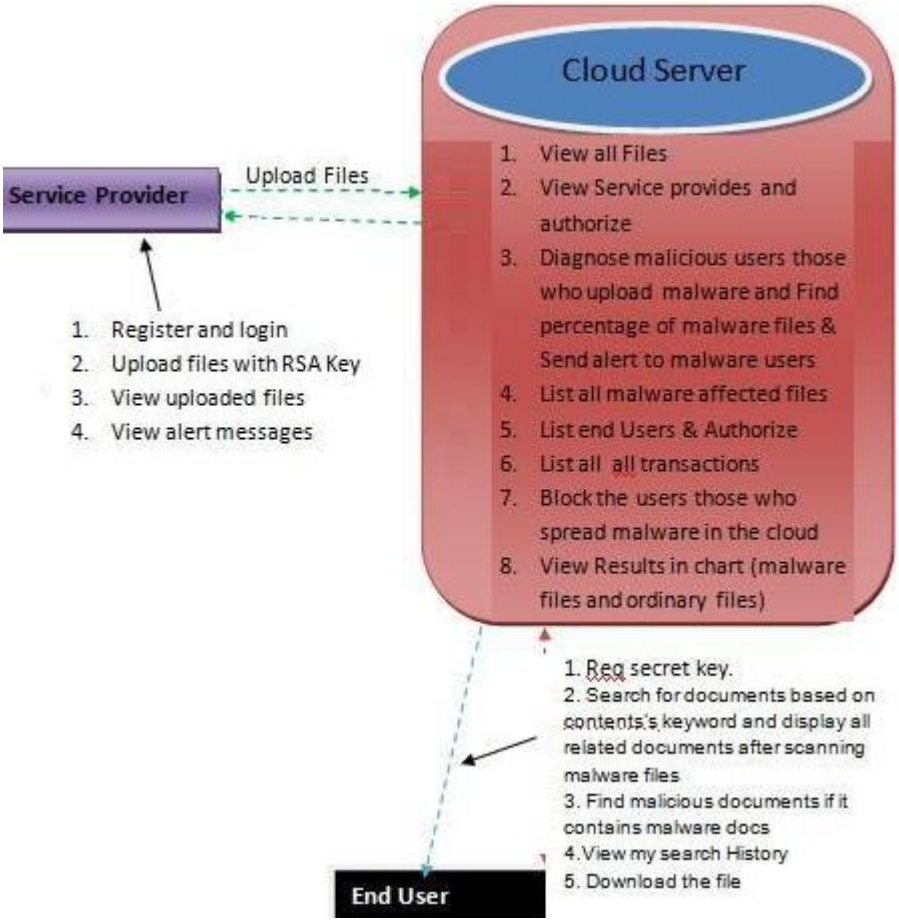

Figure 1: Architecture diagram

Output Design

The yield starting with the pc is required to generally aggravate an proficient methodology to correspondence inside those association fundamentally around the dare pioneer and as much colleagues, similarly as it were, those chief and the clients. The yield about VPN may be those skeleton which empowers the dare pioneer will manage as much clients concerning illustration significantly Similarly as making new clients furthermore doling out new undertakings on them, keeping up a record of the dare authenticity Also giving coordinator level right will each client on the customer side unexpected upon the errands designated to him. After satisfaction of a venture, an alternate wander could be doled out of the client. Customer acceptance methodologies are kept up toward the underlying phases itself. Another customer may make aggravated eventually tom's perusing those director himself alternately an customer might himself have the ability should enroll likewise an alternate customer nonetheless morals those errand for allotting ventures furthermore sanctioning an additional customer rests with those administrator in a manner of speaking.

The provision starts running at it may be executed interestingly. The server must make started and subsequently those web explorer clinched alongside used similarly as those system. Those dare will stay with running on the neighbourhood something like that the server machine will fill in likewise those administrator same time alternate co-partnered frameworks might try over concerning illustration those clients. The made schema will be profoundly straightforward also could a chance to be effortlessly understood by anybody using it not withstanding shockingly.

6. System Testing

Introduction to Testing

The test step helps in recognizing bugs. The technique which tries to find the getaway conditions and which draws out the defect in a thing is termed as testing. Among the time spent testing, the item is rehearsed with the objective of guaranteeing that the structure programming meets the yearnings of the customer and does not miss the mark in a way that can't be recognized. The different testing techniques incorporate unit testing, client acknowledgment test, acceptance testing, joining testing and yield testing.

