An Analysis of Security Issues with Possible Solutions in Cloud Environments

Kumud Gupta, Anuradha Panjeta
Research Scholar Mtech, Lecturer Deptt.Computer Science And Engineering

Abstract - The study of various papers had enlightened me on the various prospects of privacy preservation in cloud environments. Cloud computing has attracted a lot of organizations for sharing data and resources over the cloud.A lot of approaches have been worked upon by various researchers across the globe. Cloud computing is a computing paradigm which enables flexible, on-demand of computing resources. These advantages, ironically, are the causes of security and privacy problems, which emerge because the data owned by different users are stored in some cloud server instead of under their own control. However,a lot of problems have also been encountered by the efficient researchers of the research community. The problems are related to a lot of threats like security,privacy,sharing data and identity threats. These threats can be highly vulnerable in case of authentic data sharing.So to prevent such threats a lot of techniques have been proposed. Trusted computing and privacy enforcememt via tamper resistance is one of the technique to allow the privacy secure distribution computation. Homomorphic encryption based secret sharing, combined with software re-encryption scheme to ensure security,it focuses on license management in cloud computing.Anonycontrol is also one such technique to provide privacy in cloud

Keywords – Homomorphic encryption,anonycontrol,tamper resistance.

1.INTRODUCTION

Cloud computing has proven to be great computing paradigm to share storage,computation and services among massive users transparently and is gathering a great momentum. Cloud computing uses many existing concepts, such as distributed, grid and utility computing. It focuses on the buzz word “ cloud” which means more abstract resource and services’ delivery. With the help of cloud computing any locally stored information such as email,word processing documents and spreadsheets couldbe stored remotely on cloud and any terminals, e.g., computer, laptop and PDA etc can then be used to access these information at anytime, anywhere. The “cloud” in cloud computing means the set of hardware, networks, storage, services, and interfaces .to deliver computing as a service. Cloud services uses delivery of software, infrastructure, and storage over the Internet based on demands of users, Figure 1.1 shows a cloud platform on the web. Following are the few advantages of having cloud hosted application:

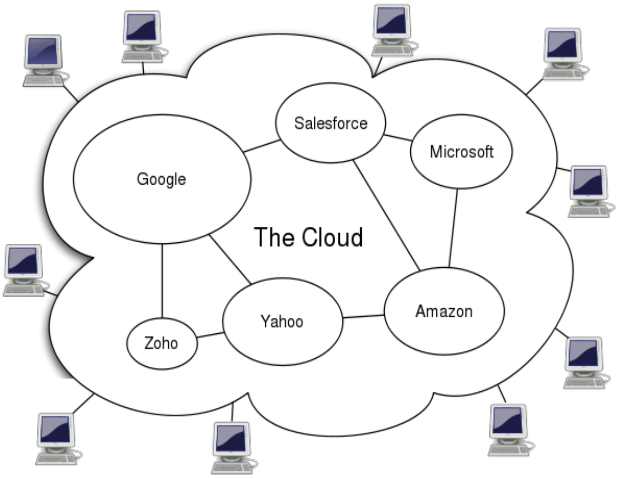

Figure 1: General architecture in cloud computing environment

It is the cost efficient method to maintain and use Cloud computing much cheaper and reduces the company’s expenditure. It provides ultimate storage according to various plans provided by the cloud provider. It is now easy to access information all across the globe using internet connection.

A basic example of cloud computing is Yahoo email, Gmail, or Hotmail etc. Sending emails is an easy task now with support of internet.. The server and email management software is all on the cloud and is totally managed by the cloud service provider Yahoo, Google etc.

1.2 Challenges in Cloud Systems

Cloud computing is in its evolving stage, so there are many problems prevalent in cloud computing including:

Data lineage, data provenance and inadvertent disclosure of sensitive information is possible

1.3 Essential Characteristics:

1.3.1 On Demand Self-service:

A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

1.3.2 Broad Network Access:

Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g. mobile phones, tablets, laptops, and workstations).

1.3.3 Resource pooling

The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. Examples of resources include storage, processing, memory, and network bandwidth[2].

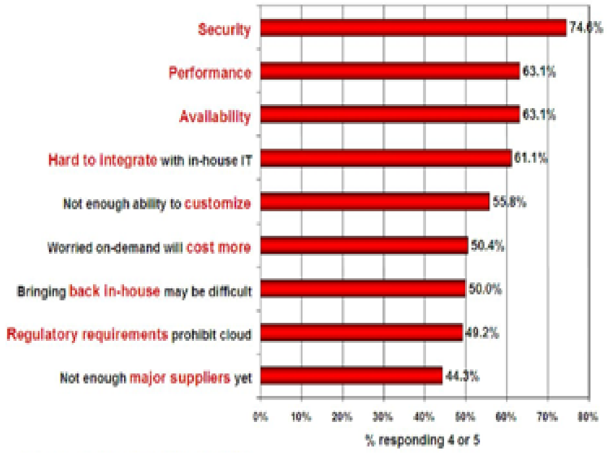

Figure 1.3: Most Prevalent challenges in cloud computing, IDC Survey

1.3.4 Rapid elasticity:

Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

2. LITERATURE REVIEW

There are a lot of privacy preserving approaches to contribute to privacy preserving in data mining. Secure management of Electronic Health Records (EHR) in distributed cloud computing environments is an important tool in cloud environments where data is provided through third party.EHR embedded with primitive attribute based cryptography helps persons to share their data effectively in health care systems.[2]

A secure cloud storage system supporting privacy-preserving public auditing can be used to securely introduce an effective third party auditor to check the integrity of outsourced data. Here a homomorphic non-linear authenticator and random masking is used to guarantee that the TPA would not have any knowledge about the data stored on the cloud server during the auditing process, this eliminates the burden of cloud user from the hectic and expensive auditing task, and removes the users fear of outsourced data to be leaked.[3]

The problem of privacy-preserving graph query can be easily solved in cloud computing (PPGQ). To reduce the times of checking subgraph isomorphism, the principle of "filtering-and verification" is utilised to remove as many negative data graphs as possible before verification.[4]

Secure outsourcing of linear programming (LP) computations can also be used.The LP computation outsourcing is decomposed into public LP solvers running on the cloud and private Lp parameters owned by the customer. The resulting flexibility allows to explore appropriate security efficiency trade off .

