International Engineering Journal For Research & Development

Vol.4
Issue 5

E-ISSN NO:-2349-0721

Impact factor : 6.03

DESIGN OF MODEL FOR DATA SECURITY IN CLOUD COMPUTING ENVIRONMENT

Himanshu Kale
Information Technology
Prof.Ram Meghe Intitute of Technology & Research
Amravati,India
himkale@gmail.com

Pravin Nerkar
Information Technology
Prof.Ram Meghe Intitute of Technology & Research
Amravati,India
pravinnerkar2007@gmail.com

Rupesh Hushangabade
Information Technology
Prof.Ram Meghe Intitute of Technology & Research
Amravati,India
rmhushangabade@mitra.ac.in

Abstract-

Using cloud storage, users can remotely store their data and enjoy the on-demand high-quality applications and services from a shared pool of configurable computing resources, without the burden of local data storage and maintenance. However, the fact that users no longer have physical possession of the outsourced data makes the data integrity protection in cloud computing a formidable task, especially for users with constrained computing resources. However, when outsourcing the data and business application to a third party causes the security and privacy issues to become a critical concern. Throughout the study at hand, the authors obtain a common goal to provide a comprehensive review of the existing security and privacy issues in cloud environments. This paper will discuss security issues in cloud computing and propound a new solution to secure data storage in the cloud environment.

Keywords— ***security, cloud computing, virtualization, distributed collaborative services, data encryption.***

Introduction

Cloud computing has been envisioned as the next generation information technology (IT) architecture for enterprises, due to its long list of unprecedented advantages in the IT history: on-demand self-service, ubiquitous network access, location independent resource pooling, rapid resource elasticity, usage-based pricing and transference of risk [1].Similar to confidentiality, the notion of integrity in cloud computing concerns both data integrity and computation integrity. Data integrity implies that data should be honestly Stored on cloud servers, and any violations (e.g., data is lost, altered, or compromised) are to be detected. Computation integrity implies the notion that programs are executed without being distorted by malware, cloud providers, or other malicious users [2]. A cloud computing system offers to its users the illusion of "infinite" computing and storage capacities on an on-demand basis. Examples of commercial cloud computing platforms include Amazon Elastic Compute Cloud (EC2) and Simple Storage Service (S3), Google App Engine, Microsoft Azure, etc. Virtualization [3]. In a trust negotiation process, two parties who are unknown to each other, establishes trust through an iterative bilateral exchange of credible digital identities [4].The increasingly frequent use of Cloud Computing created new security risks. Thereby increasing the interest of hackers to find new vulnerabilities and exposing users to see their data compromised [5].Cloud storage security concerns the user's data security. The purpose of this paper is to achieve data security of cloud storage and to formulate corresponding cloud storage security policy.

BACKGROUND

As a disruptive technology with profound implications, cloud computing is transforming the very nature of how businesses use information technology. One fundamental aspect of this paradigm shifting is that data are being centralized or outsourced to the cloud [1].The importance to distinguish general security issues from cloud-specific security issues. In addition, cloud computing vulnerabilities are discussed and summarized from various aspects. Consider the cloud environment as anew computing platform to which the classic methodology of security research can be applied as well [2]. Virtualization plays a vital role in cloud computing. In particular, for the purpose of scalability and flexibility of resource delivery, a cloud computing system does not provide each user with a different physical machine—instead, it allocates each user to an independently managed virtual machine (VM) which can be dynamically created, modified, and migrated [3].Trust negotiations are invaluable in collaborative applications as i) collaborations often persist over a limited time period, and therefore, ii) organizational restrictions for inclusion of these collaborative users into their local security policies. Digital identity management (IDM) is vital to facilitate reliable and seamless trust negotiations [4].The "Distributed

denial-of-service" or DDOS is a sophisticated type of attack to crash a server or a network and make it unavailable to users by temporarily interrupting or suspending the services of a machine in the internet [5].

