International Journal of Computing Science and Information Technology, 2017, Vol.5, 07-12
ISSN: 2278-9669, January 2017 (http://ijcsit.org)

A novel approach for data integrity protection in cloud

Mohamed Abdul-Aziz Gaffar Ahmed, Yasir Abdelgadir Mohamed
Telecommunication Department, Future University, Collage of Computer Science, Karary University
Khartoum, Sudan
maagaa.sudan1994@gmail.com *yasir_eym@yahoo.com*

Abstract

This main aim of this paper is to propose a new method for data integrity and confidentiality in cloud. In the past few years cloud has become the buzzword in computing, however, this wide acceptance and ease of use exposed the new IT based technology into a number of data integrity (correctness of data) and security issues. Integrity of user data in the cloud servers is one of the most important concerns of users nowadays. Cloud computing has grown from being a promising business concept to one of the fast growing segments of the IT industry. But as more and more information on individuals and companies are placed in the cloud, concerns are beginning to grow about just how safe an environment it is. Security is one of the major issues which reduces the growth of cloud computing and complications with data privacy and data protection continue to plague the market. Cloud service users need to be vigilant in understanding the risks of data breaches in this new environment. So all previous studies have proved that there is a challenge facing the cloud servers regarding security, integrity and confidentiality of user's data. Moreover, the most difficult part in protecting user's data is related to the Lack of confidence that comes from the clandestine which is the owner of the servers. In this dissertation, integrity of user's data in the cloud servers which is considered as one of the most important concerns of users nowadays will be handled. A method for protecting user's data while being hosted will be deployed.

Keywords: ***MANETS, Blob-Seer, RBAC.***

1. Introduction

Cloud computing is an evolution of the way we use computers that is now rapidly increasing its popularity due to advancement of the internet technology. It is a convenient in many ways but mostly because if you have internet, you can access it and it also saves money.

It is hard to explain what exactly is the "cloud" but essentially it is a computer that you can access from anywhere with an internet connection, which is very convenient now everyone has a smartphone. There are a lot of different cloud services.

Email is one of the most popular, the files you have in your inbox for example are stored on your email provider's server. For a lot of time people used their email to store documents they need firstly by sending an email to themselves, than most providers featured some space you could upload files, and we have services like Google drive with more than 10gb of free space where you can upload your stuff.

Different approaches to cloud computing is made by huge companies. It is cheaper for them to leave the old computers that can perfectly run the cloud service application and just pay little for great services.

Another use of cloud computing, this time for small companies, is using not only cloud hardware but software too. For example it is not required to buy Microsoft office and AutoCAD when it can rent for a lot cheaper.

The delivery of computing services over the Internet. Cloud services allow individuals and businesses to use software and hardware that are managed by third parties at remote locations.

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources. Could services can serve online file storage, Social networking sites, Webmail and Online business applications.

Cloud computing has grabbed the spotlight in the year 2013 at a conference in San Francisco, with vendors providing plenty of products and services that equip IT with controls to bring order to cloud chaos. Cloud computing trend is increasing rapidly so to make cloud computing more popular the very first step for the organization is to identify exact area where the cloud related threats lie. At an unusual pace, cloud computing has transformed business and government. And this created new security challenges. The development of the cloud service model provide business – supporting technology in a more efficient way than ever before .the shift from server to service based technology brought a drastic

change in computing technology. However these developments have created new security vulnerabilities, including security issues whose full impressions are still rising. [1]

2. Related Works

Various authors proposed different frameworks to detect and stop large number of attacks which are discussed below. Integrity of user data in the cloud servers is one of the most important concerns of users nowadays. In this paper we will analyze different methodologies and protocols, which the customer/users can use to check the correctness of their data with the simplest possible way and less overhead at the customer side and to overcome the challenges faced by cloud servers for the security and integrity of user's data.

Authors in [1] proposed a generic management framework which allows the providers to enforce complex security policies. They designed an expressive policy description language to be easily interfaced with various data management systems. They efficiently protected a data storage system by evaluating their security framework on top of BlobSeer data management platform.

Other work investigated the problem of assuring customer integrity. In order to provide a way for the user to check data integrity the authors provided a scheme. This proof can be agreed up on by both the cloud provider and customer and can be in corporate in the service level agreement.

The Authors in [2] suggested four methods for cloud security and privacy which are access control method which is an application of Role Based Access Control (RBAC), and policy integration method which is a dynamic policy control mechanism, and Identity management method which prevent the un-authorized secondary usage of data. And user control method which solves the problem of cloud users losing
control of their data.

In [3] the researcher focused on technical security issues such as VM-Level attacks, isolation failure, management interface, and compromise and compliance risks. They proposed a cloud security architecture using which organizations can protect themselves against threats and attacks. The key points for architecture are single-sign on, increased availability, single management console and virtual machine protection.

