MARKCLOUD - Software for Data Confidentiality and Security in Cloud Computing Environments

Rashidah. F. Olanrewaju, Saqib Iqbal Hakak and Othman Khalifa
Department of Electrical and Computer, Kulliyyah of Engineering
International Islamic University Malaysia
P.O Box 10, 50728 Kuala Lumpur, Malaysia

Abstract

Cloud computing is one of the most recently emerged technology which offers resource on demand facility. Cloud computing is an information technology deployment model that involves entrusting data to information systems managed by external parties on remote servers or "in the cloud." In cloud, resources, in terms of infrastructure, applications and data are deployed via the internet as a distributed service by service provider, which make use of applications without installations. This technology allows much more efficient computation by centralizing storage, memory, and processing as well as band width. However, despite the surge in activity and interest, there are significant, persistent concerns about confidentiality and security of data in cloud computing that prevented business organizations from fully accepting cloud platforms. In this paper, cloud computing security issues have been addressed. In addition, and equally important, an algorithm has been proposed that can be used between service providers and data owners to safeguard multi-way authentications and tighten access control for sensitive data in both public and private.

Keywords

Authentication, cloud computing, data confidentiality, digital watermarking, cloud marking.

1.Introduction

Cloud computing is an information technology deployment model that involves entrusting data to information systems managed by external parties on remote servers. In cloud, the architecture is distributed that keep resources in a centralize server on a scalable platform. The centralized server is to provide on demand computing resources and services to the clients with various needs [1]. Cloud platforms are offered to clients so that they may use their own cloud as they desire by cloud computing providers. The concept is similar to that of Internet service providers ISP who provide wide range of services to their clients in terms of surfing speed, downloading speed etc. Currently, there are three types of services offered by cloud computing providers which are Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS).

Today, many of the industries like Microsoft, Amazon, Google, Yahoo, Rackspace, SoftLayer and Salesforce.com are making big waves in cloud computing technology. Some of the leading cloud companies are as soon in figure 1.

Figure 1: Big companies in cloud [2]

Most of the mentioned companies benefited from cloud by Reduction in expenditure on Hardware & Software Deployment. It is also important to note that among the benefits of cloud computing is low maintenance cost as well it increase competitive environment. Business from different location and platform can use cloud conveniently.

Although, Cloud computing provides many facilities centralized storage, data processing, better bandwidth and memory, the security issues in cloud is still a concern. This matter has led to many organizations reluctant to embrace cloud services. Thus, in this paper, the main security problems in cloud computing have been identified. In addition, and equally importantly, an algorithm namely MarkCloud has been proposed that can be used between cloud service providers and data owners to safeguard multi-way authentications and tighten access control for sensitive data in both public and private clouds.

The organization of paper is as follows: Section II explains the concept of cloud computing along with its types. Section III explains the services provided by cloud computing while Section IV elaborates on security issues in Cloud computing. Framework of the proposed MarkCloud algorithm and conclusion is given in Section V

2.CONCEPT OF CLOUD COMPUTING

The concept of cloud computing relies on sharing of computer resources by instead of having personal devices or servers to run the applications. It is completely internet dependent technology making use of cyber infrastructure, and each client is assigned its own cloud, thus clients can use different services such as remote storage, resource on demand computing, data processing, integration, manage applications etc on pay per service basis. Figure 2 shows various services offered by cloud computing to its clients.

A. Types of a Cloud

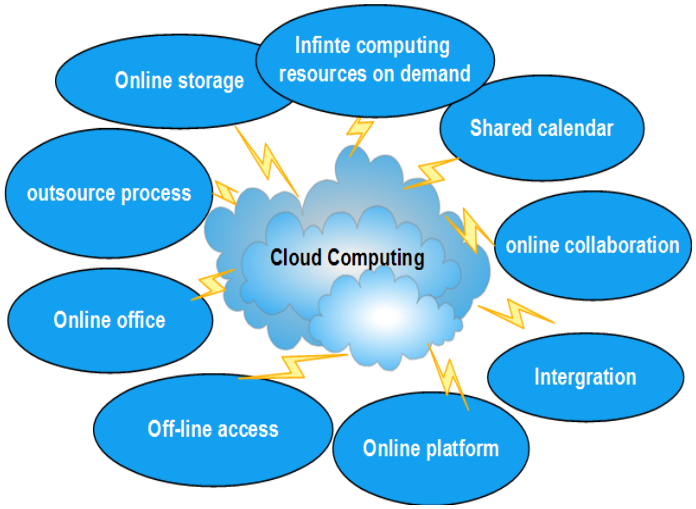
The cloud computing has four basic deployment models which are, Private cloud, Public cloud, Hybrid cloud and Community cloud [6]. Following is the description of these four deployment models:

1) **Private cloud**: cloud which is owned, leased or managed by any private organization .This kind of cloud is usually within the premises i.e. on - premises but can be outside the premises. The users or service providers who use private cloud usually have improved security as compared to public cloud although private cloud is more expensive than public cloud. Although, there is no any further addition in terms of legal requirements, security regulations, bandwidth limitations as compared to public cloud but still it is more secure due to optimized control of infrastructure [6]. Eucalyptus system is one of the best example of private cloud [7].

2) **Public Cloud**: it is that type of cloud in which users have little control over the cloud and the control is within third party. In this type of cloud, users simply use the services provided by any third party and are charged according to usage. The third party alone is responsible for all activities of cloud like installation activity, maintaining activity or resource providing activity to the end user. At a time many organizations can use the same infrastructure and users are given resources dynamically. In this kind of cloud, no access or authentication techniques can be implemented [6].One of the best example of this kind of cloud is Google search engine.

3) **Hybrid Cloud**: composed of more than one cloud deployment model. In this model, the transfer of data takes place through a hybrid model, which is composed of two or more different models. The companies can outline the needed services and goals with the help of this model [8].This model can useful for some secure services like pay roll processing or receiving customer payments [6].However, there is a major drawback getting different services from different sources and to implement that from a single location may be difficult or complicated. Amazon web services are example of Hybrid cloud.

4) **Community Cloud**: This cloud is for a shared cause in which many organizations have some agreement, based on that agreement, these organizations use the cloud and share the required infrastructure such as for in banking industries, linking contact book from Yahoo and linEdu and face book.



B. Figure 2: Cloud computing capabilities

3.SERVICES OFFERED BY CLOUD COMPUTING

Following are the services provided by cloud computing:

A. **Platform as a service (PAAS) -**This is a high level service in cloud computing. It used by web developers for custom applications development, testing and deployment platform. Applications are accomplished in PAAS with the aid of programming languages and tools [3]. Here, developers can use the equipment without requiring having such equipment physically. Hence, developing of quality programs and then transferring to the end users via internet at a reduced cost can be accomplished. Though developers will need to accept some restrictions on the type of software they can write in exchange for built-in application scalability [12]. An example is Google's App Engine [13], which enables users to build Web applications on the same scalable systems that power Google applications.

B. **Infrastructure as a service (IAAS)** – In this service, it make provision of virtual computing resources to the users such as hardware, networking, software and equipment, this includes storage facilities, processing power, operating system and virtualization technology to manage such resources. IAAS providers make use of resources to run and deploy their applications [3]. Infrastructure can scale up and down dynamically based on application and resource needed [12], that is it allows provision of resources on demand without requiring any long term commitment. Example of such is and S3 (Simple Storage Service) [14] where compute and storage infrastructures are open to public access with a utility pricing model; Amazon EC2 (Elastic Cloud Computing) Service [15] allows pay for compute capacity hourly with no long-term commitments. This frees organizations or individual from the costs and complexities of planning, purchasing, and maintaining hardware and transforms what are commonly large fixed costs into much smaller variable costs.

C. **Software as a service (SAAS)** - SAAS is a special purpose application software which is delivered over the internet to cloud clients. The users simply view the software developed by others through web browser and offer a service to users to buy it. Users can acquire services through, usage-based pricing model. Salesforce is an example of industry leader in providing online Customer Relationship Management Services. Live Mesh from Microsoft allows files and folders to be shared and synchronized across multiple devices. Figure 3 depicted the cloud computing services and the target users/client.

