ISSN (Online): 2456-0448
International Journal Of Innovative Research In Management, Engineering And Technology
Vol. 2, Issue 7, July 2017

Analysis of Security Issues, Authentication, Authorization and its Solutions in Cloud

[1] Hendry Leo Kanickam, [2]Dr.L.Jayasimman
[1] Research Scholar in Computer Science, Srimad Andavan Arts & Science College, Trichy, India.
[2] Asst. Professor in Computer Science Srimad Andavan Arts & Science College, Trichy, India.

Abstract: ***Cloud computing is an expensive model for the on-demand network. Cloud Computing (CC) refers to the delivery of computing resources across the Internet, applications & services by which it can run on a spread across the network. This Network used for hosted services and virtualized resources delivered over the internetworking. Cloud Computing has three main categories (a) Virtualization– The network has no limit on resources, they are virtual. (b) Abstraction–The full details of software, which run on the physical system (c) Resource sharing - This facility is used for pay per what they used. There are three categories of Cloud Computing: (a) Infrastructure-as-a-Service (IaaS), (b) Platform-as-a-Service (PaaS) and (c) Software-as-a-Service (SaaS). The data stored on Cloud computing are safe and secure then only users will believe in this environment. Access Controls for a particular file and directory, Flex list Models, SLAs, etc. But still, there are few disadvantages in security. While user admittance data from Cloud Computing Authorization and Authentication are most important. In this paper the cloud issues are analyzed for providing a novel solution and deals with the authentication and authorization on Cloud Computing.***

Keywords- ***Cloud Computing, Cloud Security, Authentication, Authorization.***

I. INTRODUCTION

Cloud computing refers to the delivery of computing resources across the Internet. Instead of keeping data the hard drive or updating applications for our needs, the cloud provides the service over the Internet, at one place to another location, to store information or use its applications. By doing so, it will give rise to certain privacy implications. “Cloud services” allow public and industry people to use software and hardware that are managed by third parties at remote locations. Examples of cloud services include on-line file storage, mobile, social networking sites and on-line business applications. The cloud computing model allows access to information and computer resources from anywhere over the network. Cloud computing provides a service on shared team of resources, data storage space, networks, machine processing power and user applications. In our study, different types of authors are focused security views on the data communication and its related issues, many authentication technique and authorization. The cloud environment, the providers were also had risks as that of users.

II. BACKGROUND WORK (REVIEW OF LITERATURE

This paper proposed various security techniques for data protection(Kire Jakimoski, (2016), This paper explained secure authorization mehonism for cloud computing(Taranpreet Bhatti, Ashish James, Siddhi Narvekar,”(2016), a cloud computing surroundings, more entities are involved. The cloud has different types such as private, public, hybrid may be different kinds of issues when compare all types of cloud private cloud has less security needed , public cloud needs more security for data level and network level(R.Balasubramanian & M.Aramudhan, 2012). Cloud computing faces just as more security threats that are found in the existing computing platforms, networks, intranets, internet in enterprises. These threats, risk vulnerabilities come in various forms (Pradeep Kumar Tiwari, Dr. Bharat Mishra ,2012). this paper analyses current situation of M – learning, then the M –learning support for mobile cloud computing(V.Sujatha Bai, S.Hendry Leo Kanickam, N.Vijayaraj, 2012),Kerberos is the authentication technique utilized to authenticate the clients to the server in Client-Server architecture. Cloud Computing can also be viewed as distributed Client-Server architecture, where Cloud Provider is a Server and Cloud User is a Client, which communicates by the intermediates, named as Cloud negotiator. It has two main components- Ticket Granting Server and Authentication Server (Shabnam Sharma, Usha Mittal 2013). According to the survey through previous papers, Data security is considered as an important research topic in cloud computing. The major issues related to data security include integrity, availability, confidentiality, transparency of data (Jasleen Kaur, Anupma Sehrawat, 2014). The security for Cloud Computing is emerging area for research work, and this paper discusses various types of authentication methods and multi-factor user authentication.(Deepa Panse, P. Haritha ,2014). Regarding security,

various levels in data, network, virtual machine, etc. were discussed. It has various issues handled by some methodologies adopted (Aarti Singh, Manisha Malhotra, 2015). Currently, security in information technology is treated as a key constraint element to address the increased number of Hackers or attackers who access data using the new technologies. Among them, cloud computing technology is used by many companies. Analysis of authentication and authorization technique discussed by way of authenticated user can enter the system, and authorized party can access the data like read or write the information. Access control is a very important security technique that is used to regulate who can view and use resources in a computing environment. Access control plays an important defense for data privacy (Nilesh Mahajan, Devyani Patil, 2016), This paper explained cloud computing has more number of risk in provider level security compare than user level security (S.Hendry Leo Kanickam ,L.Jayasimman, 2016), This model mainly describes the overall structure of the cloud storage, it is a data outsourcing storage services in recent years and developed cloud computing concept using homomorphic encryption proposal.(S.Hendry Leo Kanickam ,2016).

