IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 9, September 2017

Survey of Multi-Key Distribution System for mobile computing with Generalized Proxy Model

M. Sripriya M.Sc.[1], S. Jayabharathi M.Sc., MCA., M.Phil.[2],

M. Phil Full Time Scholar Vivekanandha College for Women, Tiruchengode[1]

Assistant Professor, Vivekanandha College for Women, Tiruchengode[2]

Abstract: Mobile cloud computing applications. To ensure a correctness of users' data in the mobile cloud, our study an effective and secure distributed model including a Self-Proxy Server (SPS) with self-created algorithm. The model resolves a communication Mobile cloud computing provides a novel ecommerce mode for organizations without any upfront investment. Since cloud computing uses distributed resources in open environment, it is important to provide secure keys to share the data for developing bottleneck due to re-encryption of a shared data in the cloud whenever users are revoked. It offers to reduce security risks and protect their resources because a distributed SPS dynamically interacts with Key Manager (KM) when the mobile users take on cloud services. This paper describe a survey of comprehensive mobile cloud design which provides an effective and secure mobile cloud computing services on mobile devices.

Keywords: Mobile Cloud Database, SPS, Key Management, Multi key Distribution, Self Proxy Server.

I. INTRODUCTION

Mobile computing is human –computer interaction next to which a computer is estimated in the direction of be ecstatic during normal usage, which allows for transmission of data, voice and video. Mobile computing networks and infrastructure networks as well as communication properties involves mobile communication, mobile hardware, and mobile software. Communication issues include ad hoc, protocols, data formats and concrete technologies. Hardware includes mobile devices or device components.

Mobile software deals with the personality and requirements of mobile applications. Portability: facilitate movement of device(s) within the mobile computing environment. Connectivity: Ability to continuously stay connected with minimal amount of lag/downtime, without being affected by movements of the connected node Social Interactivity: Maintaining the connectivity to collaborate with other users, at least within the same environment. Individuality: Adapting the technology to suit individual needs. Mobile Computing is perceptive that allows diffusion of data, power plus imprison through a computer or any other wireless enabled device without having to be connected to fixed physical link.

The mobile communication in this case, refers to the connections arrangement in place to guarantee that perfect and reliable communication go on. These would include devices such as protocols, services, bandwidth, and portals necessary to make possible and support the stated services. The data format is also defined at this stage. This ensures that there is no impact with other presented systems which offer the same service. Since the media is unguided / unbounded, the overlaying transportation is mostly radio wave-oriented. That is, the signals are carried over the air to intended devices that are capable of receiving and sending similar kinds of signals.

II. LITRATURE SURVEY

J. Broberg [1] describe a cloud computing is a new computational paradigm that offers an innovative business model for organizations to adopt IT without upfront investment. Despite the potential gains achieved from the cloud computing, the model security is still questionable which impacts the cloud model adoption This paper [1] introduces a detailed analysis of the cloud security problem. To investigate the problem from the cloud architecture perspective, the cloud offered characteristics perspective, the cloud stakeholders' perspective, and the cloud service delivery models perspective. Based on this analysis they derive a detailed specification of the cloud security problem and key features that should be covered by any proposed security solution.

Cloud computing provides the next generation of internet based, highly scalable distributed computing systems in which computational resources are offered 'as a service'. The most widely used definition of the cloud computing model

is introduced by NIST as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction.

An adaptive model-based approach is tackling the cloud security management problem. Models will help in the problem abstraction and the capturing of security requirements of different stakeholders at different levels of details. Adaptive-ness will help in delivering an integrated, dynamic and enforceable cloud security model. The feedback loop will measure the security status to help improving the current cloud security model and keeping cloud consumers aware with their assets' security status (applying the trust but verify concept).

T. Mather [2] describe a Cloud computing transforms the way information technology (IT) is consumed and managed, promising improved cost efficiencies, accelerated innovation, faster time-to-market, and the ability to scale applications on demand (Leighton, 2009). According to Gartner, while the hype grew exponentially during 2008 and continued since, it is clear that there is a major shift towards the cloud computing model and that the benefits may be substantial (Gartner Hype-Cycle, 2012 As per the definition provided by the National Institute for Standards and Technology (NIST) "cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction". It represents a paradigm shift in information technology many of us are likely to see in our lifetime.

