Implement Security using smart card on Cloud

Amish Kumar Aman[1], Vijay Prakash[2]

Abstract

Cloud is a concept of accessing the data from their own datacenters such that the chances of eavesdropping have been reduced and storage cost is reduced. Here in this paper we are giving a brief survey of various cloud based technique implemented so far. Although there are various techniques implemented so far for the cloud computing but here we are giving a survey of not only cloud based techniques but also the concept of smart cards for the authentication between one cloud to another cloud.

Keywords

Cloud Computing, Security, Public Verifiability

1. Introduction

The Internet is becoming an increasingly vital tool in our everyday life for professional and personal users and they becoming more numerous. In the present scenario business is increasingly conducted over the Internet. And in the field of internet cloud computing is one of the most revolutionary concepts of recent years.

The Cloud, is referred to, involvement of using computing resources hardware and software which combindly delivers services over the Internet (Figure1). Many companies accepts the third party to host them on its large servers instead of building their own IT infrastructure to host databases or software, so the company would have access to its data and software over the Internet. The use of Cloud Computing is gaining popularity due to its mobility, huge availability in low cost. On the other hand it brings more threats to the security of the company's data and information. In recent years, data mining techniques are most using technique. Discovering knowledge in databases becoming increasingly vital in various fields: business, medicine, science and engineering, spatial data etc. The Cloud Computing provides its users benefit of unprecedented access to valuable data that can be turned into valuable insight that can help them achieve their business objectives.

Amish Kumar Aman, SVITS Indore, India.
Vijay Prakash, SVITS Indore, India.

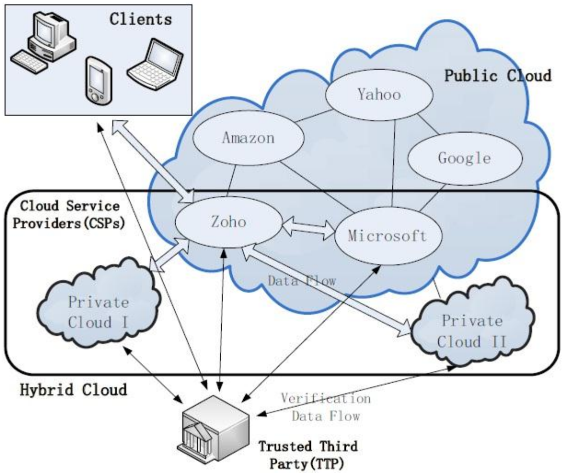

Figure 1: Computing paradigm shift of the last half century [1] by yang

1.1 Data Mining and Cloud Computing

Data mining in cloud computing is the process of extracting structured information from unstructured or semi-structured web data sources. It allows organizations to centralize the management of software and data storage, with assurance of efficient, reliable and secure services for their users.

Cloud computing refers to software and hardware delivered as services over the Internet. The implementation of data mining techniques through Cloud computing will allow the users to retrieve meaningful information from virtually integrated data warehouse that reduces the costs of infrastructure and storage.

1.2 Security in Cloud Computing

Internet-based online services provides huge amounts of storage space and customizable computing resources, this computing platform shift, however, is eliminating the responsibility of local machines for data maintenance at the same time. As a result, users are at the mercy of their cloud service providers for the availability and integrity of their data. So the data security is an important aspect of quality of service. In the case of cloud computing environment the traditional cryptographic primitives for the purpose of data security protection cannot be directly adopted due to the users' loss control of data. Therefore, verification of correct data storage in the cloud must be conducted without explicit knowledge of the whole data.

Authentication using Smart Cards

The authentication scheme mainly consists of 4 steps:
1. Registration Phase
User of any cloud chooses own ID and PW, before to registration on central server, it computes MAC (ID) and MAC (ID||PW), then it send to central server S over a secure channel.
Upon receiving the registration request from user U of cloud.
S compute A=MAC (ID) xor MAC (X||ID)
B= A xor MAC (ID||PW)
C=MAC (A)
D=MAC (ID||PW) xor MAC (X)
The central server S issues a card to user U by storing {B, C, D, and MAC (.)} into card memory. The smart card is delivered to user U through secure channel.
2. Login Phase
User U inserts the card to the card reader and keys in ID* and PW*. The card reader computes.

