ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 12, December 2017

A Survey on Authentication Techniques for Single User in Cloud Computing Using Secret Sharing

Nehal Markandeya[1], Rachana Patil [2]

P.G. Student, Department of Computer Engineering,Pimpri Chinchwad College of Engineering, Pune, Maharashtra, India[1]

Lecturer , Department of Computer Engineering,Pimpri Chinchwad Polytechnic, Pune, Maharashtra, India[2]

ABSTRACT: Cloud computing is a cost-effective, scalable and flexible model. It provides network services to a range of users including individual and business over the Internet. It has brought the revolution in the era of traditional method of storing and sharing of resources. It provides a variety of benefits to its users such as effective and efficient use of dynamically allocated shared resources, economics of scale, availability of resources etc. A new concept, Cloud computing, uses low-power hosts to achieve high quality service. However, the authentication is one of the important problems in Cloud computing environment.

Security and privacy are major challenges in cloud computing. Various malicious activities from illegal users such as data misuse, strict access control and limited checking may result into harmful or illegal access of critical and private data of these cloud users. In this work, brief view of user authentication techniques in cloud computing environment is stated. Authentication and authorization for data access on cloud is more than a necessity.Using Shamir's secret sharing to secure authentication on cloud for single user is most efficient way.

KEYWORDS*:* Cloud computing, Authentication, Authorization,Secret sharing.

I. INTRODUCTION

Cloud computing, also on-demand computing, is a kind of Internet-based computing that provides shared processing resources and data to computers and other devices on demand. It is a model for enabling ubiquitous, on-demand access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services), which can be rapidly provisioned and released with minimal management effort. Cloud computing and storage solutions provide users and enterprises with various capabilities to store and process their data in third-party data centers. It relies on sharing of resources to achieve coherence and economy of scale, similar to a utility) over a network.

Advocates claim that cloud computing allows companies to avoid upfront infrastructure costs, and focus on projects that differentiate their businesses instead of on infrastructure. Proponents also claim that cloud computing allows enterprises to get their applications up and running faster, with improved manageability and less maintenance, and enables IT to more rapidly adjust resources to meet fluctuating and unpredictable business demand. Cloud providers typically use a "pay as you go" model. This can lead to unexpectedly high charges if administrators do not adapt to the cloud pricing model.

The present availability of high-capacity networks, low-cost computers and storage devices as well as the widespread adoption of hardware virtualization, service-oriented architecture, and autonomic and utility computing have led to a growth in cloud computing. Companies can scale up as computing needs increase and then scale down again as demands decrease.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

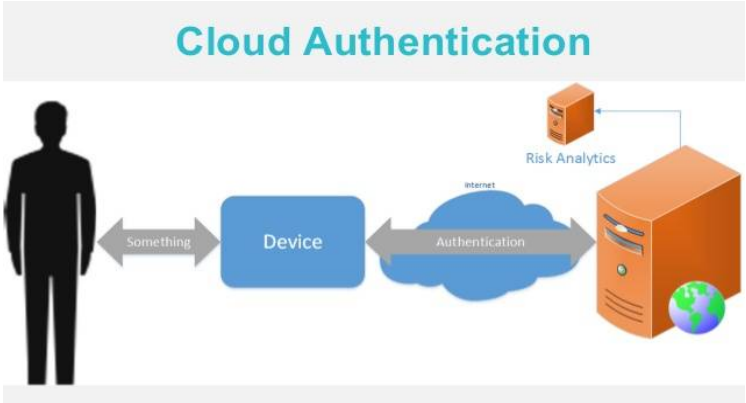
Visit: www.ijirset.com

Vol. 6, Issue 12, December 2017

Cloud computing has become a highly demanded service or utility due to the advantages of high computing power, cheap cost of services, high performance, scalability, accessibility as well as availability. Some cloud vendors are experiencing growth rates of 50% per year, but being still in a stage of infancy, it has pitfalls that need to be addressed to make cloud computing services more reliable and user friendly.