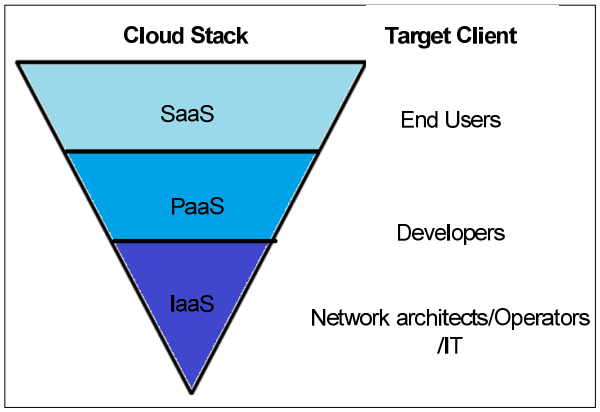


Figure 3: cloud computing services and target users/client

4.SECURITY ISSUES IN CLOUD COMPUTING

In cloud computing, users are to access cloud using some form of identities such as digital credentials, passwords and digital certificates for authorization. If any intruder or attacker could forged or steal these credentials, the cloud computing system will suffer from various attacks such as spoofing attacks, fabrication, flooding and modification. Primarily, it is known that document made public on internet are vulnerable to attacks, however, it is more severe in case of cloud computing because of different users access same data center and it is difficult to place or execute sophisticated security algorithms which may be complex for the users of the cloud. Moreover, it is difficult to enforce a common standardized credential protection mechanism due to the variety of services rendered at each cloud platform. Hence security in cloud is more challenging.

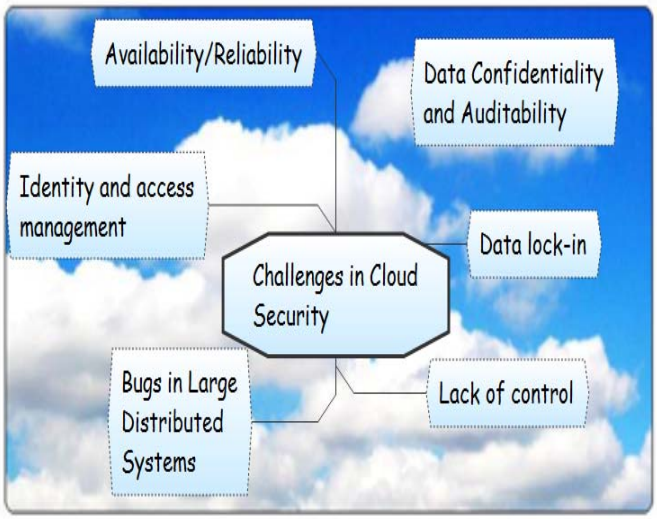


Figure 4: Security issues in cloud computing

In cloud, file sharing, online storage, online collaboration and accessing same data center may create new security threat and customer privacy issues. There are numerous potential risks to privacy and security in any cloud that requires entrusting organizations or personal data to third party. Despite the benefits and advancing in cloud computing, however, the security issue is a concern. Security issue arises due to the fact that the users who use a particular cloud for any purposes do not actually know where their data goes and, is their data in safe hands? which is very worrisome issue. Hence, embracing of cloud is not high as compare to it benefit. Although some security developments are taking place, such as formation of CSA(cloud security alliance) and OSA(open security architecture) whose aim is to devise ways to improve security concerns in cloud computing, however, intruder still sneak in the system and thus, providing security in the domain of cloud computing is becoming challenging day by day. Although it is not possible to exhaust all security issues in cloud computing, some of the main security issues have been highlighted with reference to literature:

i. **Availability of Data and service**

It is a timely access to data. Clients data needed should be readily available even when there are unpredicted power outages or hardware/software failure [16] Availability also involve ensuring that data are prevented from disasters such as natural disaster, machine faults, etc. which may cause unavailability of data. Furthermore, attacks. attackers makes use of large botnet's to reduce the profits of SaaS providers by creating Distributed Denial of Service (DDoS) hence, making their services unavailable [2]. Thus, a concrete plan should be devised for dealing with system failure of service provider along with denial of service attack [4]. Users expect high accessibility from cloud facilities; it is very attractable for large customers with business-continuity opportunity to transfer to Cloud Computing in critical situations.

