A Novel Approach for User Authentication in Cloud

Miss. Vrushali R. Hirkane Dr. V. M. Thakare Dr. S. S. Sherekar

***Abstract*:- Cloud Computing has been envisioned as the next-generation architecture of IT Enterprise. In cloud computing application software and databases are moving to the centralized large data centers. This mechanism brings about many new challenges, which have not been well understood. Security and privacy concerns, however, are among the top concerns standing in the way of wider adoption of cloud. In cloud computing the main concern is to provide the security to end user to protect files or data from unauthorized user. Security is the main intention of any technology through which unauthorized intruder can't access your file or data in cloud. In this paper we analyzed a three method preserving cloud computing privacy architecture, authentication architecture, Cloud information accountability (CIA) framework. The proposed model increases the security at the security access point level of cloud computing and status monitor system with data log mechanism. This framework ensures the user by keeping user's data privacy giving access policies. And log mechanism contain the user policy according to that user has privilege to access services and data in cloud**

***Keywords* – authentication, security, privacy, cloud services.**

I. INTRODUCTION

Cloud computing has emerged from grid computing [1], and it is a recent technological trend that aims to provide services and information through the Internet according to demand and the payment is made according to what it is used. Cloud computing realizes the management of a resource pool automatically and dynamically through software and hardware. The computational model in the Clouds aims to provide three benefits [2]. The first is related to cost reduction since it is not necessary acquire new machines and maintaining them. Second, there is a great flexibility to add and replace computational resources in terms of hardware and software in a manner which met the needs of users. Last, the users do not need to know where the services and resources are localized physically when they want to access them. Cloud services are offered in three models. These are known as the SPI Models which are derived from Software, Platform and Infrastructure as a service.

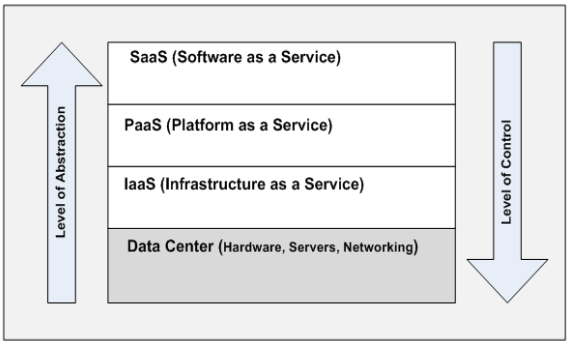

Fig.1 Cloud Computing Services Architecture

The software as a service (Software as a Service - SaaS) the client is offered with applications running on a cloud infrastructure. They can be accessed by multiple devices browser. The consumer does not need to bother on how to manage or control the infrastructure (network, server, OS, storage, etc.).The platform as a service (Platform as a Service - PaaS) offers an infrastructure with a high level of integration to test implementations and applications in the cloud. It is through a PaaS that operating systems, programming languages and development environments are provided to test applications. Infrastructure as a service (Infrastructure as a Service - IaaS) offers the consumer with processing, storage, networks and several basic computational resources so that the consumer is able to deploy and run the software he wants. Cloud computing has some advantages and some challenges. One advantage is that services are quick, simple and their cost is inexpensive. They have the characteristic resiliency in that resources are occupied and liberated according to demand. The amount of available resources is more than consumers have in Indeed. Consumers do not need to worry about processing power, energy use, or license systems. Cloud computing has some challenges such as security, reliability, availability, privacy, interoperability and service level agreement.

II. BACKGROUND

Much research has been done on security and privacy of user in cloud computing environment. Model for hiding the presences of individual from shared database. Ambiguity hides the presences of individual. A client based privacy manager for cloud computing. Privacy in the cloud risk to privacy and confidentiality from cloud computing. Proposed a cloud trust module in security aware cloud[1].Provable data possession at

untrusted stores. Accountability mechanisms to address privacy concerns of end users and then develop a privacy manager .A distributed approach to accountability are from. An agent based system specific to grid computing. Cloud security and privacy: an enterprise perspective on risks and compliance. Accountability as a way forward for privacy protection in the cloud. Preventing information leakage from indexing in the cloud. Promoting distributed accountability in the cloud [2].