A. problem justification

Integrity of user data in the cloud servers is one of the most important concerns of users nowadays. In this paper we will analyze different methodologies and protocols, which the customer/users can use to check the correctness of their data with the simplest possible way and less overhead at the customer side and to overcome the challenges faced by cloud servers for the security and integrity of user's data.

Our paper discusses the model based on MAS architecture of cloud and data encoding mechanism to enhance the integrity of Data centers. Multi Agent Systems (MAS) are basically used in artificial intelligence area as a technique for finding solution to the problems.

Cloud computing paradigm brings a lot of security challenges which are still to be resolved. The main concern is about the Integrity of data in cloud data storage. If a cloud service provider modify or delete our data from the storage due to some private problem then in that case how will we be able to verify that our data is modified or how will we be able to generate proofs that our data has been altered. These all are very serious issues related to Cloud computing .So in this paper we have discussed the current security mechanism to ensure the integrity of data in cloud storage. We have suggested a third party auditing mechanism to verify the integrity of data periodically without accessing the whole data.

3. An Approach for Data Integrity

Data security Issue-when we talk about data storage in the cloud computing or on premise application deployment model, the sensitive data of every enterprise continues to reside within the enterprise boundary and is focus to its physical, logical and personnel security and access control guidelines. Though in Software-as- a Service model or public cloud the enterprise data is stored outside the enterprise boundary, by the CSP. So as a result, the CSP must agree to implement additional security checks to ensure data security and need to prevent breaches because of security vulnerabilities in the application or through malicious employees. These all above concern issues require to use a strong encryption techniques for the protection of the data because the some traditional encryption which have been used since, are not as powerful as we need. The data protection needs to be implemented in order to secure data from the following uncertainties.

The **main idea** is enabling the customer to monitor the hosted data remotely. The normal case is that the cus-

tomer will never know whether hosted data has been modified or not since there is no tool for such table.
A snapshot of the data will be stored before being outsourced along with a hash value that should be immune to change or modification. An agent will be sent to check the hash value frequently and accordingly the data integrity as illustrated in Fig [1]. Whenever a change takes place within the hosted data then the calculated hash is matched to the stored one and accordingly a modification can be observed.

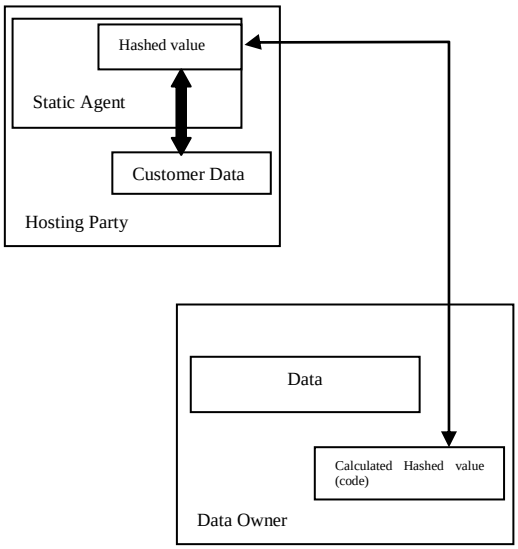

Figure 1. Integrity checking Model

Trust issue Trust in the both conventional IT business and cloud computing need to be earned. Trust is also a major issue in cloud computing. Trust revolve around assurance and confidence that people, data, objects, information will perform or behave in projected way. Trust can be in between, human to human, machine to machine, human to machine or machine to human. Therefore in cloud computing when any user store their data on cloud storage, they must have trust to the cloud provider so that they don't scare to put their data on cloud, likewise we use Gmail server, yahoo server because we trust our provider. As we know that cloud is becoming popular, many people are using cloud but still people have some doubt in their confidential mind that their data might not be safe in the cloud like they don't put their account no, passport copy and other confidential information they might think that their information may be stolen or misused. Therefore cloud provider must have to come forward to tackle with the trust issue and build trust with the users so that more and more people will be able to take advantage of cloud computing without having any doubt.

Data locality issue in the data storage model of cloud computing environment the user the applications provided by the service provider and process their data but in this scenario the user does not have any knowledge about where their data is being stored, in many situations this can be a legal issue.

Data integrity Data integrity in the cloud system means preserving information integrity. The data should not be lost or modified by unauthorized users. Data integrity is the basis to provide cloud computing service such as SaaS, PaaS, and IaaS. Data integrity can be obtained by techniques such as RAID-like strategies and digital signature.

Cloud computing provides a distributed computing environment comprises of heterogeneous components like hardware, software, firmware, networking as well as services. It changed the entire process that distributed computing used to present e.g. Grid computing, server-client computing. Cloud computing describes recent developments in many existing IT technologies and separates application and information resources from underlying infrastructure.
Cloud computing generally works on three type architecture namely:
SaaS (Software as a Service).
PaaS (Platform as a Service).
IaaS (Infrastructure as a Service).
There are different issues and concerns with each of the cloud computing technology.