III. CLOUD SECURITY ISSUES AND CHALLENGES

Cloud computing has many challenges always been there. Industries are increasingly responsive of the big business value that cloud computing bring out and taking more steps towards an alteration to the cloud. A smooth transition entails a thorough understanding of the advantages as well as challenges are involved. The cloud computing technology is contains some issues. The main challenge to cloud computing is how it addresses the security and privacy concerns of businesses thinking of adopting it. The fact that the valuable venture data will reside outside the company firewall raises serious concerns. Hacking and attacks on cloud infrastructure would affect multiple clients, even if only one site is attacked. These risks can be solved by using security applications, encrypted file systems, data loss software, and buying security hardware to track unusual behavior across servers. In fig 1 explained about cloud service architecture

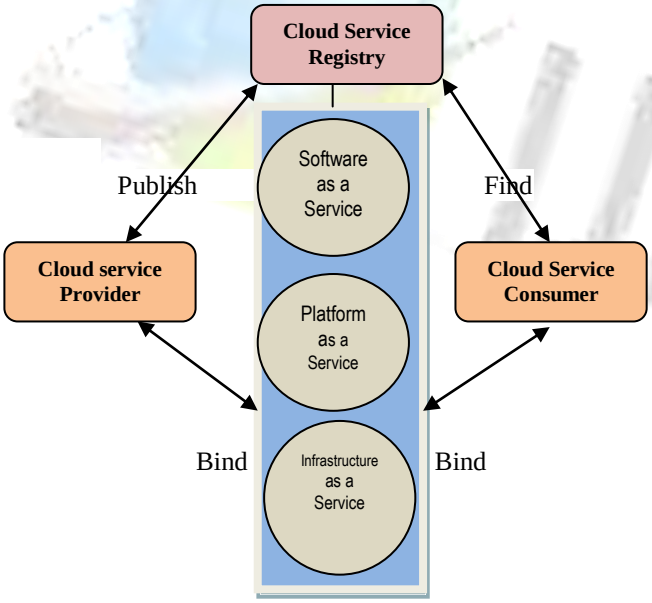

Fig 1.Cloud Service Architecture

A) Some of the failures are available in Provider Level Security

- Different types attacks(Internal, External) were happened by using of files
- Availability, Reliability and audibility Issues
- Country, Continent, Legal and Regulatory Issues
- Provider and Customer Security Systems
- Insecure Application Programming mediator

- Malicious Insiders entered
- Shared Technology Vulnerabilities
- Data Loss/Leakage problems
- Account, Service & Traffic Hijacking problem

B) Types of Security

Secure Data Transmission
•Data sharing with authorized users
•Transparent Security Protocols

Network Security
•Secure User Interface
•Robust Administrative Interface
•Secure Application Programming Interface

Interface Security
•Virtual Machine Management
•Virtualization
• Know about VM Identification

Virtual Machine Security
•Standardized and configured Service Level Agreement
•Audit
•Trust Management among participants

Compliance level system
•Data Location Privacy
•Cryptography Techniques for data level security
•invisible & Redundant Backups of data

IV. TRADITIONAL AUTHENTICATION AND AUTHORIZATION

Authentication Techniques

i) User Level Authentication:
In this authentication, user uses his login id and password stored in system servers and validates user credentials.
ii) Smart Card based authentication:
Authentication of cryptographic or stenographic data
iii) Biometrics:
Third party authentication user has to give a response such as username, token, retina scan or fingerprint. It is very useful only when data is top confidential e.g. Military.
iv)Grid Based Authentication:
This authentication is to entrust identity guard.
v) Knowledge Based Authentication:
This facility provides more confidence in user's identity to challenge attacker that is unbreakable. In this providers can ask to user about right information to confirm information about the user that already known through registration process like cross verification.
vi)Machine Level Authentication:
In this method of authentication, user can use their account allowing for secured authentication performed without any intrusion.

vii) One Time Password: (OTP)
It is a dynamically generated password which is valid for once only so if hacker hack this password he can't use it.OTP has two types: 1) Synchronous – in which token device is synchronized with authentication services by using time as a core piece of an authentication process. Asynchronous - an asynchronous token device to authenticate user use a challenge-response scheme.
viii) World Level authorization& agreement
The name suggested, all security rules and policies defined in this method are globally declared. This type classified as local and global authentication. E.g. Global –Organizational Membership, Prohibited Group.