By formulating private data owned by the customer for LP problem as a set of matrices and vectors,to be able to develop a set of efficient privacy-preserving problem transformation techniques, that helps customers to transform original LP problem into some arbitrary one while protecting sensitive input/output information.

Oruta is also a new privacy preserving public auditing mechanism for data shared in an untrusted cloud. Oruta utilises ring signatures to construct homomorphic authenticators so that the third party auditor is able to verify the integrity of shared data for a group of users without retrieving the entire data . It can also be used to support batch auditing, which can audit multiple shared data simultaneously in a single auditing task.I t supports dynamic operations. The dynamic operation means an insert, delete or update operation on a single block in shared data. [6]

The use of DRM (DIGITAL RIGHTS MANAGEMENT) concept for cloud computing to show how license management for software in the cloud can be achieved in a privacy friendly manner.[5]

Cryptography or traditional cryptography lags a certain prospect of protection and hence to achieve that lag we introduce FHE (FULLY HOMORPHIC ENCRYPTION) to enure complete security of data over cloud environments.[1]

IBE OR IDENTITY BASED ENCRTPTION AND ABE OR ATTRIBUTE BASED ENCRYPTIONS can also be used to support privacy preservation for mining.[7]

3. CONCLUSION

The threats to privacy in cloud environments have been facing major challenges.To overcome the threats and instill an effective technique ,Oruta has been studied.In Oruta,the use of ring singnatures and homomorphic encryption has been utilised for public auditing,before the data is made available to the third party.Likewise,an approach known as DRM,also constitutes the homomorphic encryption and software reencryption of the data.Integrity threats and security threats are managed under the IBE approach.Trusted computing is also one of the major issues and is removed through FHE.taking into considerations such efficient approaches,the privacy has been preserved to a lot extent in cloud environments.

3.Table

AUTHOR /YEAR	APPROACH /TECHNIQUE	FINDINGS	REFERENCES
MARTEN VAN DJIK AND ARI JUELS,2010	FHE	Trusted computing i.e .privacy enforcement via tamper resistance.	[1]
Shivaramakrishnan Narayan, Martin Gagné and Reihaneh Safavi-Naini,2010	EHR	Patient centric health record management using ABE and data is preserved.	[2]
D. Srinivas,2011	TPA	Homomorphic non linear authenticator and random masking.	[3]
Ning Cao*†*, Zhenyu Yang*†* , Cong Wang*‡*, Kui Ren*‡* , and Wenjing Lou*†*,2011	PPGQ	Filtering and verification to prune negative graphs.	[4]
Ronald Petrlic and Christoph Sorge, 2012	DRM	Homomorphic encryption-based secret sharing scheme, combined with software re-encryption scheme to ensure security.	[5]
Boyang Wang, Baochun Li, *Member,*Hui Li,2012	ORUTA	Oruta the first privacy preserving public auditing mechanism for shared data in the cloud utilising ring signatures.	[6]
Taeho Jung*§*, Xiang-Yang Li*§*, Zhiguo Wan*†* and Meng Wan *‡,2013*	IBE	Attribute based privilege scheme known as Anonycontrol to preserve privacy in cloud storage.	[7]

REFERENCES

[1] Marten van Dijk, Ari Juels,” On the Impossibility of Cryptography Alone for Privacy Preserving Cloud Computing”,2010

[2] Shivaramakrishnan Narayan, Martin Gagné and Reihaneh Safavi-Naini,” Privacy Preserving EHR System Using Attribute-based Infrastructure”,2010

[3] D. Srinivas,” Privacy-Preserving Public Auditing In Cloud Storage Security”,2011.

[4] Ning Cao†, Zhenyu Yang† , Cong Wang‡, Kui Ren‡ , and Wenjing Lou†,” Privacy-Preserving Query over Encrypted Graph-Structured Data in Cloud Computing”,2011.

[5] Ronald Petrlic and Christoph Sorge,” Privacy-Preserving DRM for Cloud Computing”, 26th International Conference on Advanced Information Networking and Applications Workshops,2012.

[6] Boyang Wang, Baochun Li, Member,Hui Li,” Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud”,IEEE Transactions on Cloud Computing,Volume:2,Issue:1,Issue Date :March 2014,2012.

[7] Taeho Jung§, Xiang-Yang Li§, Zhiguo Wan† and Meng Wan ‡,” Privacy Preserving Cloud Data Access With Multi-Authorities”,2013.

AUTHOR'S PROFILE

KUMUD GUPTA has received her Bachelor of Engineering degree in COMPUTER SCIENCE and Engineering from kurukshetra university kurukshetra ,Haryana in the year 2013. At present she is pursuing M.Tech. with the specialization of Computer science and engineering from SSGI.

ANURADHA PANJETA has received her MTECH degree in computer science and engineering from SSGI,Haryana in the year 2012. At present she is working as an Associate Professor at SSGI.