International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No. (02), January 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

An Analysis of Data Protection With Efficient Monitoring of The Cloud

Piyush Jain[1] Shashi Sharma[2]

[1]M.Tech Scholar, [2]Assistant Professor, Department of Computer Science & Engineering,
Jaipur Institute of Technology, Group of Institution, Jaipur, Rajasthan (India)

ABSTRACT

Cloud computing has had a transformative effect upon distributed systems. It has been one of the precursors of supposed big data revolution and has amplified the scale of software, networks, data and deployments. Cloud deployment is a rapidly and regularly change in scale and composition. This has led to the development of monitoring as a service tools which abstract the intricacies of the monitoring process. Various tools have restricted functionality and trust critical operations to third parties which often lack reliable SLAs with high costs. Still a need comes for more effective and understandable way to handle security over cloud where number of aspects seen in respect of performance including monitoring latency, resource usage and elasticity tolerance. Through investigation of multiple monitoring approaches in conjunction with a thorough examination of cloud computing compare the best one.

***Keywords**: Cloud Security, Privacy, Trust, Virtualization, Data Protection*

I. INTRODUCTION

Large scale systems each stage presents a vast range of challenges for IT peoples. Use of cloud computing provide affordable, scalable nad storage delivered in short time provide the task more feasible with proper monitoring. Monitoring is an empirical process. Dispensed alongside many conventional system many of the latencies involved in monitoring and management. In cloud computing the capacity on large and expensive infrastructure, licensing software, or training new personals make easy for customer. It provides a flexible way to access the storage and computation resources on demand. Rather than the large investment on infrastructure cloud service to be drive by many companies which can be implement through minimum managerial interaction. As per need the collection of virtualized and inter-connected computers that consists of parallel and distributed systems which can be dynamically presented and provisioned the computing resources based on Service Level Agreements (SLA) that is established by the settlement between the customers and service provider in cloud. Moving on to the cloud management is always concern about the data and services. It may arise many security challenges regarding the use of cloud computing includes the privacy and control, virtualization and accessibility vulnerabilities, credential and identity management, confidentiality, authentication of the respondent device and integrity. Still because of the cost and easy access in global word the adoption of cloud computing is growing with ensuring the complex security level, compliance and regulatory.

Cloud computing is use through Virtual Machines as a simulations from operating system to the end-user application. The effective management of the servers is performed by the combination of the virtualization

layer, software layer, and the management layer. The ability to implement security rules and monitoring throughout the cloud is done by the management layer.

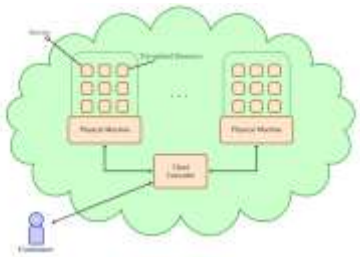


Fig. 1 Data Center Model for Cloud Computing

In the case of large scale systems, monitoring is crucial in order to understand complex and emergent system properties. Current monitoring tools originate from previous paradigms of computing including Cluster, HPC, Grid and conventional server computing which have differing requirements to cloud computing. But above in all Varanus, a new monitoring system utilizing these strategies in order to provide robust and reliable monitoring for large scale cloud deployments.

II. BACKGROUND

Cloud data is a collection of information or files regarding a individual person or an enterprise that is being stored in cloud. Cloud data usually suffers threats from various threat agents.

Anonymous Attacker: Is usually a non-trusted cloud service consumer without permission in the cloud.

Malicious service Agent: who actually intercept and forward the network traffic that flow with in a cloud.

Trusted Attacker: A trusted attacker shares IT resources in the same cloud environment as the cloud consumer.

Malicious insider: Who actually acts on behalf of cloud provider. Hence Cloud data security has become the primary focus of cloud researchers.

Data security: Data security is applied as one of the privacy measure to protect the digitalized information to protect the unauthorized access to computers associated with databases and many websites. It also protects the data from corruption as many of the organizations needs to be more prioritized by size and genre. More than encryption, Data security mainly involves three service models in this cloud computing. Normally, data is having two states of threats in cloud security called as Data at rest and Data in Transit.

Data at Rest refers to the storage of data in clouds and Data in Transit refers to the movement of data in or out from the cloud. Based on the nature of data protection, confidentiality and integrity are the two mechanisms that are needed to protect the data.

Data at Rest: This state refers to the any of the data that can be accessed using internet and can be stored in the clouds. This is the technique that can acts as a backup as well as live data. In the earlier studies, it is difficult to protect the data at rest in many organizations if there is no private cloud. At this case, they do not have data in control. This becomes

main challenge and can be resolved by a well maintained private cloud which is controlled carefully.