PREVIOUS WORK DONE

Cong Wang at el (2013) [1], third-party auditor (TPA) to check the integrity of outsourced data and be worry free. To securely introduce an effective TPA, the auditing process should bring in no new vulnerabilities toward user data privacy, and introduce no additional online burden to user.
Zhifeng Xiao at el (2013) [2], present the relationships among them, the vulnerabilities that may be exploited by attackers, the threat models, as well as existing defense strategies in a cloud scenario.as well as discussing the vulnerabilities, which may be exploited by adversaries in order to perform various attacks. Defense strategies and suggestions were discussed as well.
Ron C. Chiang at el (2015) [3], demonstrate in EC2 a new type of security vulnerability caused by competition between virtual I/O workloads—i.e., by leveraging the competition for shared resources, an adversary could intentionally slow down the execution of a targeted application in a VM that shares the same hardware. Focus on I/O resources such as hard-drive throughput and/or network bandwidth—which are critical for data-intensive applications.
Albert Zomaya at el (2017) [4], propose trust based federated identity management as a cloud based utility service. The main component of this model is the trust establishment between the cloud service provider and the identity providers. We propose novel trust metrics based on the potential vulnerability to be attacked, the available security enforcements and a novel cost metric based on policy dependencies to rank the cooperativeness of identity providers.
MostaphaDerfouf at el (2015) [5], proposed solution is to add a program to encrypt the data before being fragmented and duplicated on the different storage devices and integrate the decryption functionality in restitution program so that the encrypted data will then be decrypted by the restitution program to present them to the user .Since the size of data to store is generally big, it is necessary to use a symmetric encryption algorithm based on the same cryptographic key to encrypt and decrypt data

EXISITING METHODOLIGIES

A. Third-party auditor (TPA):

Users should be able to just use the cloud storage as if it is local, without worrying about the need to verify its integrity. Thus, enabling public auditability for cloud storage is of critical importance so that users can resort to a third-party auditor (TPA) to check the integrity of outsourced data and be worry free. To securely introduce an effective TPA, the auditing process should bring in no new vulnerabilities toward user data privacy, and introduce no additional online burden to user.[1]

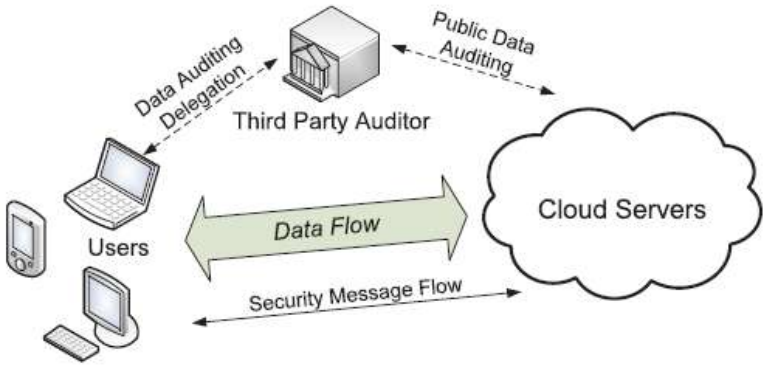


Fig 1.The architecture of cloud data storage service.

B. Ecosystem of Cloud Security and Privacy:

The ecosystem of cloud security and privacy in view of five security/privacy attributes (i.e., confidentiality, integrity, availability, accountability, and privacy-preserve ability), shown in Fig. 2, that are the most representative ones in current research advances. Some researchers regard privacy as one component of security, while in this research, separate privacy from security due to its importance and specialty in cloud environments. Privacy is considered as highly relevant to security, as well as other security attributes that have positive or negative influences on privacy. The security ecosystem is generic and is applicable to any computer and networked systems.[2]

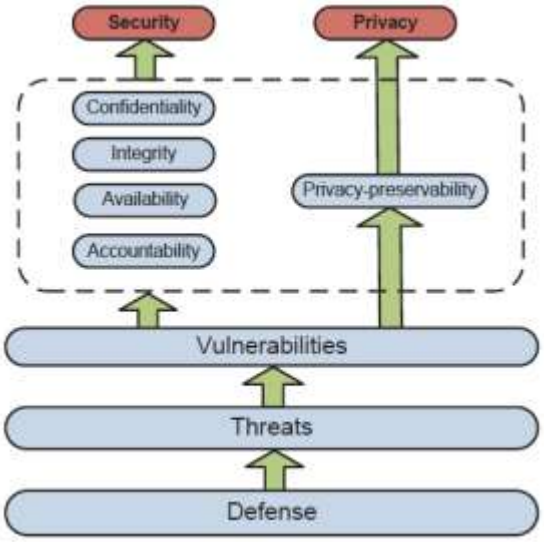


Fig 2. Ecosystem of Cloud Security and Privacy

C. Exploiting Virtual Machine Vulnerability (Swiper):

Demonstrate in EC2 a new type of security vulnerability caused by competition between virtual I/O workloads—i.e., by leveraging the competition for shared resources, an adversary could intentionally slow down the execution of a targeted application in a VM that shares the same hardware. In particular, focus on I/O resources such as hard-drive throughput and/or network bandwidth—which are critical for data-intensive applications. Implement Swiper, a framework which uses a carefully designed work load to incur significant delays on the targeted application and VM with minimum cost (i.e., resource consumption). Conduct a comprehensive set of experiments in EC2, which clearly demonstrates that Swiper is capable of significantly slowing down various server applications while consuming a small amount of resources [3].