4. Implementation

This part illustratest how the system it work.

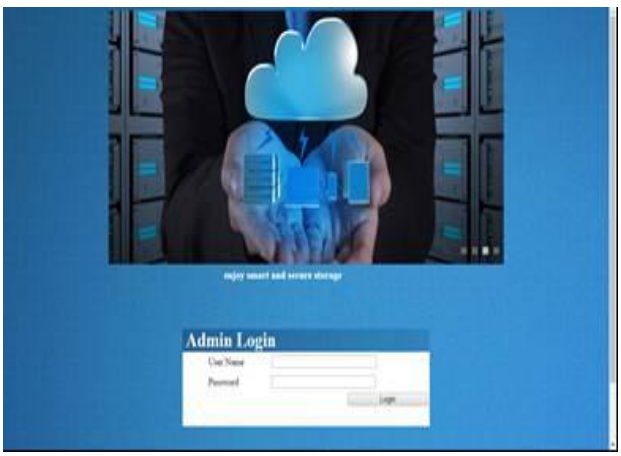

Figure. 2 System's Home page

The home screen enables the admin to choose the operation mode. The verification and authentication phases run through this mode as shown in Fig [2].

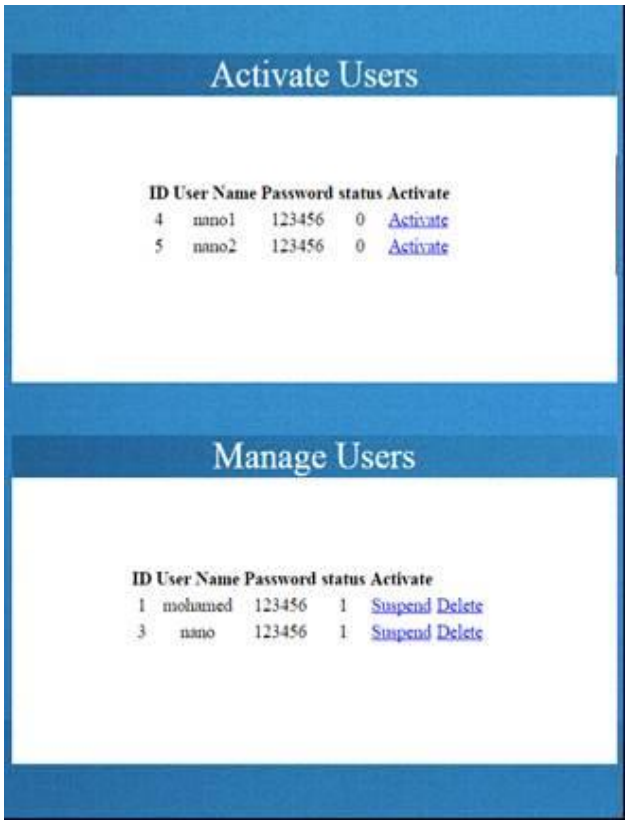

Figure. 3 Monitoring System

Fig [3] illustrates the monitoring interface through which the users' actions those are logon to the system can be controlled. The data owner can verify whether any body including the hosting party is logged on.

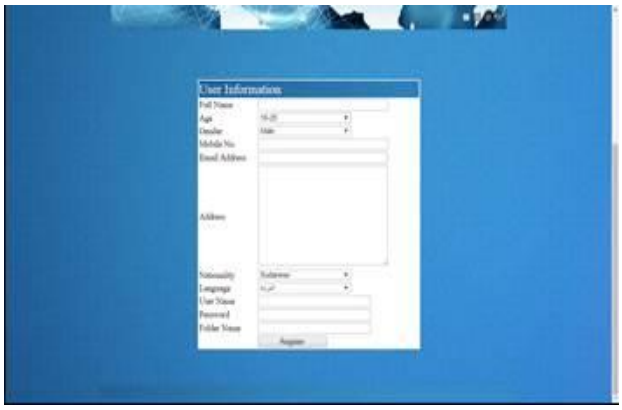

Figure. 4 Users Signing Interface

And interface for signing and interacting with the system is illustrated in Fig [4].