B. Authorization model

When handing over the access control for data information the security level indicates the data sensitivity and categories which describe the kinds of information of the data. While assigning the access control for security level, it concentrated clearance and set of categories describe what kinds of data has certain right to use and access a particular data. The United State's lot of research idea goes on. In order to Authentication and Authorization for cloud computing, Context-aware platform stores, each user's personal information and profile, etc. It provides suitable services to the users. This context-aware model authenticate user can right of entry preference and use the cloud computing services.

The cloud computing solution means there will be employees of the provider make use of the customer's data and its applications. Similarly employees of the customer who needs to perform operations on the providers systems. Customers must ensure that the cloud provider has processed and functionality that govern who has access to the customer's data and applications. Conversely, the clouds providers must allow the customer to assign and managing the roles and associated levels of authorization for each of their users agree their security policies. For example, a cloud customer agreement and its security policies, whose role allows generating, purchase requests, but approval is given for another employee who is responsible for approving the request

i) The cloud provider must have a secure system for provisioning and manage unique identities for their Users and services. This Identity and Access Management (IdAM) functionality must support simple resource access and robust customer application and service work flow models.

ii) Chase introduced a multi- system authority in this approach each and every user has an unique ID and they are all interact with each key constraint creator using different pseudo code format. One user's contain different pseudo code to his or her private key, but key creators doesn't know about the private keys, and thus they can't link multiple pseudo code belonging to the same user. In fact they are even unable to differentiate the same user in dissimilar transactions. Also, the attributes set divided into N disjoint sets and managed by N attributes level authorities. That is, an attribute authorized member will provide key components which it is in- charge off. In this setting, even if an authorized successful guess a user's ID, if it knows only some parts of the user's oriented attributes, which are not enough to form out the user's uniqueness. However, the method proposed by Chase *et al.* Considered the basic threshold-based ABE, which stated at the beginning of this section lack expressing in conditions of encryption rule. In addition, many related literature works have been published to create more advanced schemes where data needs were secure and efficiently protected, which in turn served as the base of the research on security protocol in cloud computing environment.

V. PROPOSED SOLUTION

This system will prove that there is a one way of solution for the cloud environment. Most of the earlier authors concentrated on cloud service user's security not the provider end.

ISSN (Online): 2456-0448
International Journal Of Innovative Research In Management, Engineering And Technology
Vol. 2, Issue 6, June 2017

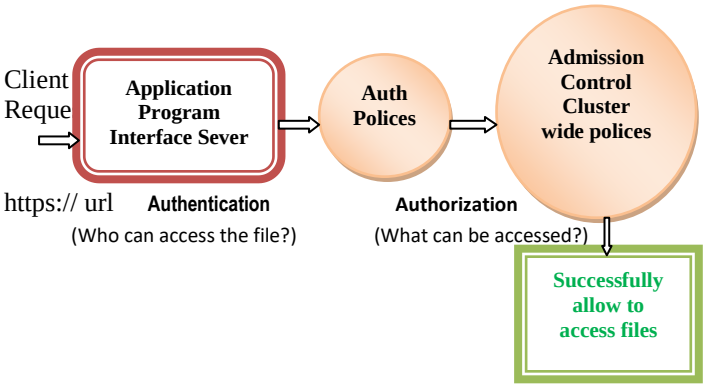

Fig 2. Authentication & Authorization model

The Cloud computing are depending upon through the internet and remote systems or servers in maintaining data for running and executing various applications. The authentication issues were also solved by privacy preserving concept. In fig. 2 specified how to enter a new user and if the user entered it wants to verify whether a person has authenticated user or not. Afterward what kind of files are accessing in the way of authorized manner then a person can get full privileges of admission control of suitable control polices .The application program interface servers check whether getting a request from a client ant its respond it. The policy terms recognized by the authorities and world level agreement; Public cloud has most level security when compares to private clouds but our proposal mainly concentrated on secured public cloud users and providers and without any further issues. Compare with previous traditional authentication and authorization model to propose a world level authorization model of the solution will be discussed.

VI. CONCLUSION AND FUTURE WORK

This paper discusses the various ideas. Cloud computing issues and Traditional Authentication techniques and Authorization, features and dilemmas. Literature review as background work in the cloud computing, the issues related to cloud, some of the failures are available in provider Level security, secure data transmission, authentication technique, authorization model finally a Novel proposed solutions, to tackle these problems. This system proves that there is a solution which covers in the cloud environment. Most of the earlier authors concentrated on cloud service user's security, not the provider oriented security. In this proposal, all the cloud issues are going to sort out in the package of solution. In future the proposal, implementation level will be discussed.