Public cloud: Public clouds are provided by a designated service provider and may offer either a single tenant (dedicated) or multi-tenant (shared) operating environment with all the benefits and functionality of elasticity and the accountability/utility model of cloud. The physical infrastructure is generally owned by and managed by the designated service provider and located within the provider's data centers (off premises). All customers share he same infrastructure pool with limited configuration, security protections, and availability variances. One of the advantages of a public cloud is that they may be larger than an enterprise
Private cloud: Private clouds are provided by an organization or their designated services and offer a single-tenant (dedicated) operating environment with all the benefits and functionality of elasticity and accountability/utility model of cloud. The private clouds aim to address concerns on data security and offer greater control, which is typically lacking in a public cloud. There are two variants of private clouds:
(i) on-premise private clouds and (ii) externally hosted private clouds. The on-premise private clouds, also known as internal clouds are hosted within one's own data center. This model provides a more standardized process and protection, but is limited in aspects of size and scalability. IT departments would also need to incur the capital and operational costs for the physical resources.
This is best suited for applications which require complete control and configurability of the infrastructure and security. As the name implies, the externally hosted private clouds are hosted externally with a cloud provider in which the provider. Hybrid cloud: Hybrid clouds are a combination of public and private cloud offerings that allow for transitive information exchange and possibly application compatibility and portability across disparate cloud service offerings and providers utilizing standard or proprietary methodologies regardless of ownership or location. With a hybrid cloud, service providers can utilize third party cloud providers in a full or partial manner, thereby increasing the flexibility of computing. The hybrid cloud model is capable of providing on-demand, externally provisioned scale. The ability to augment a private cloud with the resources of a public cloud can be used to manage any unexpected surges in workload. Corporate partnerships and offshore outsourcing involve similar trust and regulatory issues. Similarly, open source software enables IT department to quickly build and deploy applications, but at the cost of control and governance. Similarly, virtual machine attacks and web service vulnerabilities existed long before cloud computing became fashionable. Indeed, this very overlap is reason for optimism; many of these cloud computing roadblocks have long been studied and the foundations for solutions exist

H.-L. Truong [3] describe a Cloud computing has elevated IT to newer limits by offering the market environment data storage and capacity with flexible scalable computing processing power to match elastic demand and supply, whilst reducing capital expenditure.
However the opportunity cost of the successful implementation of Cloud computing is to effectively manage the security in the cloud applications. Security consciousness and concerns arise as soon as one begins to run applications beyond the designated firewall and move closer towards the public domain. The purpose of the paper[8] is to provide an overall security perspective of Cloud computing with the aim to highlight the security concerns that should be properly addressed and managed to realize the full potential of Cloud computing. Gartner's list on cloud security issues, as well the findings from the International Data Corporation enterprise panel survey based on cloud threats, will be discussed in this paper.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 9, September 2017

The success of modern day technologies highly depends on its effectiveness of the world's norms, its ease of use by end users and most importantly its degree of information security and control. Cloud computing is a new and emerging information technology that changes the way IT architectural solutions are put forward by means of moving towards the theme of virtualization: of data storage, of local networks (infrastructure) as well as software.

It is the easiest solution to test potential proof of concepts without investing too much capital. Cloud computing can deliver a vast array of IT capabilities in real time using many different types of resources such as hardware, software, By following [11] guiding principles discussed in this paper, a great deal of insecurities may be easily expelled, saving business owners' valuable time and investment. Cloud computing has the potential to become a frontrunner in promoting a secure, virtual and economically viable IT solution and future work and progress lies in standardizing Cloud computing security protocols.

E. Deelman [4] describe a Cloud computing has been envisioned as the next-generation architecture of IT activity. In difference to established solution, wherever the IT services are under appropriate physical, logical and personnel controls, cloud computing moves the appliance software and databases to the large data centers, wherever the management of the data and services may not be fully reliable. This unique attribute, however, poses many new security challenges which have not been well understood.

Within a cloud computing environment all such commands may not be received and executed by all of the cloud servers due to unreliable network communications. To solve this problem they are proposing time-based re-encryption scheme. In this method automatic re-encryption of data will takes place based on the internal clock value present at the cloud server. To execute this automatic re-encryption they will make use of encryption technique called Attribute Based Encryption (ABE) with DES (Data Encryption Standard). ABE provides fine –grain access control and easier user revoking system and DES will provide Encryption technique.

An alternative solution is to apply the proxy re-encryption (PRE) technique. This approach [13] takes advantage of the abundant resources in a cloud by delegating the cloud to re-encrypt data. This approach is also called command driven reencryption scheme, wherever cloud servers execute re encryption while receiving commands from the data owner. However, command-driven re-encryption schemes do not consider the underlying system architecture of the cloud environment.

