Volume 5, Issue 1, January 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Literature Survey on Automated Order Processing System

Priyanka Shinde, Sujata Patel, Saylee Naik, Gayatri Chavan
Information Technology & Pune University
Maharashtra, India

Abstract — Cloud computing has characteristics and service models which include pooling of services, on demand services and broad network access. It covers controls that could be implemented in layers. Cloud computing is one of the most widely used and acceptable technique. Because of this it came into attention of various groups of people, so the security and maintenance of cloud is major issue. In this paper we have point out some of the major issues effecting the security and reliability of the cloud. Offers a Monitoring Platform-as-a-Service to each cloud consumer.

Keywords- Cloud Computing, Order Processing, Cloud Services.

I. INTRODUCTION

The cloud provider controls under the three service models. Any service-level agreement (SLA) should clearly delineate these lines of responsibility. The desired controls don't change significantly for a given layer according to whether the cloud provider or customer services to a large industry group or the public. Most clouds receiving publicity are public clouds, which are resources owned and managed by a vendor that sells or leases its services to a large industry group or the public. .While Operating a higher-layer device (IDS, IPS, or proxy) at the border that's responsible for all the traffic in and out of the data center might not be feasible. The traffic volume could be extremely high, preventing the available solutions from scaling to allow the required performance. Operating a higher-layer device (IDS, IPS, or proxy) at the border that's responsible for all the traffic in and out of the data center might not be feasible. The traffic volume could be extremely high, preventing the available solutions from scaling to allow the required performance. Middleware is natural place to monitor secure communication between various system components.

Cloud computing has matured into providing inexpensive, practical and on-demand access to computing resources. It is realising *utility computing*—the vision of the Grid and other distributed systems before it. One of the least satisfactory aspects of cloud computing is the lack of assurances about security.

II. LAYERS AND SERVICE MODELS

A cloud is modeled in seven layers: facility, network, hardware, OS, middleware, application, and the user. Monitoring at physical layer is generally in the purview of physical security. A robust physical-security policy will have many facets for surveillance, personnel, continuity of operations, and architectural resilience. Controlling and monitoring physical access to the hardware is a high priority, and surveillance should at least include closed-circuit cameras and patrolling security guards.

Architectural security should be sufficient to protect the data center from physical attack, given the value of the data inside. The provider should regularly review and update these policies as conditions change. The network access between the customer data and the users across the Internet. This border between relatively trusted space (the provider's facilities) and the inherently untrustworthy network outside is, like all such borders, important for information security and monitoring. The traffic volume could be extremely high, preventing the available solutions from scaling to allow the required performance. Unless the data center only offers one or a very few types of services, the rules for the device would be too vague to provide much value. In hardware layer provider can use software to monitor the connection topology, memory use, bus speeds, processor loads, disk storage, temperature, voltage, and so on. The provider must measure such quantities to effectively load-balance its resources. This monitoring's security implications aren't as clear. However, the provider should audit hardware configurations to verify that nothing has tampered with them. Otherwise, the provider is concerned primarily with availability and should document and report as with the facility layer.

In general, fewer features in an OS translate to fewer failure points. Given that an OS in a cloud environment has few essential functions, nonessential functionality should be removed. The host OS monitors and arranges all system calls between the virtual machines (VMs) and the hardware, so it can access any data passing to or from the VM. The cloud provider should deploy a single, hardened, pared-down OS throughout its cloud. It can then monitor these systems' images for any binary changes.

Middleware is a broad topic that can range from virtualization management tools, to data format conversion, to allowing applications to abstract away from the cloud architecture on which the middleware runs.1 Some middleware also claims to perform security functions across heterogeneous cloud architectures, such as enforcing role-based access control in a distributed fashion.2 Middleware is a significant potential weak point in a cloud provider's or customer's information assurance capabilities. Provider should be able to demonstrate that all its middleware will accept and

transmit only encrypted data. If middleware will be part of the trusted code base provided to the customer, the provider should protect it against malicious manipulation just as strongly as the OS. If an attacker replaced or modified middleware functions, it would be as damaging as modifying the OS, if not more so.

Regardless of the middleware's function, there are various safeguards to implement and pitfalls to avoid. The middleware is the natural place to monitor and secure communication between various system components because it mediates between the applications and the OS. So, the provider should be able to demonstrate that all its middleware will accept and transmit only encrypted data. If middleware will be part of the trusted code base provided to the customer, the provider should protect it against malicious manipulation just as strongly as the OS. In application layer For software as a service (SaaS), the cloud layers I previously discussed are merely the vehicle with which to provide the application. The application is the forward-facing aspect of the SaaS provider and so will expose the most code to potentially malicious users.

Applications should continue to uphold standard best practices, such as sanitizing all inputs. Host-based application security is analogous to some functions that antivirus software provides in a more traditional host-protection model. However, antivirus behavior, which operates a blacklist to identify forbidden actions, differs fundamentally from white lists, which identify permissible actions. White lists are far more secure than blacklists but lead to a much more restricted environment and are difficult to build and maintain.

III. CLOUD COMPUTING AND SECURITY

Cloud computing [6] is the latest incarnation of utility computing: the notion that computing services can be provided in a manner that is abstracted away from the computing resource itself. A key aspect is the sharing of resources to increase their utilisation: the consequent economy of scale offered to cloud providers allows them to sell slices of resource on demand in a cost effective manner.