Data in Transit: This normally refers to the movement of data in the cloud. The data can be in the form of a database or a file that is stored in the cloud. This data can be requested at anytime, anywhere for future use at any location. Whenever the data is uploaded to the cloud at any particular instant of time, it refers to the data in transit. This is a sensitive data that can be encrypted at any time like usernames and passwords. The unencrypted data also refers to the data in transit.

III. SECURITY ISSUES AND THREAT MODELS

Security related issues of cloud data:

Data breaches: It is one of the regions in the cloud which gives the known data about all the users. And tends to huge effect on security.

Data loss/leakage: Due to insufficient authentication, authorization and audit controls, there are many ways to compromise the data such as deletion or alteration of records without backing up the original content. This would become a serious problem in the area of cloud computing.

Insecure Application Programming Interfaces(API's): These API's provides an internal and integral security to the cloud services based on their availability. These type of interfaces should be designed in a way to provide a better protection against both intruders and accidental attempts.

Malicious insiders: They are the intruders who reveal the employee's access to physical and virtual assets based on the employee monitoring and how they are analyzed. In the area of cloud computing, every organization needs not to be known the requirements of the technical details of the services that are delivered. The risks are high at this type of

situations.

Unknown Risk profile: data about who shares your infrastructure may be related. Cloud abuse: Service abuse means that attackers may abuse the cloud service and acquire the extra data available or destroy the interest of other

users.

Shared technology issues: (IaaS) it is mainly based on shared infrastructure (e.g., GPUs, CPU caches, disk partitions etc.), but not designed for strong isolation properties for multitenant architecture.

Physical security: No idea about where the resources are running. *Data seizure Risk:* Company has violated the law (risk of data seizure by (foreign) government).

Data control: Who controls the encryption/decryption keys?

Data integrity: Ensuring the data integrity which means storage, retrieval and transfer. Really means that it modifies only in response to legal transactions In the cloud environment the security issues come under many ways can be technical and non-technical. To cover all the security issues possible within the cloud are really still is a challenge. But the major Classification of security issues found within the cloud are like Abuse and Nefarious Use of Cloud Computing, Insecure Application Programming, Interfaces, Malicious Insiders, Shared Technology Vulnerabilities, Data Loss/Leakage, Account, Service and Traffic Hijacking, Unknown Risk Profile and more. Also in cloud computing any threat model is based upon the four classical security requirements of confidentiality, Integrity, Availability and Authentication.

Data authorization: In Payment Card Industry Data Security Standard (PCI DSS) data logs should be provided the security managers and regulators.

Data availability: The aim for availability of Cloud Computing systems is to protect its users can utilize them at any time .

Data Access Control: the confidential data is hacked illegally due to lack of security.

Data location: When the user makes use of cloud computing services, don't realize this issue that data is stored in which place, and the service is located in what place?

Data Confidentiality: Confidentiality means storing user's information securely in Cloud systems

Data Relocation: Another issue is the movement of data from one location to another. Data is initially stored at an appropriate location decide by the Cloud provider. However, it is often moved from one place to another.

Recovery: the client doesn't know where the data is coming from a cloud user will give the information to the customer. That leads to happening of data damage and does the user gives the restoration and so it takes much time to complete the task .

Investigative Support: the vendor ensures the capacity to scan any illegal activity.

Long-term possibility: ideally the cloud user neither get gained nor become poor .

Denial of service: Denial of a service consists of variety of techniques designed to deny users or client access to specific system and network resources. In denial of service attacks of resources are input-output, Network bandwidths, CPU utilization, Disk space and Memory utilization. Most common example of denial of service attack is the distributed DoS (DDoS)

External attack: Scanning, Malicious cracking, and probing to gather infrastructure data. The examples are insertion of malicious code or virus

Theft: The Physical theft of software or hardware, to steal the secret data for benefit is example.

Fraud: Collusion, data manipulation, falsified transaction, and other change of data integrity i.e. modification of information are the examples of fraud.

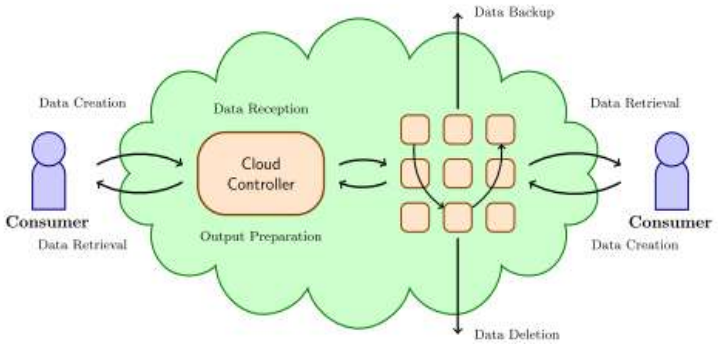


Fig 2. Data Lifecycle Threat Model for the Cloud

A third-party audit performs tests of the subject matter to form a view on the matter of assertions. In which cloud service provider security safeguards meet the security standards and also to assess the effectiveness of its control over the collection, use, retention, and disclosure of personally identifiable information.

