ISSN:0975-9646

Security on Cloud Using Mass Storage Device for Authentication

SnehaNaik
Student,
Department of Computer Science & Engineering,
SVCE Indore

Pranay Chauhan
Asst. Professor
Department of Information Technology,
SVCE Indore

Abstract: Cloud may be a concept of accessing the information from their own datacenters such the possibilities of eavesdropping is reduced and storage value is reduced. But when a number of clouds have been implemented and the data is stored dynamically then the verifiability of the node from one cloud to another is typical to achieve and the security of the data dynamics is also difficult to achieve. The work implemented here provides security of the data storage in clouds using new concept of authentication using mass storage device. The authentication provided using mass storage device is an efficient technique which provides more security to the data storage in clouds.

Keywords: Cloud Computing, Public Verifiability, Security

1. INTRODUCTION

The internet is changing into a progressively essential tool in our daily life for skilled and individual users and that they changing into more numerous. Within the present state business is progressively conducted over the internet and cloud computing is one of the foremost revolutionary concepts of current years [1].

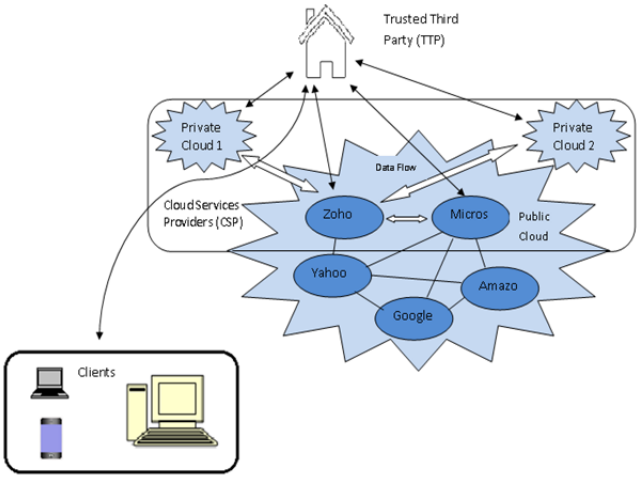

Figure 1: Computing paradigm shift of the last half century

The Cloud is a type of computing that relies on sharing computing resources other than using local servers or personal infrastructure to handle applications (Figure1). Most of the companies uses third party server rather than structure their own IT setup to host databases or software, that the company would have access to its knowledge and software over the web [2]. The utilization of Cloud Computing is gaining fame because of its quality, vast accessibility in low cost. On the opposite hand it brings additional threats to the safety of the company's knowledge and information. In recent years, data processing techniques are most victimization technique [3]. Discovering information in databases is very important in numerous fields: business, medicine, science and engineering, special data etc. The Cloud Computing provides its user's advantage of unprecedented access to valuable knowledge that may be changed into valuable insight that may facilitate them accomplish their business objectives.

1.1 Data Mining and Cloud Computing

Data mining or information discovery is that the computer-assisted method of excavation through and analyzing monumental sets of information so extracting the meaning of the information. Data processing tools predict behaviors and future trends, permitting businesses to create proactive, knowledge-driven decisions. Data mining tools can answer business queries that historically were excessively time overwhelming to resolve. They scour databases for hidden patterns, finding prognostic information that specialists might miss as a result of it lies outside their expectations [4].

Cloud computing is often defined as a type of computing that relies on sharing computing resources instead of having native servers or personal devices to handle applications [5].

1.2 Security in Cloud Computing

Internet-based on-line services provides vast amounts of resources for computing and storage space, those computing platform transfer, however, responsibility eliminating of native machines for knowledge maintenance at a similar time [6]. As the outcome, users are at the clemency of their service providers of cloud for the ease of use and integrity of their information. That the information security is a crucial part of quality of service. Within the case of cloud computing surroundings the normal cryptographic primitives for the aim of information security protection cannot be directly adopted attributable to the users' loss management of information. Therefore, verification of correct information storage within the cloud should be conducted without express information of entire data.

2. RELATED WORK

Early introduced a new scheme which provide remote information integrity and verifiability means that dynamic information operations. The method first off identifies the difficulties and potential security issues of direct extensions with absolutely dynamic information updates. It achieves

proficient information dynamics and improves the Retrievability model by manipulating the classic Merkle Hash Tree (MHT) construction used for block tag authentication. It's extremely proficient and secure technique [7] proposed a approach for planning and deploying end-to end secure and distributed software for the safety of information. It guarantees that—above a little trustworthy code base—data can't be leaked by buggy or malicious software parts. This can be crucial for cloud infrastructures, during which the keep information and hosted services all have totally different owners whose interests aren't aligned. It offers information tagging schemes and enforcement} techniques that may facilitate form the aforesaid trustworthy code base and cloud-hosted services that have end-to-end information flow control [8].