A cloud is basically a large scale distributed system where a data owner's data is replicated over multiple servers for high availability. The same as a distributed system, the cloud will understand failures common to such systems, for example server crashes and network outages. Accordingly, re-encryption commands sent by the data owner may not propagate to all of the servers in a timely fashion, hence creating security risks.

The security necessities of this scheme are as follows:

- Access control correctness. This requires that a data user with invalid keys cannot decrypt the file.
- Data consistency. This requires that all data users who request file F, should obtain the similar content in the similar time slice.
- Data confidentiality. The file content can only be known to data users with valid keys. The CSP is not considered a valid data user.
- Efficiency. The cloud servers should not re-encrypt any file unnecessarily. This means that a file has not been requested by any data user should not be re-encrypted.

In this method considers two types of adversaries:- The first type of adversary is the CSP. The CSP adversary is considered honest-but-curious. This means that the CSP will always correctly execute a given protocol, but may try to gain some additional information about the stored data. The second type of adversary is malicious data users. The data user adversary will try to learn the file content that he is not authorized to access. This adversary is assumed to possess invalid keys (either with incorrect attributes or time). They also assume the data user adversary can query any server in the cloud. Note that both an honest-but-curious CSP and malicious data users can exist together. In this paper[12] propose that by using Reliable Re-encryption Scheme(R3 scheme), remove the condition of unreliability in cloud by using access control and access time with that a new addition of DES algorithm of cryptography that is using hybrid cryptography.

S. Mehrotra [5] consider the data that exhibits a more complex structure such as labeled graph data (e.g., web graphs). Show how to encrypt this type of data in order to perform focused subgraph queries, which are used in several web search algorithms. Our construction is based on our labeled data and basic graph encryption schemes and provides insight into how several simpler algorithms can be combined to generate an efficient scheme for more complex queries.

The most common use of encryption is to provide confidentiality by hiding all useful information about the plaintext. Encryption, however, often renders consider the problem of encrypting structured data (e.g., a web graph or a social network) in such a way that it can be efficiently and privately queried. For this purpose, [15] introduce the notion of structured encryption which generalizes previous work on symmetric searchable encryption (SSE) to the setting of arbitrarily-structured data. Present the model for structured encryption, the formal security definition and several efficient constructions.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 9, September 2017

The present schemes for performing queries are two simple types of structured data, specifically lookup queries on matrix-structured data, and search queries on labeled data. To show how these can be used to construct efficient schemes for encrypting graph data while allowing for efficient neighbor and adjacency queries. To address this problem they introduce the notion of structured encryption. A structured encryption scheme encrypts structured data in such a way that it can be queried through the use of a query-specific token that can only be generated with knowledge of the secret key. In addition, the query process reveals no useful information about either the query or the data. An important consideration in this context is the efficiency of the query operation on the server side. In fact, in the context of cloud storage, where one often works with massive datasets, even linear time operations can be infeasible.

Several interesting future directions are suggested by this work. The most immediate is whether efficient and non-interactive structured encryption can be achieved while leaking less than the query and intersection pattern. The construction of efficient dynamic structured encryption schemes (i.e., that allow for updates to the encrypted data) is another direction left open by this work. Of course, the construction of schemes that handle other types of structured data and more complex queries on the data types considered here would also be interesting.

III. METHODOLOGY

A cloud is basically a large scale distributed system where a data owner's data is replicated over multiple servers for high availability. However, there are still a number of challenges because they are preventing the mobile users to take on cloud services. A model for key distribution based on data re encryption is applied to a cloud computing system to address the demands of a mobile device environment, including limitations on mobile data usage, storage capacity, processing power, and battery etc. When an encrypted data is stored and decryption key is allocated to user, they can access data from cloud.

While a user is revoked and he has decryption key he can access data still, thus to overcome from this problem here is a need of immediate re encryption of data by data owner. When re-encryption is done the newly generated, decryption keys are distributed to authorized users. This resolution will lead to performance bottleneck, particularly when there are many user revocations. A solution is to apply a distributed self proxy re encryption technique, so this scheme proposes Self Proxy Server (SPS). It coordinates and chooses keys by Key Manager (KM) whenever group membership changes.