International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No. (02), January 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

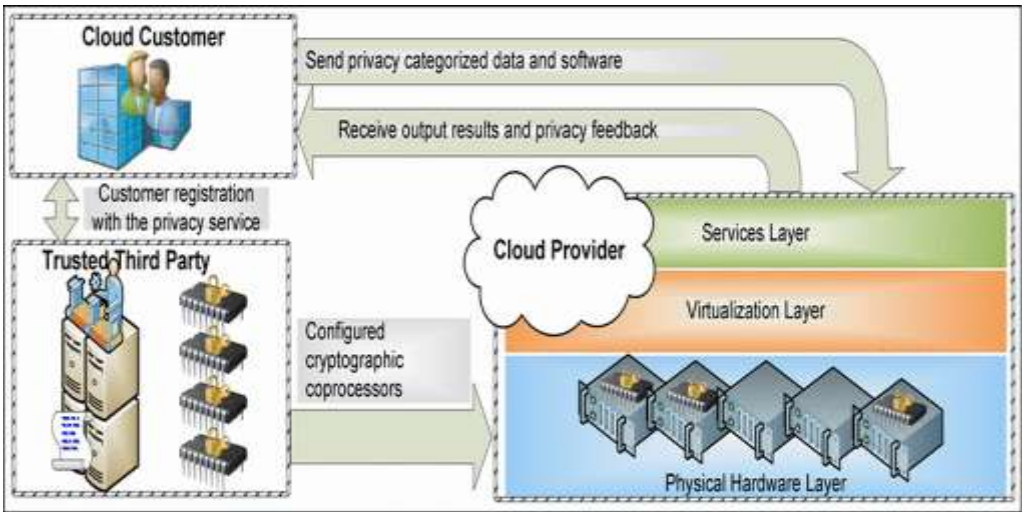


Fig. 3 Cloud Architecture

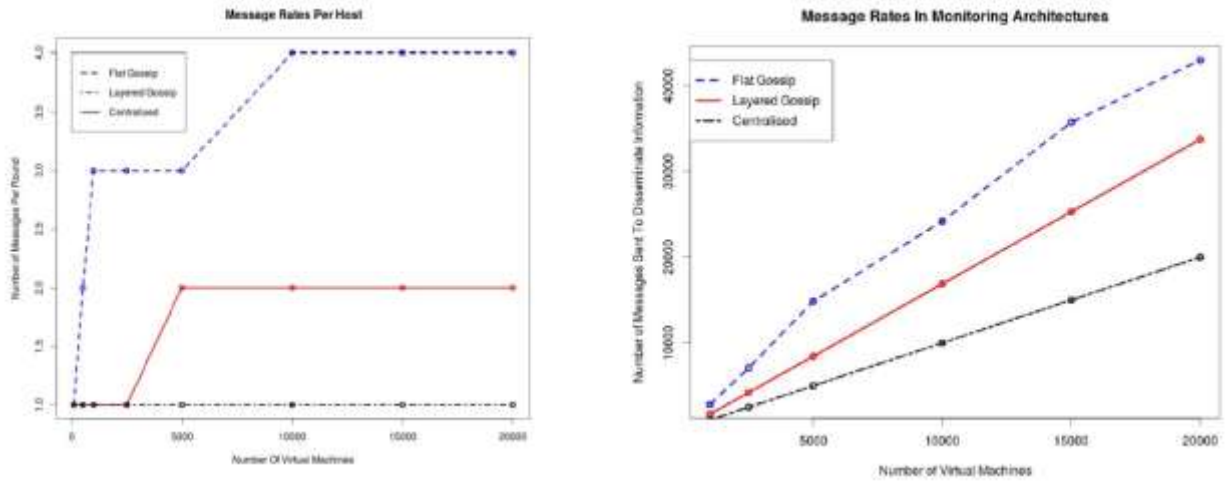
IV. EVALUATION

In the following section we will numerically evaluate Varanus against alternative monitoring strategies. A common criticism of gossip protocols is their potentially significant use of bandwidth. In Varanus computational complexity is reduced at the expense of communication complexity. In order to examine the implications of this trade-off we simulated the layered gossip architecture of Varanus, a more basic flat gossip scheme and a conventional centralized monitoring architecture (such as that of Nagios). The simulation was created in Python using the Nessi library [7]. Our software simulation implements the same data collection strategy as the actual monitoring system. The simulation records the number of messages required in order to disseminate a monitoring metric from one host to the monitoring system. Figure 4 illustrates the findings from this experiment. The two gossip based architectures have notably higher