References

[1]Kire Jakimoski, (2016), "Security Techniques for Data Protection in Cloud Computing", International Journal of Grid and Distributed Computing, No. 1, pp.49-56.
[2]Taranpreet Bhatti, Ashish James, Siddhi Narvekar,"(2016) Secure Authorized Deduplication on Hybrid Cloud",(2016 International Research Journal of Engineering and Technology (IRJET),3 , 1574-1578.
[3]Nitin Naik and Paul Jenkins," (2016)A Secure Mobile Cloud Identity: Criteria for Effective Identity and Access Management Standards", IEEE on Mobile Cloud Computing, Services, and Engineering, DOI:0.1109/MobileCloud.2016.22
[4] R.Balasubramanian, M.Aramudhan,(2012) Security Issues: Public vs. Private vs. Hybrid Cloud Computing, International Journal of Computer Applications 55(13),35-41.
[5] Aarti Singh, Manisha Malhotra (2015) Security Concerns at Various Levels of Cloud Computing Paradigm: A Review, International Journal of Computer Networks and Applications 2, 41-45
[6] Pradeep Kumar Tiwari, Bharat Mishra (2012) Cloud Computing Security Issues, Challenges and Solution, International Journal of Emerging Technology and Advanced Engineering 2, 306-310.
[7] Jasleen Kaur, Anupma Sehrawat, (2014), Survey Paper on Basics of Cloud Computing and Data Security, *International Journal of Computer Science Trends and Technology* 2,16-19.
[8] Nilesh Mahajan, Devyani Patil(2016), Study of Authentication and Authorization in Cloud Computing, International Journal on Recent and Innovation Trends in Computing and Communication 4, 178-180.

[9] Shabnam Sharma, Usha Mittal (2013) Comparative Analysis Of Various Authentication Techniques In Cloud Computing, International Journal of Innovative Research in Science, Engineering and Technology 2, 994-998.
[10] Lee, K. (2012). Security Threats in Cloud Computing Environments. International Journal of Security and Its Application, 6(4), 25-32.
[11] Singh, S, and Jangwal, T. (2012). Cost breakdown of Public Cloud Computing and Private Cloud Computing and Security Issues. International Journal of Computer Science & Information Technology, 4(2), 17-31.
[12] V.Sujatha bai , S.Hendry Leo Kanickam , N.Vijayaraj (2012), "Research on M-Learning Supported by 3G/4G",Intenational journal of Computer application , IWAY Number 1, pp 12-15
[13] Taeho Jung, Xiang-Yang Li, Zhiguo Wan and Meng Wan (2013), Privacy Preserving Cloud Data Access With Multi-Authorities, cs CR, 6,1-9.
[14] Deepa Panse, P. Haritha (2014), Multi-factor Authentication in Cloud Computing for Data Storage Security, International Journal of Advanced Research in Computer Science and Software Engineering,4 ,629-634.
[15]Abdelmajid Hassan, Mansour Emam,"Additional authentication and authorization using Registered Email-ID for Cloud computing" (IJSCE) ISSN: 2231-2307, Volume-3, Issue-2, May 2013.
[16] E. Mykletun, M. Narasimha, and G. Tsudik, "Authentication and integrity in outsourced databases," Trans. Storage, vol. 2,no. 2, pp. 107–138, 2006.
[17] S.Hendry Leo Kanickam ,Dr.L.Jayasimman ,Dr.A.Nisha Jebaseeli(2016) , "A Survey on Layer wise Issues and Challenges in Cloud Security" , IEEE Xplore, ISSN: 978-1-5090-5573-9/16 , DOI 10.1109/WCCCT.2016.49 , pp 168-171
[18] S.Hendry Leo Kanickam(2016) , "Security Oranization of Cloud Storage Based on Homomorphic Encryption Proposal" , Roots International Journal of Multidisciplinary Researches , Volume -2 ,Issue 10, pp. 64-68.

Author I

Mr.S.Hendry Leo Kanickam working as an Assistant Professor in Department of Information Technology ,St.Joseph's College (autonomous) Trichy, India. He received his M.Phil Degree in Bharathidasan University in 2008 and also He is pursuing Ph.D (Computer Science) in Bharathidasan University.

Author II

Dr. L. Jayasimman working as an Assistant Professor, with Department of Computer Science, Srimad Andavan Arts & Science College, Trichy, India. He received his M.Tech Degree in Bharathidasan University, Trichy, India in 2008 and completed his PhD (Computer Science) in Bharathidasan University in 2014.