D. Trust Negotiations Utility Service Model:

There are application level authorizations. Since the applications reside in cloud domains, there may be different authorization policies at the cloud service provider level. This is the second level. Then, in accessing different identity providers based on the way these identity providers are distributed, additional authorization policies may be required. In computing the policy dependent cost metric, do not consider the application specific policy requirements as the aim is to estimate the reliability of the IDPs in term of their cooperativeness.[4]

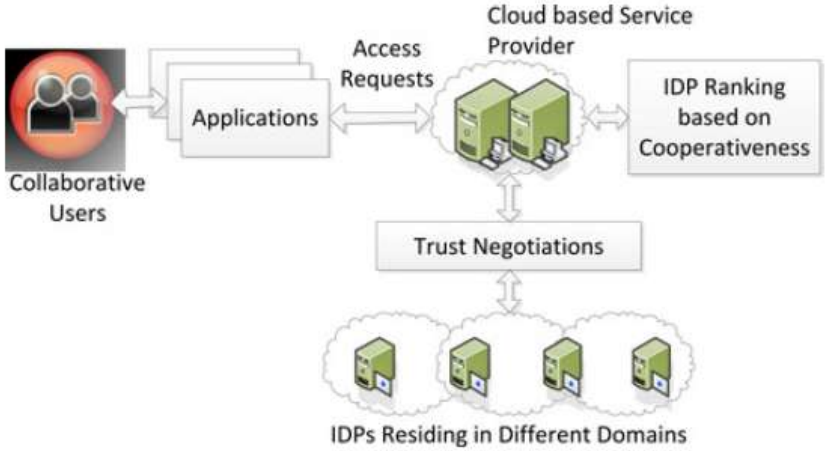


Fig 3.Functional entities in cloud based trust negotiations utility service model.

ANALYSIS AND DISCUSSION

TPA may concurrently handle multiple audit sessions from different users for their outsourced data files, we further extend our privacy-preserving public auditing protocol into multiuser setting, where the TPA can perform multiple auditing tasks in a batch manner for better efficiency. Extensive analysis shows that our schemes are provably secure and highly efficient [1].

The relationships among them, the vulnerabilities that may be exploited by attackers, the threat models, as well as existing defense strategies in a cloud scenario [2].

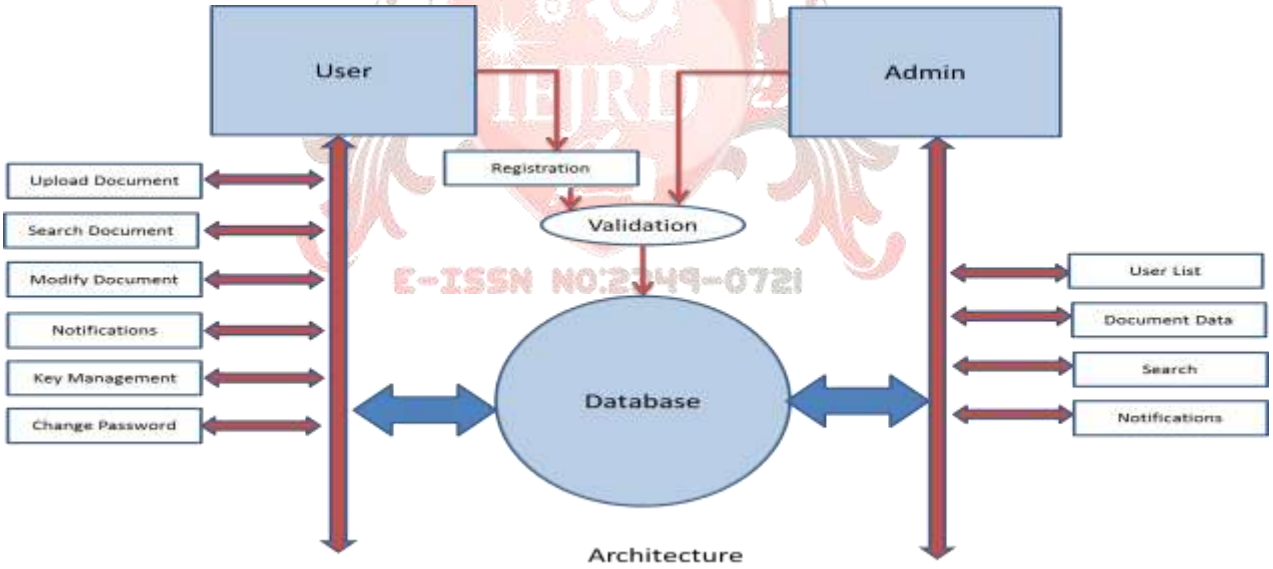
Implement Swiper, a framework which uses a carefully designed work load to incur significant delays on the targeted application and VM with minimum cost (i.e., resource consumption) [3].
Lincoln laboratory, real-life attacks and vulnerabilities extracted from Common Vulnerabilities and Exposures (CVE) repository and fuzzy rule based evaluations. The results of the evaluations imply the significance of the proposed trust model to support cloud based utility services to ensure reliable trust negotiations using federated identity management [4].
Security threats and vulnerabilities have appeared with this new concept so the cloud providers must identify these security issues and try to protect against them [5].