ii. **Data security**

Another most interesting and important research topic in cloud computing is data security. In cloud computing, the service providers do not have complete access to the physical security system of data centers [4], so they cannot specify the security setting remotely and to be dependent on the infrastructure provider. Thus, it is difficult to know exactly, if all security services properly configured or not [4]. In this case, infrastructure provider must fulfill confidentiality, and audit ability. Data security issues arise in data such as:

a) Da**ta Lock-In where** customers cannot extract programs from the cloud and data from one location to other or inconsistence problem.
b) **Data Transfer Bottlenecks** – when applications is moved from one place to another.
c) **Traffic management and analysis –** difficulty in computing traffic matrices among hosts
d) **Network Security- This is** Ability to differentiate types of network with different level of security such as is it public, private small or big network
e) **Data Integrity-** Data can be corrupted at any level in cloud computing. In traditional data centers, there is a single database for storing data but in case of clouds , the place is not fixed as data is stored in clouds and user don't know exact location of data and data duplication can arise anywhere as there is no proper way of monitoring integration of data.
f) **Data Privacy**: This is related to knowing whether the privacy of data has been lost or not and immediate measures be in place to address such.

These were some major security issues in cloud computing, which needs to get resolved in order to groom this technology further.

5.MARCKCLOUD

MARKCLOUD is a proposed algorithm which requires intelligence to be put in the data itself. Hence data needs to be self-describing and defending, regardless of its environment. Here data is watermarked and packaged with a usage policy that protects it from disclosure of piracy & erasure. MarkCloud will be placed in any public or private cloud. Consequently, users and service providers will be communicating or exchanging data via MarkCloud. Markcloud will cover three major security issues; data integration issue, data transmission issue and intrusion detection. This security measure will be accomplished by use of digital watermarking. The methodology is explained in the form of a diagram as shown in Figure 5.

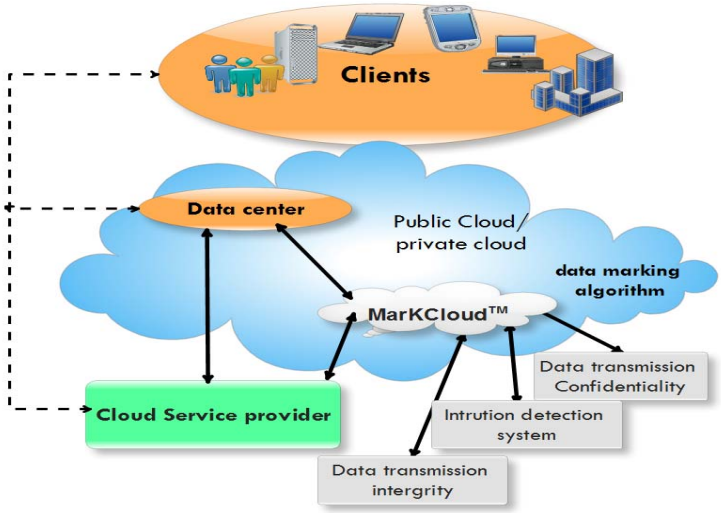


Figure 5: MarkCloud algorithm frame work

CONCLUSION

Cloud Computing is one of the major emerging technology in this era of modern and scientific age as it provides many services like saas , iaas, paas in very easy and efficient way. However, in order to make this under process technology perfect and complete, the most important issues related to security must be addressed and resolved once for all as no one can compromise with the security of his/her data. Although, researches are going on in the same domain but it needs more efforts. In this paper, main security issues are addressed along with proposed algorithm MarkCloud. With MarkCloud**,** both public and private users of cloud such as financial institutions, healthcare, forensic and education institutions can safety enjoy data protection, ensure that any data uploaded/downloaded is from correct source (not counterfeit). It can also use for automatic piracy detection and authentication.