Proposed a new security load balancing architecture that is predicated on Multilateral Security (LBMS), once it reaches on peak-load it will migrate tenants' VMs mechanically to the perfect security physical machine. This protocol is based on CloudSim, a Cloud computing simulation. This design makes an attempt to avoid potential attacks when VMs migrate to physical machine owing to load balancing [9].

Focused on cost and time sensitive data processing in hybrid cloud settings, where both computational resources and data might be distributed across remote clusters. Authors developed a model for the class of Map-Reducible applications which captures the performance efficiencies and the projected costs for the allocated cloud resources. There model is based on a feedback mechanism in which the compute nodes regularly report their performance to a centralized resource allocation subsystem. The resources are then dynamically provisioned according to the user constraints [10].

Authors have extensively evaluated there system and model with two data-intensive applications with varying cost constraints and deadlines. There experimental results show that the system effectively adapts and balances the performance changes during the execution through accurate cloud resource allocation. They show that there system is effective even when one of the involved clusters drastically and instantly reduces its compute nodes. The error margins of our system's ability to meet different cost and time constraints are below 1.2% and 3.6% respectively.

Method for blog comment spam detection taking the assumption that spam is any reasonably uninformative content. It offers a language to measure the ―in formativeness‖ of a group of blog comments and tokenization independent metric. It uses an ungenerous hand-labeling strategy will operate at a capricious high exactitude level, and it dominates exactitude and recall. This model provides the content complexity metric, the utilization of a noise-tolerant logistic regression and the analysis methodology [11] introduced a handwriting authentication system. The process allows secure access to restricted data in the cloud using a mobile phone. It is composed of pre-processing, feature extraction, classification and authentication process. The classification process is based on three different classification techniques: ANN, KNN, and Euclidean Distance classifier. The classifier algorithm employs parallel combination of classifiers in order to achieve satisfactory accuracy on both recognition and error rate [12].propose a simple and effective online signature verification system that is suitable for user authentication on a mobile device. The benefits of the proposed algorithm are as follows. First, a histogram based feature set for representing an online signature can be derived in linear time and the system requires a small and fixed-size space to store the signature template. In addition, since the feature set represents only statistics about distribution of original online signature attributes, the transformation is non-invertible. As a result, the privacy of the original biometric data is well-protected. Second, a user-specific classifier comprising of a user-specific quantization step size vector and its associated quantized feature vector can be trained using only enrollment samples from that user without requiring a training set from a large number of users. Several experiments performed on MCYT and SUSIG datasets demonstrate effectiveness of the proposed method in terms of verification performance as compared to existing algorithms [13].

Security analysis of online signature verification system as compared to that of 4-digits PIN, and two usability metrics is also presented. Further investigation includes the use of other biometric key binding approaches, like fuzzy commitment, in order to strengthen security of the system, even when stored templates, helper data etc., are compromised, while preserving verification performance. Lastly, it is possible to derive a fusion approach by combining the proposed method with other existing approaches, e.g., DTW, HMM-based, etc., in order to improve verification performance, especially for applications where privacy of the signature traits is less critical.proposed a Novel mutual authentication protocol for cloud computing using secret sharing and steganography. The protocol is designed in such a way that it uses steganography as an additional encryption scheme. The scheme achieves authentication using secret sharing. Secret sharing allows a part of the secret to be kept in both sides which when combined becomes the complete secret. The secret contains information about both parties involved. Further, out of band authentication has been used which provides additional security [14].

Demonstrated how Cloud-Trust can be used to assess the security status of IaaS CCSs and IaaS CSP service offerings, and how it is used to compute probabilities of APT infiltration (high value data access) and probabilities of APT detection. These quantify two key security metrics: IaaS CCS confidentiality and integrity. Cloud-Trust also produces quantitative assessments of the value and contribution of specific CCS security controls (including several optional security controls now offered by leading commercial CSPs), and can be used to conduct sensitivity analyses of the incremental value of adding specific security controls to an IaaS CCS, when there is uncertainty regarding the value of a specific security control (which may be optional and increase the cost of CSP services) [15].

Presented dynamic risk-based access control architecture for cloud computing, with an application to cloud federations. The architecture is built as an XACML extension, adding flexibility for resource and information sharing in a dynamic

environment such as the cloud, while keeping the distribution and scalability features. The architecture is based on the use of risk policies, which describe the risk metrics considered most important by users and providers [16].