A*= B xor MAC (ID* || PW*)
C*= MAC (A*)
Then checks C and C* are equal or not. If not terminate to again login process. Otherwise yes, user U is a legitimate user of the card. Then the card reader generates a random no. R and compute.
E= A* xor R
Cid=MAC (ID||PW) xor R
F=MAC (A||D||R||Tu) where Tu is current time at login request.
And sends the login request message {F,E,Cid,Tu,MAC (ID)} to the central server.

3. Verification Phase
Upon receiving the login request message { F,E,Cid,Tu,MAC (ID)}. Central Server verifies the validity of time delay between Tu' and Tu where Tu' is the time travel of the message.
Tu'-Tu <= ∆T
If the time delays the verification process is accepted. Then central Server Computes

A*= MAC (ID) xor MAC (X|| MAC (ID))
R*=A* xor E
G=MAC (ID||PW)*=Cid xor R
D*=MAC (ID||PW)* xor MAC (X)
F*=MAC (A*||D*||R*||Tu)
And checks whether F and F* are equal or not.If they are not equal then rejects the login request. If true then central Server S computes
Fs=MAC (MAC (ID)||D||R||Ts)
Where Ts is the time when message to send and sends acknowledgement message (Fs,G,Ts).
Card reader compute

G*=MAC (ID||PW)
Fs*=MAC (MAC (ID)|| D||R||Ts)
If G and G*, Fs* and Fs are same, then card reader make session key and share both user U and central server S.
Sk=Mac (Mac (ID)||Ts||Tu||B)
Otherwise terminate to again login process.

4. Password Change Phase
After the login valid user (checks C*=C)
Then it ask for new password PWnew
Then compute
B*=A xor MAC (ID||PWnew)
D*=MAC (ID||PWnew) xor MAC (ID||PW) xor D
And change the value of B and D to B* and D*.

2. Related Work

In 2010 Yan Zhu, Huaixi Wang, Zexing Hu, Gail-Joon Ahn, Hongxin Hu, Stephen S. Yau [1] proposed a provable data possession to provide the integrity of data. it is a cooperative provable data possession scheme in hybrid clouds. It gives scalability of service and data migration, and cooperatively store and maintain the clients' data. It requires less overhead so that communication complexity can be minimized.

In 2009 Qian Wang, Cong Wang, Jin Li1, Kui Ren, and Wenjing Lou introduced a new scheme which gives remote data integrity and verifiability means dynamic data operations. The scheme firstly identifies the difficulties and potential security problems of direct extensions with fully dynamic data updates. It achieves efficient data dynamics and improves the Retrievability model by manip-ulating the classic Merkle Hash Tree (MHT) construction used for block tag authentication. It is highly efficient and secure technique.[2]

In 2012 Tekin Bicer, David Chiu and Gagan Agrawal [3] proposed a modeling-driven resource allocation framework. This technique supports time and cost sensitive execution and it is useful for data-intensive applications which executed in a hybrid cloud setting. It is capable of meeting execution deadlines within a 3.6% margin of error, cost constraints within a 1.2% margin of error and also minimizes the execution time of application.

In 2011 Haoming Liang, Wenbo Chen and Kefu Shi proposed an approach which analyses the programming and task scheduling model according to the present-used cloud computing system. It gives examples to explain the process of programming and its modifying directions, as well as the process within which services and resources exchange. It gives explanation of Cloud computing, how social network may increase the Qos through changing the service load will be discussed. [4]

In 2010 Ravi Sandhu, Raj Boppana and Ram Krishnan proposed a new approach to instrument the cloud with hooks and supporting protocols and to develop mechanisms to increase mission-driven performance, resilience and security policies into the computing and communication infrastructure. By this approach twin issues of availability and security in the cloud can be adequately addressed. [5]

In 2011 Guannan HU and Wenhao ZHU[5] introduced a dynamic user-integrated cloud computing architecture. This architecture integrates clients with storage capacity and computing competency to data center dynamically, it expands the scale of cloud computing data center. Collaboration of clients with the data center provides services to the other users.