The data of the user are very sensitive in nature, so to provide privacy to them service providers provide username and password to authenticate the user and only use of the username/password security token for authentication leaves consumer vulnerable to phishing attack.

To maintain the confidentiality of the data of cloud various cryptographic techniques are used to ensure security of the data but recent attacks make this work much difficult. The Internet had always provided some remote access but increasing bandwidth made it necessary to consider computing beyond firewall-protected local administrative domains, giving rise to new security concerns. Web-based, Service-Oriented Architectures took the provision of computing to a global scale. The Grid [7] explicitly draws an analogy between performing computing and the electricity grid. Users should be able to plug in and do their computing work with little or no attention to how the distributed computing is actually orchestrated. While grid technologies were popular for scientific infrastructure, they did not have great commercial impact. Cloud computing gained significant momentum with widespread user adoption of dynamic websites (e.g. for ecommerce).These were typically hosted on servers with PC compatible.

IV. RELATED WORK

There are many research works related to the monitoring of cloud computing infrastructures. This revision of the state-of-the-art is only focused on software used to monitor infrastructures and their services leaving aside other monitoring tools such as network traffic monitoring, QoS monitoring, SLA-monitoring, security monitoring or any other monitoring based on physical sensor devices.

There are some monitoring solutions for cloud computing infrastructures already published in the literature despite of the fact that the number of real downloadable applications is really scarce. So, *Shao et al* [4], *Huang & Wang* [5] and *Rak et al* [6] provide a centralized monitoring architecture for cloud computing infrastructures only suitable for small size deployments due to the lack of scalability associated to the centralized monitoring approach. *Tovarnak and Pitner* [7], *Dhingra et al* [8], *Selvi & Govindarajan* [9], *Katsaos* [10] together with *Shao et al* [4], *Huang & Wang* [5] provide monitoring solutions focused on the installation of a software agent in the cloud customer's VMs.

V. MONITORING PLATFORM AS SERVICE

It presents a novel monitoring architecture addressed to the cloud provider and the cloud consumers. This architecture offers a Monitoring Platform-as-a-Service to each cloud consumer that allows to customize the monitoring metrics.

The cloud provider sees a complete overview of the infrastructure whereas the cloud consumer sees automatically her cloud resources and can define other resources or services to be monitored. This is accomplished by means of an adaptive distributed monitoring architecture automatically deployed in the cloud infrastructure.

Monitoring from the point of view of the Cloud Provider

The cloud provider needs to have a complete overview of the cloud infrastructure. It requires information coming from all the possible sources of the cloud computing infrastructure. To mitigate possible bottlenecks, the architecture proposed performs a distributed monitoring (based on *DNX*) to balance this monitoring workload.

It is worthy to mention that it has been decided to install one DNX slave component in the computer of the cloud controller. The reason of this architectural decision is to cover a scenario in which there is not any other DNX slave running in the system. The rest of DNX slaves are running in VMs, so this decision covers the scenario in which there is not any VM running in the system.

VI. CONCLUSION

The centralized servers can allow the sharing of customer data between restaurants, if allowed to do so explicitly by both the customer and the business, then this can help in providing better recommendations and user experience to the patrons. This is really not possible in the stand alone systems that currently exist.A high-quality service system should be customer-centric, i.e., it should immediately recognize the identities, favourite meals and expenditure records of customers so as to provide customer-centric services. Therefore, using advanced technologies to improve service quality has attracted much attention in recent years. In recent years, various product recommendation systems have been developed to enhance customer satisfaction and perceived value. Defined as a system which recommends an appropriate product or service after learning the customers' preferences and desires, recommendation systems are powerful tools that allow companies to present personalized offers to their customers. SExtracting users' preferences through their buying behaviours and histories of purchased products is the most important element of such a system.

ACKNWOLEDGEMENT

First & foremost we would like to thank our mentor & guide to Mr. Pritesh Patil, H.O.D., Information Technology for his constant support & guidance. His active cooperation & involvement have helped us through the various stages of project Development. We would also like to express our gratitude to Mr. Pritesh Patil , for his thoughtful recommendations & suggestions. Last but not the least we would like to thank Mr. P.K. Kumbhar for extending his support.

REFERENCES

[1] Boniface, M. et al. (2010), *Platform-as-a-Service Architecture for Real-Time Quality of Service Management in Clouds*, 5th International Conference on Internet and Web Applications and Services (ICIW), Barcelona, Spain: IEEE, pp. 155–160,doi:10.1109/ICIW.2010.91

[2] Hamdaqa, Mohammad. *A Reference Model for Developing Cloud Applications*.

[3] Bacon, Jean, et al. "Information Flow Control for secure cloud computing." [2014]: 1-14.

[4] *"Cloud computing Challenges and Related Security Issues ". A survey paper, Traian Andrei,* ta8@wustl.edu, *14th May 2009*

[5] *Dinesh.C,* P.G Scholar, Computer Science and Engineering " *Data Integrity and Dynamic Storage Way in Cloud Computing,."*

[6] L.M. Kaufman, "Data Security in the World of Cloud Computing," *IEEE Security & Privacy*, vol. 7, no. 4, 2009, pp. 61–64.

[7] V. J. Winkler, *Securing the Cloud: Cloud Computer Security Techniques and Tactics*. Elsevier, 2011.