A cloud user stores their sensitive data on cloud thus it is the responsibility of cloud service providers to establish secure communication mechanism. To provide secure storage for storing data and secure channels for sending and receiving data cloud is most preferable way.Various malicious activities such as data misuse from illegal users may harm the cloud.Hence it requires more secure user authentication techniques in cloud computing environment.

The goal of this paper is to focus on most secure single user authentication method for cloud computing. In this paper, some useful authentication techniques are used to secure cloud. This paper also gives the overview of comparative study of different authentication techniques.



The rest of the paper is organized into the following sections: Section 1 gives an introduction about the cloud and security in cloud computing. Section 2 describes a brief literature review on the various authentication methods to protect integrity of user and to protect user's data. Sections 3 describe various authentication attacks and secure authentication techniques to protect data on cloud. Section 4 includes the comparative study of various popular authentication methods. Finally, Section 5 concludes this paper**.**

II. LITERATURE REVIEW

In the paper [1] Dr.Santosh Lomte, Shraddha Dudhani proposed authentication model using Kerberos technique and threshold cryptography.Now a days the cloud computing is emerging and versatile technology. For storage IT requires many of hardware, software and network infrastructures. Cloud computing solve this problem in cost effective manner.On other side all data is virtual and cloud is as open services and they are using public network for their application and services, which in turn has question on security issues like authentication data loss.

In the paper [2], Akanksha Upadhyaya, Monika Bansal proposed that Cloud computing is a cost-effective, scalable model of providing network services to a range of users including individual and business over the Internet. Authentication and authorization for data access on cloud is more than a necessity.They attempts to overcome these security challenges. The proposed methodology provides more control of owner on the data stored on cloud by restricting the access to specific user for specific file with limited privileges and for limited time period on the basis of secret key using symmetric as well as asymmetric mechanism. The integrity and confidentiality of data is ensured doubly by not only encrypting the secret key but also to the access permission and limited file information.

In the paper [3], Reshmi G.,Rakshmy C. S. proposed novel classification system for existing authentication methods in MCC(mobile cloud computing). Further, the pros and cons of the various methods are discussed and present a comparative analysis and recommends future research in improving the surveyed implicit authentication by establishing cryptographic security of stored usage context and actions.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 12, December 2017

In the paper [4],Ali A.Yassin, Abdullah A. Hussain, Keyan Abdul-Aziz Mutlaqproposed scheme which focuses on two-factor authentication that used image partial encryption to overcome above aforementioned issues and drawbacks of authentication schemes. Additionally, we use a fast partial image encryption scheme using Canny's edge detection with symmetric encryption is done as a second factor. In this scheme, the edge pixels of image are encrypted using the stream cipher as it holds most of the image's data and then applied this way to authenticate valid users.
In the paper [5],B.Sumitra C.R. Pethuru,M.Misbahuddin focuses on identifying the various authentication attacks in cloud environment. An attempt has been made to understand the root cause of the authentication attacks and propose possible mitigation measures in a cloud environment.

In the paper [6], Kajal Chachapara, Sunny Bhadlawala proposed that framework allow generating a key for particular users with particular permissions. Cloud user can generate keys for different users with different permissions to access their files. This framework uses cryptography algorithms like AES and RSA. AES is most secure algorithm in cryptography. Once key is generated user (user who have generated a key for their own files) can provide that key to decided user (user for whom key is generated). So when decided user will try to access files on cloud with that key, permission decided by owner will be given to that user. This is partial access to user and more secure then providing password to user. Cloud service providers can also add concept of defining files also like cloud user can generate key for particular file, particular user and particular permission. Those keys then can be provided to different users.