In 2011 Xiang Li, Jing Liu ,Jun Han and Qian Zhang proposed. The article describes design of micro-learning platform architecture constructed through cloud computing technology, details the layered architecture design of micro-learning platform based cloud, aiming at depending on the powerful computing capacity and mass storage of cloud to better meet the practical learning requirements of life-long learners. [6]

In 2009 Xinwen Zhang, Joshua Schiffman, Simon Gibbs, Anugeetha Kunjithapatham, and Sangoh Jeong [7] proposed a solution for authentication and secure session management between weblets running device side and those on the cloud. It provides secure migration and authorizes cloud weblets to access sensitive user data via external web services. It gives application integration between private and public clouds in an enterprise environment. [8]

In 2010 Yan Zhu, Huaixi Wang, Zexing Hu, Gail-Joon Ahn, Hongxin Hu, Stephen S. Yau [9] proposed data possession scheme in hybrid clouds which supports scalability of service and data Migration. It gives the scenario of multiple cloud service providers to cooperatively store and maintain the clients' data. This scheme gives less overhead and reduces communication complexity.

In 2009 Qian Wang, Cong Wang, Jin Li1, Kui Ren, and Wenjing Lou introduced a protocol Which firstly identify the difficulties and potential security problems of direct extensions with fully dynamic data updates and secondly shows how to construct an elegant verification scheme for seamless integration. It manip-ulates the classic Merkle Hash Tree (MHT) construction for block tag authentication. [10]

In 2012 Arash Nourian and Muthucumaru Maheswaran introduced new image encoding scheme that enhances the privacy of the images and allows the clouds to perform certain forms of computations on the images. This encoding scheme uses a chaotic map to transform the image after it is masked with an arbitrarily chosen ambient image. [11]

In 2010 Jean Bacon1, David Evans1, David M. Eyers1, Matteo Migliavacca2, Peter Pietzuch2, and Brian Shand [12] proposed a approach for designing and deploying end-to end secure and distributed software for the security of data. It guarantees that—above a small trusted code base—data cannot be leaked by buggy or malicious software components. This is crucial for cloud infrastructures, in which the stored data and hosted services all have different owners whose interests are not aligned. It gives data tagging schemes and enforcement techniques that can help form the aforementioned trusted code base and cloud-hosted services that have end-to-end information flow control.

In 2008 Jia Yu, Rajkumar Buyya and Kotagiri Ramamohanarao introduced an approach for allocating suitable re-sources to workflow tasks so that the execution can be completed which can satisfy objective functions specified by users. It tries to improve existing workflow scheduling algorithms which developed and deployed by various Grid projects. [13]

In 2008 Jon Oberheide,Kaushik Veeraraghavan,Evan Cooke,Jason Flinn and Farnam Jahanian [14] proposes a new model which gives the concept of possibility to spend bandwidth resources to significantly reduce on-device CPU, memory, and power resources. It shows the in-cloud model enhances mobile security and reduces on-device software complexity and gives platform-specific behavioural analysis engines. Its benchmarks on

Nokia's N800 and N95 mobile devices show that its mobile agent consumes less CPU and memory while also consuming less power as compared to existing on-device antivirus software.

In 2012 Luís Mendonça and Henrique Santos presented the research and tests which define an effective set of traffic parameters capable of modeling both normal and abnormal activity of networks, focusing on botnet activity detection through anomalous and cooperative behavior. It also proposed detection framework prototype which tested using real traffic collected in the University of Minho campi edge. [15]

In 2012 Alex Kantchelian Justin Ma and Ling Huang [16] method for blog comment spam detection taking the assumption that spam is any kind of uninformative content. It gives a language to measure the "informativeness" of a set of blog comments and tokenization independent metric. It uses a parsimonious hand-labeling strategy can operate at an arbitrary high precision level, and it dominates precision and recall. This model gives the content complexity metric, the use of a noise-tolerant logistic regression and the evaluation methodology.

In 2011 Pengfei Sun Qingni Shen, Ying Chen Zhonghai and Wu Cong Zhang [17] proposed a new security load balancing architecture which is based on Multilateral Security (LBMS), when it reaches on peak-load it can migrate tenants' VMs automatically to the ideal security physical machine. This protocol is based on CloudSim, a Cloud computing simulation. This architecture makes an effort to avoid potential attacks when VMs migrate to physical machine due to load balancing.