REFERENCES

[1] Rabi Prasad Padhy, Manas Ranjan Patra,Suresh Chandra Satapathy(IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS) *Vol. 1, No. 2, December 2011)*

[2] E. Batambuze III , 2013 in Features, How - To, Latest Posts, Things To Consider When Choosing A Cloud Provider, Accessed July 2013.
http://pctechmag.com/2013/06/things-to-consider-when-choosing-a-cloud-provider/

[3] I. Sriram, A. Khajeh-Hosseini "Research Agenda in cloud technologies.

[4] V. Krishna Reddy, B. Thirumala Rao, Dr. L.S.S. Reddy, P. Sai Kiran (Global Journal of Computer Science and Technology-Volume 11 Issue 11 Version 1.0 July 2011)

[5] Chang, F., Dean, J., Ghemawat, S., Hsieh, W. C., Wallach, D. A., Burrows, M., & Gruber, R. E. (2008). Bigtable: A distributed storage system for structured data. *ACM Transactions on Computer Systems (TOCS)*, *26*(2), 4.

[6] Rabi Prasad Padhy, Manas Ranjan Patra,Suresh Chandra Satapathy(IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS) *Vol. 1, No. 2, December 2011)*

[7] B. R. Kandukuri, R. Paturi V, A. Rakshit, "Cloud Security Issues", In Proceedings of IEEE International Conference on Services Computing, pp. 517-520, 2009.

[8] M. Jensen, J. Schwenk, N. Gruschka, L. L. Iacon, "On technical Security Issues in Cloud Computing,"Proc. of IEEE International Conference on Cloud Computing (CLOUD-II, 2009), pp. 109-116, India, 2009.

[9] K. Hwang, S Kulkarni and Y. Hu, "Cloud security with virtualized defence and Reputation-based Trust management," Proceedings of 2009 Eighth IEEE International

[10] M. D. Dikaiakos, D. Katsaros, P. Mehra, G. Pallis, A. Vakali, "Cloud Computing: Distributed Internet Computing for IT and Scientific Research," IEEE Internet Computing Journal, vol. 13, issue. 5, pp. 10-13, September 2009. DOI: 10.1109/MIC.2009.103.

[11] L. Ronald, K., R. Dean Vines "Cloud Security -A Comprehensive Guide to Secure Cloud Computing", Wiley Publishing, Inc.,2010

[12] I. Foster, Y. Zhao, I. Raicu, S. Lu, Cloud Computing and Grid Computing 360-Degree Compared, 2008.

[13] Google App Engine, accessed June 2013 http://code.google.com/appengine/, 2008.

[14] Amazon Simple Storage Service (Amazon S3),
http://aws.amazon.com/s3, 2008.

[15] Amazon Elastic Compute Cloud (Amazon EC2),
http://aws.amazon.com/ec2, 2008.
http://aws.amazon.com/pricing/ec2/

[16] R. F. Olanrewaju, Nor'ashikin Bte. Ali, Othman Khalifa, Azizah AbdManaf, ICT in Telemedicine: Conquering Privacy and Security Issues in HealthCare Services, eJICST, 2013.

Biography

RASHIDAH FUNKE OLANREWAJU, is currently an Assistant Professor in the Department of Electrical and Computer Engineering, Faculty of Engineering, International Islamic University Malaysia. She earned her BSc. Hons in Software Engineering at University Putra Malaysia, in 2003. Graduated from International Islamic University Malaysia (IIUM) in 2006 with M.Sc in Information & Computer Engineering and Ph.D. (Engineering) in 2011 in the same University. She is a member of The IEEE Society, Women in Engineering, member of the Arab Research Institute of Science and Engineers ARISE) and member of Malaysian Society for

Cryptology Research. She has published in several scholarly journals and articles in ISI index databases. Her area of expertise and research interest includes information security; network security, watermarking systems, Intelligent image processing, neural networks; complex valued neural network, application of artificial intelligence in environmental management, cloud computing and secure telemedicine. Her email is frashidah@iium.edu.my.