The distributed SPS provides not only encryption and decryption keys but also immediate re encryption keys for shared data. After communicating with KM, it automatically receives necessary keys from KM by self created algorithm. A distributed SPS scheme is one solution where multiple proxy are automatically deployed in several clouds. Mobile Cloud Provider (MCP) has significant resources and expertise in building and managing distributed cloud storage servers and computational services to data, owns and operates live cloud computing systems. Data Owner (DO) has data to be stored in the cloud and rely on the cloud for data computation, consists of both individual consumers and organizations.The Key Manager (KM) generates and manages all data encryption, decryption and re encryption keys. It is provided live cloud computing by MCP and governed by Trusted Third Party (TTP). The data owner of MCP shares data to many other cloud users. The data is encrypted with a key from KM and then stored in the cloud along with Access Control List (ACL) indicating the user group. Upon access request from a user, the cloud communicates with SPS, based on ACL and SPS requests a self created algorithm. According to the self created algorithm, SPS uses re-encryption algorithm to transfer the encrypted format that can be decrypted by the user's private key. The user can download the encrypted data from the cloud and use the decryption key.

Data owner: Data owner an entity who stores the data inside cloud storage and wishes to employ the cloud application services to process the data. A data owner must register with cloud storage provider and must be logged-in in order to upload the data or access the data or authorize the data.

Algorithm:
Input : Original Data File
Output: Cipher text file
Steps:

Step1: Generate Random Symmetric key (KE) under the access tree t'
Step2: Encrypt owner data file using modified CP-ABE with symmetric key (KE)
Step3: Archive / Encapsulate the cipher text of key (KE) and cipher text of data
Step4: Store the encapsulated/archived cipher text data in the CSP

Application Service Provider: An entity to be authorized to access cloud storage data. It is application software resides in vendor's system or cloud and can be accessed by users through a web browser or a special purpose client software. For example, PDF Merge is an online tool which can be used to merge several PDF files into one PDF

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 9, September 2017

file. With proper authorization, PDF Merge fetches the source PDF files from cloud storage. As a result, uploading files from data owner's local device is avoided.

Algorithm: Decrypt (CT, SK, x)
Input: Decrypt Node, Cipher text (CT), Secret Key (SK)
Output: Decrypted data (plain data)
Steps:

Step1: x is a leaf node of access tree and is the attribute attached to x
Step2: decrypt (CT, SK, x)
Step3: $e(D_i,C_x)/e(D'_i, C'_x) = e(g_1^{ra} H(i)^i, g_2^{px(0)}/e(H(i)^i, g_2^{px(0)})$
Step4: stores the result fz= $(f_{z0}, f_{z1,\ldots} f_{z\,n-1})$, $f_{zi}=e(g_1,g_2)^{raPzi(0)}$

Cloud Storage Provider: an entity which supplies storage as a service to its clients and also provides access application programming interfaces to ASP when ASP holds a valid access token. Drop box and Just Cloud mentioned previously are examples of such entity.

Algorithm:
Input: security parameter k
Output: public key
Steps:

Step1: Choose bilinear map (e: $G_1 * G_2 \rightarrow G_T$ of prime order q
Step2: Generate g_1, g2
Step3: generate random exponent ß
Step4: publish the public key CPK= (G_1, G2, g1, g2, $h=g_1^{ß}$, $f=g_2^{1/ß}$)
Step5: keep the secret key CSK (CPK= (ß)

The importance of fuzzy search has received attention in the context of plaintext searching in information retrieval community. They addressed this problem in the traditional information-access paradigm by allowing user to search without using try and approach for finding relevant information based on approximate string matching. The approximate string matching algorithms among them can be classified into two categories: on-line and off-line. The on-line techniques, performing search without an index, are unacceptable for their low search efficiency, while the off-line approach, utilizing indexing techniques, makes it dramatically faster.
The proposed algorithm analyze from the perspectives of internal and external adversaries. For internal adversaries, all entities in the system are considered to be trusted, in the sense that they can exploit threats to subvert authorization control and data security, but still honestly follow the protocol. External adversaries may not run the protocol but try to launch general attacks to violate data security.
In order to address the aforementioned issues, propose fuzzy authorization (FA) for cloud storage which is a secure file sharing scheme with high scalability and flexibility by leveraging and modifying cipher text-policy attribute based encryption (CP-ABE) and OAuth. The term fuzzy means that this authorization scheme possesses attribute-discrepancy tolerance. In other words, a secret key associated with one attribute set can be applied to another attribute set through proper adjustment as long as the two attribute sets share certain amount of overlap.