In 2012 Pragya Jain and Anjali Sardana proposed a novel hybrid scheme that integrates anomaly and signature detection with honeypots. At first level it used Signature based detection for known worm attacks, that makes the system operate in real time. At the second level Any deviation from the normal behavior can be easily detected by anomaly detector and at the Last level is honeypots detects zero day attacks. It gives resource efficient advantage of honey farm because it deployes honeypots and both the detectors. The Controller redirects the traffic to the respective honeypots. [18]

3. Analysis

Cloud computing security plays a vital role on the public verifiability. This work studies the problem of ensuring the integrity of data storage in Cloud Computing. We consider the task of allowing a third party auditor (TPA), on behalf of the cloud client, to verify the integrity of the dynamic data stored in the cloud. The introduction of TPA eliminates the involvement of client through the auditing of whether his data stored in the cloud is indeed intact.

Public verifiability also allows clients to delegate the integrity verification tasks to TPA while they themselves can be unreliable or not be able to commit necessary computation resources performing continuous verifications.

4. Conclusion and Future Work

Cloud computing offers users the potential to reduce operating and capital expenses by leveraging the authorization benefits offered by large, managed infrastructures. The concept of cloud in the accessing of data from one node to another in the network requires security in the inter clouds so a concept of hybrid clouds has been introduced, although it is an efficient technique for the data access between different clouds but chances of different attacks in the cloud has also been increased. Here in this paper a brief survey of various cloud computing techniques and security authentication using smart cards has been given.

Major concern is how to construct verification protocols that can accommodate dynamic data files. We explored the problem of providing simultaneous public verifiability and data dynamics for remote data integrity check in Cloud Computing. Our construction is deliberately designed to meet these two important goals while efficiency being kept closely in mind.

References

[1] 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.

[2] 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.

[3] Tekin Bicer, David Chiu and Gagan Agrawal, “Time and Cost Sensitive Data-Intensive Computing on Hybrid Clouds”, 2012 IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing, PP. 636 – 643, May 2012.

[4] Haoming Liang, Wenbo Chen and Kefu Shi “Cloud Computing: Programming Model and Information Exchange Mechanism”, Proceedings of the 2011 International Conference on Innovative Computing and Cloud Computing (ICCC '11), PP. 10-12, 2011.

[5] Ravi Sandhu, Raj Boppana and Ram Krishnan “Towards a Discipline of Mission-Aware Cloud Computing”, Proceedings of the 2010 ACM workshop on Cloud computing security workshop(CCSW '10), PP.13-18, 2010.

[6] Guannan HU and Wenhao ZHU, “A Dynamic User-integrated Cloud Computing Architecture”, Proceedings of the 2011 International Conference on Innovative Computing and Cloud Computing (ICCC '11) , pp: 36-40, 2011.

[7] 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.

[8] 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.

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

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

[11] Arash Nourian and Muthucumaru Maheswaran ,“Towards Privacy Enhanced Limited Image Processing in the Clouds”, Proceedings of the 9th Middleware Doctoral Symposium of the 13th ACM/IFIP/USENIX International Middleware Conference (MIDDLEWARE '12), Article No. 5, 2012.

[12] Jean Bacon1, David Evans1, David M. Eyers1, Matteo Migliavacca2, Peter Pietzuch2, and Brian Shand3, “Enforcing End-to-End Application Security in the Cloud”, Proceedings of the ACM/IFIP/USENIX 11th International Conference Middleware (Middleware '10), pp. 293-312, 2010.

[13] 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.

[14] 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.

[15] Luís Mendonça and Henrique Santos, “Botnets: A Heuristic-Based Detection Framework”, Proceedings of the Fifth International Conference on Security of Information and Networks (SIN '12), pp. 33-40, 2012.

[16] Alex Kantchelian Justin Ma and Ling Huang “Robust Detection of Comment Spam Using Entropy Rate”, Proceedings of the 5th ACM workshop on Security and artificial intelligence (AISec '12), pp. 59-70, 2012.

[17] Pengfei Sun Qingni Shen, Ying Chen Zhonghai and Wu Cong Zhang, “POSTER: LBMS: Load Balancing based on Multilateral Security in Cloud”, Proceedings of the 18th ACM conference on Computer and communications security (CCS '11), pp. 861-864, 2011.

Amish Kumar Aman M.E. [Computer Sc & Engg.]
4.5 Yr. Expertise on software technology in various reputed organization in India.