Cloud computing security plays an important role on the general public verifiability. This work studies the problem of making certain the integrity of information storage in Cloud Computing. We tend to consider the task of permitting a third party auditor (TPA), on behalf of the cloud client, to verify the integrity of the dynamic information stored on cloud. The introduction of TPA eliminates the involvement of client through the auditing of whether his information stored within the cloud is so intact. Public verifiability conjointly permits clients to delegate the integrity verification tasks to TPA whereas they themselves are often unreliable or not be able to commit necessary computation resources performing continuous verifications.

3. PROPOSED APPROACH

Verification using Mass Storage Device

The verification scheme mainly consists of four steps:

1. **Registration Phase:**

The user chooses own ID and PW, before registering on central server, it calculates MAC (ID) and MAC (ID||PW), after that it sends it to central server S over a secured channel.

On reception of registration request from user U.

S compute W=MAC (ID) xor MAC (A||ID)

X= W xor MAC (ID||PW)

Y=MAC (W)

Z=MAC (ID||PW) xor MAC (A)

The central server S generates and issues a card to the user U by storing {X, Y, Z, and MAC (.)} in the mass storage device memory. The mass storage device is delivering to the user U through secured rout.

2. Login Phase:

User U inserting card in the card reader. The card reader check if card is valid then go to login page and user enters ID* and PW*. Otherwise terminates the login process & transfers user again to registration page. After entering ID* nad PW* card reader computes.

W*= X xor MAC (ID* || PW*)

Y*= MAC (A*)

Then checks Y and Y* are equal or not. If not then terminates the login process & transfers user again to login. Otherwise If yes, then user U is a legitimate user of card. Then the card reader produces a random number R and compute.

B= W* xor R

Yid=MAC (ID||PW) xor R

C=MAC (W||Z||R||Tu) where Tu is current time of login request.

And sends login request message {C,B,Yid,Tu,MAC (ID)} to main server.

3. Verification Phase:

On receiving the login request message { C,B,Cid,Tu,MAC (ID)}. Central Server verifies time delay validity between Tu' and Tu where Tu' is the time travel of the message.

Tu'-Tu <= ΔT

If the time delays the verification process is accepted. Then central Server Computes

W*= MAC (ID) xor MAC (A|| MAC (ID))

R*=W* xor B

D=MAC (ID||PW)*=Cid xor R

Z*=MAC (ID||PW)* xor MAC (X)

C*=MAC (W*||D*||R*||Tu)

And checks whether C and C* are equal or not. Rejects the login request if they are not found equal. If true then central Server S computes

Cs=MAC (MAC (ID)||Z||R||Ts)

Where Ts is the time when message to send and sends acknowledgement message (Cs,D,Ts).

Card reader compute

D*=MAC (ID||PW)

Cs*=MAC (MAC (ID)|| Z||R||Ts)

If D and D*, Cs* and Cs are same, then card reader make session key and share both user U and central server S.

Sk=Mac (Mac (ID)||Ts||Tu||X)

Otherwise terminate to again login process.

4. Password Change Phase:

After the login valid user (checks Y*=Y)

Then it ask for new password PWnew

Then compute

X*=W xor MAC (ID||PWnew)

Z*=MAC (ID||PWnew) xor MAC (ID||PW) xor Z

And change the value of X and Z to X* and Z*.

4. SIMULATION AND RESULT

Table 1. Proposed work from various attacks

Replay attack	yes
Identity disclosure attack	Yes
Man-in the middle attack	Yes
Identity Spoofing	Yes
Insider attack	Yes
Password based attack	Yes
Eavesdropping	Yes
Outsider attack	Yes

As shown in the table 1 is the prevention of our proposed work from various attacks in the attack.

Table 2. Proposed Authentication Factor

Number of bits in token	Number of bits in secrete value
32	128

As shown in the table 2 is the analysis of first factor authentication. Here the number of bits generated in secrete value depends on the number of bits taken in token.

5. CONCLUSION AND FUTURE WORK

Cloud computing offers users the potential to reduce operating and capital expenses by investing the authorization advantages offered by massive, managed infrastructures. The conception of cloud within the accessing of information from one node to a different within the network requires security inter lay clouds thus a thought of hybrid clouds has been introduced, though it's associate efficient technique for the data access between completely different clouds but possibilities of various attacks within the cloud has additionally been enhanced. Here during this paper a short survey of various cloud computing techniques and security authentication using mass storage device has been given.

Major concern is a way to construct verification protocols which will accommodate dynamic information files. We tend to explore the problem of providing simultaneous public verifiability and information dynamics for remote information integrity check in Cloud Computing. Our construction is deliberately designed to satisfy these two necessary goals whereas efficiency being kept closely in mind.