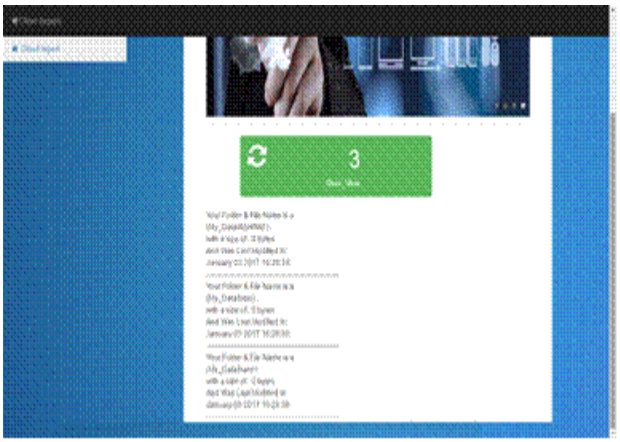

Figure.5 Tracking Report

A report for tracking files and folders that contain the required attributes through which a modification can be observed is illustrated in Fig [5].

5. Results

All previous studies and predicts have proved that there is a challenge facing the cloud servers regarding security, integrity and confidentiality of user's data. Moreover, the most difficult part in protecting user's data is related to the Lack of confidence that comes from the clandestine which is the owner of the servers.

In this dissertation, integrity of user's data in the cloud servers which is considered as one of the most important concerns of users nowadays.

To what content the objective have been achieved, so upon entering the user who is not authorized to enter, the system will monitor any modification or change is happening and give a detailed solicitation statements, whether edit, have been changed. And here the data integrity and confidentiality has been achieved. Also the system latency was reduced, also the used bandwidth was reduced will the feedback or the acknowledgment massage, and also can optimizing the periodical check timing, it's also develop the integrity part and to achieve the check for the unauthorized access and monitor the storage are activates and all modification, and generate simple feedback acknowledgment message.

6. Conclusion

Cloud computing is a technology of rapid development, however security problems have become obstacles to make the cloud computing more popular which must be solves. This proposed a security model and framework for secure cloud computing environment that identifies

security requirements, attacks, threats, concerns associated to deployment of the clouds. At the same time cloud computing technology is not just a technical problem, it is also involves standardization, supervising mode, laws and regulations, and many other aspects, there are many novels to check the integrity and confidentiality issue in cloud computing, in this dissertation it was used a new novel approach to achieve the data integrity and confidentiality in cloud that are check the data in cloud if it's modified or manipulated through an authorized user or from the clandestine that it is the owner of the servers that all data it has been hoisted on his servers, through monitor all folders and files with a contents of user data, through a calculate a total bytes of each files and also give a last modify for each files and overview for all data that has been traced, and these application can used in transaction bank as example or any company that are the data has been hosted in another place. Cloud computing is accompanied by development opportunities and challenges, along with the security problem be solved step by step, cloud computing will grow, the application will also become more and more wide.

REFERENCES

[1] Hassan, Qusay F.; Riad, laa M.; Hassan, Ahmed E. (2012). "Software reuse in the emerging cloud computing era". doi:10.4018/978-1-4666-0897-9.ch009. ISBN 978-1-4666-0897-9. Retrieved 11 December 2014.

[2] Schmidt, Eric; Rosenberg, Jonathan (2014). How Google Works. Grand Central Publishing. p. 11. ISBN 978-1-4555-6059-2.

[3] HAMDAQA, Mohammad (2012). Cloud Computing Uncovered: A Research Landscape (PDF). Elsevier Press. pp. 41–85. ISBN 0-12-396535-7.

[4] Bernstein, David; Ludvigson, Erik; Sankar, Krishna; Diamond, Steve; Morrow, Monique (2009-05-24). "Blueprint for the Intercloud – Protocols and Formats for Cloud Computing Interoperability". IEEE Computer Society: 328–336. doi:10.1109/ICIW.2009.55. ISBN 978-1-4244-3851-8.

[5] He, Sijin; L. Guo; Y. Guo; C. Wu; M. Ghanem; R. Han. "Elastic Application Container: A Lightweight Approach for Cloud Resource Provisioning". 2012 IEEE 26th International Conference on Advanced Information Networking and Applications (AINA): 15–22. doi:10.1109/AINA.2012.74. ISBN 978-1-4673-0714-7.

[6] Millard, Christopher (2013). Cloud Computing Law. Oxford University Press. ISBN 978-0-19-967168-7.

[7] Hu, Tung-Hui (2015). A Prehistory of the Cloud. MIT Press. ISBN 978-0-262-02951-3.

[8] Winkler, Vic (2011). Securing the Cloud: Cloud Computer Security Techniques and Tactics. Waltham, MA USA: Elsevier. p. 59. ISBN 978-1-59749-592-9.

[9] Mather, Tim; Kumaraswamy, Subra; Latif, Shahed (2009). Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance. O'Reilly Media, Inc. ISBN 9780596802769.

[10] Winkler, Vic (2011). Securing the Cloud: Cloud Computer Security Techniques and Tactics. Elsevier. ISBN 9781597495929.

[11] Ottenheimer, Davi (2012). Securing the Virtual Environment: How to Defend the sEnterprise against Attack. Wiley. ISBN 9781118155486.