Test case Specification

Test case specification is the test cases and the possibilities that occur for each module

Table 1: User Access permission test cases

Test Id	Test Name	Input	Output	Expected Result	Status
1	End user downloading data from server	Server IP Address	Downloaded Data from the server	Data should be downloaded	Pass
2	End user downloading data from server	Invalid Server IP Address	Cant Downloaded Data from the server	Data should be downloaded	Fail

Test Id	*Test Name*	*Input*	*Output*	*Expected Result*	*Status*
1	User Access File & SK	File Name	Get file and SK if Cloud Permitted	Get SK and file	PASS
2	User Access File MAC & SK	File Name	Should not Get file and SK if Cloud not Permitted	Get SK and file	FAIL
3	User Downloads file content	File Name	Get decrypted content if Cloud Permitted	Download Content	PASS
4	User Downloads file content	File Name	Should not Get decrypted content if Cloud not Permitted	Download Content	FAIL

Table 2: End User download permission test cases

Test Id	Test Name	Input	Output	Expected Result	Status
1	End user downloading data from server	Server IP Address	Downloaded Data from the server	Data should be downloaded	Pass
2	End user downloading data from server	Invalid Server IP Address	Cant Downloaded Data from the server	Data should be downloaded	Fail

The above table gives the test case possibilities for a data owner module when entering the IP address of cloud server. The test case result should be passed if it is directed to cloud server and it rejects in case invalid IP address.

Table 3: Unauthorised access test cases

Test Id	Test Name	Input	Output	Expected Result	Status
1	Attacker (Hacking)	File Name	Get File Details	Hack the content	PASS
2	Attacker(Hacking) With Same credential of Attacker	File Name	Get File Details	Hack the content	Fail

The above table gives the test case possibilities for an Attacker module which gives the filename and the malicious content which has added into the file or not is verified.

7. System Implementation

The principle objective of usage is to produce the code, perform different tests in light of the yield required and rectify the mistakes happening amid the project execution. Framework execution includes testing the instrument made on the setup and finding that the information is created in the focal administrator database.

Service Provider

In this module, the service provider sends the admin registration request to the cloud server and gets the acknowledgement from the cloud server for register conformation. After getting the conformation the cloud server provides the login authorization and service provider sends upload document request and acknowledges the file uploaded conformation. In this service provider upload documents with RSA key.

Cloud Server

In this module, the cloud server views all files and views service providers and authorize the service providers and it gets admin registration request from the cloud server for register conformation. After getting conformation the cloud server provides login authorization and it views all files uploaded by service providers.

It diagnose malicious users those who upload malware and find percentage of malware files and it sends alert to malware users. It blocks the users who spread malware in the cloud and it views the files segregated according to the malware content in that files like malware files and ordinary files. After, the files get uploaded by the service provider along with the RSA key and it views the files and it filters malware documents.

End User

Particular module, only user can access the file with the data with the secret key. User can search the file for a specified keyword. The data which matches for a particular keyword will be indexed in the cloud server and then response to the end user. End user will search documents based on content's keyword and display all related documents after scanning malware files.

8. Conclusion & Future Scope

The work carried out over the cloud have proposed a malware detection using one class support vector machine(SVM) which ensures maximum accuracy in detection it can possible. In the previous technique has drawbacks it cannot maximum accuracy in detection of malware entities.

Later came up with approach which is an efficient architecture and developed in order to detect malware in public cloud computing infrastructure .The experimental evaluation shows performance and also advantages of privacy preserving keyword search over encrypted data in mobile cloud computing.

The future works can be,

- The efficient way of detecting malware can be possible in public cloud computing infrastructure.
- The accuracy is more and computational cost is low so that it is more helpful in future as well

References

[1] A. K. Marnerides, M. R. Watson, N. Shirazi, A. Mauthe, and D. Hutchison, "Malware analysis in cloud computing: Network and system characteristics," IEEE Globecom 2013, 2013.
[2] M. R. Watson, N. Shirazi, A. K. Marnerides, A. Mauthe, and D. Hutchison, "Towards a distributed, self-organizing approach to malware detection in cloud computing," 7th IFIP/IFISC IWSOS, 2013.
[3] A. K. Marnerides, P. Spachos, P. Chatzimisios, and A. Mauthe, "Malware detection in the cloud under ensemble empirical model decomposition," in Proceedings of the 6th IEEE International Conference on Networking and Computing, 2015.
[4] L. Kaufman, "Data security in the world of cloud computing," Security Privacy, IEEE, vol. 7, no. 4, pp. 61–64, July 2009.
[5] N. Gruschka and M. Jensen, "Attack surfaces: A taxonomy for attacks on cloud services," in Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on, July 2010, pp. 276–279.
[6] C. Mazzariello, R. Bifulco, and R. Canonico, "Integrating a network ids into an open source cloud computing environment," in Information Assurance and Security (IAS), 2010 Sixth International Conference on, Aug 2010, pp. 265–270.
[7] S.Roschke, F. Cheng, and C. Meinel, "Intrusion detection in the cloud," in Dependable, Autonomic and Secure Computing, 2009.DASC '09. Eighth IEEE International Conference on, Dec 2009, pp. 729–734.
[8] A. Ibrahim, J. Hamlyn-Harris, J. Grundy, and M. Almorsy, "Cloudsec: A security monitoring appliance for virtual machines in the iaas cloud model," in Network and System Security (NSS), 2011 5th International Conference on, Sept 2011, pp. 113–120.
[9] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," ACM Computing Surveys (CSUR), vol. 41, no. 3, p. 15, 2009.