IV. CONCLUSION

In this survey study is describing the problem of secure authentication for storage in mobile cloud. In this paper, survey of fuzzy model which carries out a flexible file-sharing scheme between an owner who stores the data in one cloud party and applications which are registered within another cloud party. The survey security analysis shows that our Fuzzy Authorized model provides a thorough security of outsourced data, including confidentiality, integrity and secure access control. Fuzzy Authorized approach reduces the storage consumption compared to other similar possible authorization schemes. It also asserts that our scheme could efficiently achieve distance tolerance and realize fuzzy authorization in practice research study. This work mainly addresses the reading authorization issue on mobile cloud storage and it results to enable the TPA to perform audits for multiple users simultaneously and efficiently.

ACKNOWLEDGMENT

My heartfelt gratitude goes to my beloved guide **Mrs. S. Jayabharathi** Assistant Professor, Department of Computer Science, Vivekanandha College for Women, Tiruchengode, India for dedication and patience in assigning me her valuable advice and efforts during the course of my studies.

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 9, September 2017

REFERENCES

[1] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, ―Cloud computing and emerging it platforms: Vision, hype, and reality for delivering computing as the 5th utility,Future Generation Comput. Syst., vol. 25, no. 6, pp. 599–616, 2009.
[2] T. Mather, S. Kumaraswamy, and S. Latif, Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance. Sebastopol, CA, USA: O‘ReillyMedia, Inc., 2009.
[3] H.-L. Truong and S. Dustdar, ―Composable cost estimation and monitoring for computational applications in cloud computing environments, Procedia Comput. Sci., vol. 1, no. 1, pp. 2175–2184, 2010.
[4] E. Deelman, G. Singh, M. Livny, B. Berriman, and J. Good, ―The cost of doing science on the cloud: The montage example, in Proc. ACM/IEEE Conf. Supercomputing, 2008, pp. 1–12.
[5] H. Hacig€ um€ u¸ s, B. Iyer, and S. Mehrotra, ―Providing database as a service,‖ in Proc. 18th IEEE Int. Conf. Data Eng.,Feb.2002, pp. 29–38.
[6] G.Wang, Q. Liu, and J. Wu, ―Hierarchical attribute-based encryption for fine-grained access control in cloud storage services, in Proc. 17th ACMConf. Comput. Commun. Security, 2010, pp. 735–737.
[7] Google. (2014, Mar.). Google Cloud Platform Storage with server side encryption [Online]. blogspot.it /2013/08 /google-cloud-storage-now-provides.html.
[8] H.Hacig, u¸ s, B. Iyer, C. Li, and S.Mehrotra, ―Executing SQL over encrypted data in the database-service-provider model, Proc. ACMSIGMOD Int‘lConf. Manage. Data, Jun. 2002,pp. 216–227.
[9] L. Ferretti, M. Colajanni, and M. Marchetti, ―Distributed, concur- rent, and independent access to encrypted cloud databases,IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 2, pp. 437–446, Feb. 2014.
[10] A. N.Khana, M. L.M. Kiaha, S.U. Khanb and S. A. Madanic, “Towards Secure Mobile Cloud Computing: A Survey”, Future Generation Computer Systems, vol.29, Issues 5, July 2013.
[11] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, M. Zaharia, Above the clouds: a Berkeley view of cloud computing, Technical Report UCB/EECS-2009-28, EECS Department, University of California, Berkeley, Feb. 2009.
[12] R. Ranjan, A. Harwood, R. Buyya, Grid federation: an economy based distributed resource management system for large-scale resource coupling, Technical Report GRIDS-TR-2004-10, Grid Computing and Distributed Systems Laboratory, University of Melbourne, Australia, 2004.
[13] R. Buyya, R. Ranjan, Federated resource management in grid and cloud computing systems, Future Generation omputer Systems 26 (8) (2006) 1189–1191.
[14] M. Al Morsy, J. Grundy and I. Muller, “An Analysis of The Cloud Computing Security Problem”, In Proceedings of APSEC 2010 Cloud Workshop, Sydney, Australia, November 2010.
[15] Peter Mell, and Tim Grance, "The NIST Definition of Cloud Computing," 2009, http://www. wheresmyserver. co.nz /storage/media/faq-files/clouddef-v15.pdf, Accessed April 2010.
[16] Frank Gens, Robert P Mahowald and Richard L Villars. (2009, IDC Cloud Computing 2010.