III. AUTHENTICATION ATTACKS AND SECURE AUTHENTICATION TECHNIQUE

Cost and ease of use are the main benefits of cloud computing, trust and security are the two top concerns of users of cloud services. The providers of this fast growing technology need to address many issues related to virtualization distributed computing, application security, identity management, access control and authentication. However, strong user authentication that restricts illegal access to the service providing servers is the paramount requirement for securing cloud environment. In this regard, this section focuses on identifying the various authentication attacks in cloud environment. An attempt has been made to understand the root cause of the authentication attacks and propose possible mitigation measures in a cloud environment[5].
Following are some Authentication attacks-
1] Eavesdropping:Act of listening communication between two authenticated users. Solution for this attackis to use secure connection https
2]Cookie poisoning: Identity related credential stored in cookie of authenticated user is modified by attacker to gain access to resources. Solution for this attack is to use message authentication code and digital signature
3]Shoulder surfing attack:Observing entry of sensitive data via keyboard or cell phone.Solution for this attack is to use two factor authentications.
4] Customer fraud attack:Client compromises its authenticated token for personal advantage or defames organization. Solution for this attack is that verifier must be able to prove that authentication failure was victims own fault.
5] Session hijacking:Session id issued to authenticated user is not protected. Solution for this attack is to encrypt communication channel.
Shamir's Secret Sharing:

Secret sharing is the technique of distribution of secrets among the participants or group members within a group, each of the participants holds only a share of the secret
and individual shares are of no use in order to reconstruct the original secret. The original secret can be reconstructed only when a definite number of shares are combined together and individual shares does not indicate the original secret.

Shamir's Secret Sharing is an algorithm in cryptography created by Adi Shamir. It is a form of secret sharing, where a secret is divided into parts, giving each participant its own unique part, where some of the parts or all of them are needed in order to reconstruct the secret .Counting on all participants to combine the secret might be impractical, and therefore sometimes the threshold scheme is used where any k of the parts are sufficient to reconstruct the original secret.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 12, December 2017

IV. COMPARATIVE STUDY OF AITHENTICATION METHODS

Sr. No	References / parameter	[1]Secure Key for Authentication and Secret Sharing in Cloud Computing	[2]Deployment of Secure Sharing: Authenticity and Authorization using Cryptography in Cloud Environment	[6]Secure sharing with cryptography in cloud computing
1	Authentication method	Secret sharing	cryptography based	cryptography based
2	Algorithm	Kerberos, Shamir algorithm	RSA	RSA
3	Technique used	Shamir's scheme uses lag ranges of polynomial	In RSA Key exchange method is used.	In RSA key exchange method is used.
4	Time complexity	O(n)	O(Log(n))	O(Log(n))
5	Session key agreement	Not required	Yes	Yes
6	Replay attack	No	Yes	Yes
7	Impersonating attack	No	Yes	Yes
8	User privacy	Yes	Yes	Yes
9	User anonymity	Yes	No	No
10	Identity management	Yes	Yes	Yes

V. CONCLUSION

This paper discusses comparative study of different authentication methods.Password,cryptography algorithms like RSA,AES and shamir's secret sharing are used to secure authentication process. In this paper, the comparative analysis of different authentication techniques concludes that shamir's secret sharing provides more security than otherauthentication techniques for cloud computing.

REFERENCES

[1] Dr.Santosh Lomte, Shraddha Dudhani, "Secure Key for Authentication and Secret Sharing in Cloud Computing"June 2015 International Journal of Advanced Research in Computer Science and Software Engineering.
[2] Akanksha Upadhyaya Monika Bansal, "Deployment of Secure Sharing: Authenticity and Authorization using Cryptography in Cloud Environment"2015 International Conference on Advances in Computer Engineering and Applications (ICACEA).
[3] Reshmi G., Rakshmy C. S, "A Survey of Authentication Methods in Mobile Cloud Computing" 10th International Conference for Internet Technology and secured Transactions (ICITST-2015) ..
[4] Ali A.Yassin*, Abdullah A. Hussain, Keyan Abdul-Aziz Mutlaq, "Cloud Authentication Based on Encryption of Digital Image Using Edge Detection" 2015 International symposium artificial intelligence and signal processing
[5] B.Sumitra, C.R. Pethuru, M.Misbahuddin, "A Survey of Cloud Authentication Attacks and Solution Approaches" 2014 International Journal of Innovative Research in Computer and Communication Engineering
[6] K. Chachapara and S. Bhadlawala, "Secure sharing with cryptography in cloud computing" proceeding of International Conference on engineering, 2013.