message rates than that of the centralized architecture. In the case of the flat gossip architecture the message rate is around three times that of the centralised architecture. The additional overhead is due to the number of messages required to aggregate and then propagate information throughout the system. Despite a greater message rate than the centralized collection scheme, Varanus has a relatively conservative rate when compared to the flat scheme. This is due to the grouping and layering mechanisms present in Varanus which enforce a communication hierarchy which limits global communication. Despite being double the rate of the centralised system, a vast disparity only emerges when operating at scale. Even at scale we argue that the message rates imposed by Varanus are acceptable in a cloud environment. The high bandwidth, low latency environment present in clouds allows for applications to leverage greater message rates. The scare resource in cloud environments is CPU and memory and not bandwidth. We therefore contend that Varanus has achieved an acceptable level of background communication in exchange for decentralized

monitoring.

International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No. (02), January 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354



(A) (B)

(a) Simulated Messages Rates of Varanus and other architectures per host
(b) Simulated System Wide Message Rates of Varanus and other architectures

Fig. 4. Message rates in monitoring architectures

V. CONCLUSION

We have proposed Varanus, a highly decentralized monitoring system as a means to monitor large scale cloud systems without (or with a reduced need) for dedicated monitoring infrastructure. Varanus has significant benefits over existing systems, notably it provides mechanisms for programmatic runtime reconfiguration and executes monitoring analytics in a scalable, resource aware manner. As large cloud hosted systems become increasingly common we propose our system as a means of reducing the overhead, complexity and bottlenecks inherently associated with current monitoring technologies.

The architecture described here provides a mechanism for the scalable collection of monitoring metrics and the analysis of these metrics. It does not however provide a full, comprehensive monitoring suite. In order to fully monitor a system Varanus must become aware of applications running on the monitored system. What Varanus does provide however, is the foundation for an application aware monitoring system. The primary concern of future work is to develop application monitoring functions on top of the Varanus architecture described here.

REFERENCES

1. Ward JS, Barker A Observing the clouds: a survey and taxonomy of cloud monitoring. J Cloud Comput 3(1):1–30
2. Ward JS, Barker A (2013) Varanus: In Situ Monitoring for Large Scale Cloud Systems. In: IEEE 5th International Conference on Cloud Computing Technology and Science (CloudCom). IEEE. pp 341–344
3. Ward JS, Barker A (2014) Self managing monitoring for highly elastic large scale cloud deployments. In: Proceedings of the Sixth International Workshop on Data Intensive Distributed Computing. DIDC ’14. ACM. pp 3–10

4. Ward JS, Barker A (2012) Semantic based data collection for large scale cloud systems. In: Proceedings of the Fifth International Workshop on Data-Intensive Distributed Computing (DIDC). ACM. pp 13–22
5. Nagios. Nagios - The Industry Standard in IT Infrastructure Monitoring. http://www.nagios.org/
6. Massie ML, Chun BN, Culler DE (2004) The ganglia distributed monitoring system: design, implementation, and experience. Parallel Comput 30(7):817–840
7. Riemann. http://riemann.io/
8. Google (2014) Google Protocol Buffers. https://developers.google.com/ protocol-buffers/docs/overview
9. Amazon CloudWatch. http://aws.amazon.com/cloudwatch/
10. Datta A, Sharma R (2011) GoDisco: selective gossip based dissemination of information in social community based overlays. In: Proceedings of the 12th International Conference on Distributed Computing and Networking. Springer-Verlag, Berlin, Heidelberg. pp 227–238. http://dl. acm.org/citation.cfm?id=1946143.1946163
11. Jelasity M, Montresor A, Babaoglu O (2005) Gossip-based aggregation in large dynamic networks. ACM Trans Comput Syst (TOCS) 23(3):219–252
12. Renesse RV, Minsky Y, Hayden M (1998) A gossip-style failure detection service. In: Middleware'98. Springer. pp 55–70
13. Dressler F (2006) Weighted probabilistic data dissemination (wpdd). Dept. of Computer Science
14. Ongaro D, Ousterhout J (2014) In search of an understandable consensus algorithm. In: 2014 USENIX Annual Technical Conference (USENIX ATC

14). USENIX Association, Philadelphia, PA. pp 305–319. https://www. usenix.org/conference/atc14/technical-sessions/presentation/ongaro