The proposed techniques implemented here provides better authentication and chances of eavesdropping has been reduced and also prevents from various attacks such as replay attacks, DOS, etc.

REFERENCES

[1] Jia Yu, Rajkumar Buyya and Kotagiri Ramamohanarao, ―Workflow Scheduling Algorithms for Grid Computing‖, 2008 Springer Berlin Heidelberg, ISSN NO. 1860-949X, PP. 173-214, 2008.

[2] Jon Oberheide, Kaushik Veeraraghavan, Evan Cooke, Jason Flinn and Farnam Jahanian, ―Virtualized In-Cloud Security Services for Mobile Devices‖, Proceedings of the First Workshop on Virtualization in Mobile Computing(MobiVirt '08), pp. 31-35, 2008.

[3] Qian Wang, Cong Wang, Jin Li1, Kui Ren, and Wenjing Lou, ―Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing‖, 2009 Proceedings of the 14th European conference on Research in computer security(ESORICS'09), pp. 355-370, 2009.

[4] Xiang Li, Jing Liu, Jun Han and Qian Zhang, ―The Architecture Design of Micro-Learning Platform Based on Cloud Computing‖, Proceedings of the 2011 International Conference on Innovative Computing and Cloud Computing (ICCC '11), pp. 80-83, 2011.

[5] Zhang, Joshua Schiffman, Simon Gibbs, Anugeetha Kunjitha,patham, and Sangoh Jeong, ―Securing Elastic Applications on Mobile Devices for Cloud Computing‖, Proceedings of the 2009 ACM workshop on Cloud computing security(CCSW '09), pp. 127-134, 2009.

[6] Yan Zhu, Huaixi Wang, Zexing Hu, Gail-Joon Ahn, Hongxin Hu, Stephen S. Yau ―Efficient Provable Data Possession for Hybrid Clouds‖, 2010 Proceedings of the 17th ACM conference on Computer and communications security (CCS '10), pp. 756-758, 2010.

[7] Qian Wang, Cong Wang, Jin Li, Kui Ren, and Wenjing Lou, "Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing", ESORICS'09 Proceedings of the 14th European conference on Research in computer security, Pages 355-370 Springer-Verlag Berlin, Heidelberg ©2009.

[8] Jean Bacon, David Evans, David M. Eyers, Matteo Migliavacca, Peter Pietzuch, and Brian Shand, "Enforcing End-to-end Application Security in the Cloud", Middleware '10 Proceedings of the ACM/IFIP/USENIX 11th International Conference on Middleware, Pages 293-312 Springer-Verlag Berlin, Heidelberg ©2010.

[9] Pengfei Sun, Qingni Shen, Ying Chen, Zhonghai Wu and Cong Zhang," POSTER: LBMS: Load Balancing based on Multilateral Security in Cloud", CCS'11, October 17–21, 2011, ACM Chicago, Illinois, USA.

[10] Tekin Bicer, David Chiu & Gagan Agrawal presented paper entitled "Time and Cost Sensitive Data-Intensive Computing on Hybrid Clouds" at 2012, 12th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing.

[11] Alex Kantchelian, Justin Ma, Ling Huang, Sadia Afroz, Anthony D. Joseph and J. D. Tygar, "Robust Detection of Comment Spam Using Entropy Rate", AISec'12, October 19, 2012, ACM Raleigh, North Carolina, USA.

[12] F. Omr, S. FoufoU, R. HamiIa & M. Jarraya presented paper entitled "Cloud-based Mobile System for Biometrics Authentication" at IEEE 2013 13th International Conference on ITS Telecommunications (ITST).

[13] Napa Sae-Bae & Nasir Memon presented paper entitled "Online Signature Verification on Mobile Devices" at IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 6, JUNE 2014.

[14] Nimmy K. and M. Sethumadhavan, "Novel Mutual Authentication Protocol for Cloud Computing using Secret Sharing and Steganography", 978-1-4799-2259-14/$31.00©2014 IEEE.

[15] Dan Gonzales, Jeremy Kaplan, Evan Saltzman, Zev Winkelman & Dulani Woods presented paper entitled "Cloud-Trust - a Security Assessment Model for Infrastructure as a Service (IaaS) Clouds" at IEEE TRANSACTIONS ON JOURNAL GONZALES, TCC-2014-03-0102.

[16] Daniel Ricardo dos Santos, Carla Merkle Westphall and Carlos Becker Westphall, "A Dynamic Risk-based Access Control Architecture for Cloud Computing", 978-1-4799-0913-1/14/$31.00 c 2014 IEEE.