PROPOSED METHODOLOGY

The increasingly frequent use of Cloud Computing created new security risks. Thereby increasing the interest of hackers to find new vulnerabilities and exposing users to see their data compromised.
In proposed system we designed system for providing security in cloud computing .In proposed model there two sub models user model and admin module. User can documents, search documents, modified documents; Users have rights to manage the security key and changes passwords. In admin module have rights to manage data, and observation .Admin can view list of users, documents and there details. For security purposed we used MD5 algorithms which is describe as follows.

Basic steps of algorithm:

Step1: The file authentication will be check by MD5 algorithm.
Step2: Input file
a) convert file in 512 blocks
b) compress all data in 128 bit
c) Divides the data in 4 blocks of 32bit
d) apply binary shifting to each block
e) Convert each block in hex value
f) combine all blocks and create a hash value of 128 bit



Architecture

Step3: MD5 generate a hash value for each document. The hash value is generated two times. First time when user send a file. Second time when another user received the file. Both hash value must be same, if they are different that means the file has been modified.

OUTCOME AND POSSIBLE RESULT

Systematically studied the security and privacy issues in cloud computing based on an attribute-driven methodology, identified the most representative security/privacy attributes (e.g., confidentiality, integrity, availability, accountability, and privacy-preserve ability), as well as discussing the vulnerabilities, which may be exploited by adversaries in order to perform various attacks. Defense strategies and suggestions were discussed as well.

CONCLUSION

In this paper we have presented the different vulnerabilities related to cloud computing, we have also proposed a solution to improve the security of the storage of data in the cloud environment, it would be interesting to identify the other security vulnerabilities and find the appropriate solutions.

FUTURE SCOPE

From observations of the proposed method the future work will try to implement the proposed solution by using the Open Stack project taking into account the encryption time and performance.

REFERENCES

[1]Cong Wang, Sherman S.M. Chow, Qian Wang, "Privacy-Preserving Public Auditing for Secure Cloud Storage" *IEEE TRANSACTIONS ON COMPUTERS, VOL. 62, NO. 2, FEBRUARY 2013*

[2] Zhifeng Xiao and Yang Xiao,, "Security and Privacy in Cloud Computing", *IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 15, NO. 2, SECOND QUARTER 2013.*

[3] Ron C. Chiang, Sundaresan Rajasekaran, Nan Zhang, and H. Howie Huang,"Swiper: Exploiting Virtual Machine Vulnerability in Third-Party Clouds with Competition for I/O Resources", *IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 26, NO. 6, JUNE 2015.*

[4]Uthpala Subodhani Premarathne, Ibrahim Khalil, ZahirTari, and Albert Zomaya, "Cloud-Based Utility Service Framework for Trust Negotiations Using Federated Identity Management", *IEEE TRANSACTIONS ON CLOUD COMPUTING, VOL. 5, NO. 2, APRIL-JUNE 2017*

[5]MostaphaDerfouf * AminaMimouniMohsineEleuldj, "Vulnerabilities and storage security in Cloud Computing", *IEEE 2015.*