Security in cloud based e-learning computing given in. The cloud computing benefits for e-learning solutions. Seven deadly threats and vulnerabilities in cloud computing. Security and high availability in cloud computing environment [3]. A frame work comp rising of different techniques and specialized procedure res is proposed that can efficiently protect the data from the beginning to the end, i.e., from the owner to the cloud and then to the user[4]. It first identify the data mining based privacy risks on cloud data and propose a distributed architecture to eliminate the risks [5]. It is discuss about some of the techniques that were implemented to protect data and propose architecture to protect data in cloud. This architecture was developed to store data in cloud in encrypted data format using cryptography technique which is based on block cipher [6].
The Effective Privacy Protection Scheme (EPPS) is proposed to provide the appropriate privacy protection satisfying the user demand of privacy requirement and maintaining system performance simultaneously [7]. SasS protocol gives the user a chance to define the security of their data, by leaving the option of dividing the data into chunks [8]. Propose a new privacy preserving authenticated access control scheme for securing data in clouds [9].It introduces a detailed analysis of the cloud computing security issues and challenges focusing on the cloud computing types and the service delivery types. It mainly proposes the core concept of secured cloud computing [10].

This paper is organized as follows: in section 3 provides a previous work done section 4 describes the existing methodology. Sections 5 analysis and discussion section 6 explain the proposed methodology. Section 7 gives details about the possible outcome of proposed methodology. Finally, Section 8 provides conclusion and 9 gives some future lines.

III. Previous Work Done

Conventional access control approaches developed for closed domains such as databases and operating systems, or approaches using a centralized server in distributed environments, are not suitable, due to the following features characterizing cloud environments. First, data handling can be outsourced by the direct cloud service provider (CSP) to other entities in the cloud and theses entities can also delegate the tasks to others, and so on. Second, entities are allowed to join and leave the cloud in a flexible manner. As a result, data handling in the cloud goes through a complex and dynamic hierarchical service chain which does not exist in conventional environments [2].A common approach to protect user data is that user data is encrypted before it is stored. In a cloud computing environment, a user's data can also be stored additional encryption, but if the storage and encryption of a given user's data is performed by the same service provider, the service provider's internal staff (e.g., system administrators and authorized staff) can use their decryption keys and internal access privileges to access user data[3]. To prevent the access of user private data an effective method for security is required.

IV. Existing Methodology

The proposed model [1] of Preserving cloud computing Privacy (PccP) has a three - layered architecture following are layers in this architecture.

- Consumer layer
- Address mapping layer and
- Privacy preserving layer.

Any request for service by the cloud user will have to process through these three layers and then accordingly cloud user request is serviced. This architecture uses unique service dependent identity (USID) and Match logic. The main functionality of Match logic is to ensure that the duplication of generated identities is avoided and that the USID's once generated are prevented from being allocated to any new user. Proposed a novel approach [2], namely Cloud Information Accountability (CIA) framework, based on the notion of information accountability. Unlike privacy protection technologies which are built on the hide-it-or-lose-it perspective, information accountability focuses on keeping the data usage transparent and track able. Proposed CIA framework provides end-to-end accountability in a highly distributed fashion. By means of the CIA, data owners can track not only whether or not the service-level agreements are being honored, but also enforce access and usage control rules as needed. Associated with the accountability feature, system contains two distinct modes for auditing: push mode and pull mode. The push mode refers to logs being periodically sent to the data owner or stake holder while the pull mode refers to an alternative approach whereby the user can retrieve the logs as needed. This method provide a security when data is transfer but not at the storage level.
The authentication architecture [3] provides access security to data.If a user want to access the data if it belongs to protection then user have to register to the authentication cycle itself and after that user name and password it check if it match then user access the services or data. If it doesn't match then user not

allows accessing their account. If user is already registered need not require further registration. But password and username not provide a strong access security so that a new method is required which provide a data security and access security with strong password.

V. ANALYSIS AND DISCUSSION

Match Logic is that privacy preserved and service dependent user identities are being generated [1]. The Match logic mechanism also ensures that any privacy leaked identities are prevented from being allocated to the users. Furthermore, the pool of privacy preserved identities as well as the privacy leaked identities is updated. Finally the currently generated privacy preserved identity is allocated, thereby enabling the user to access cloud services**.**

Associated with the accountability feature, CIA system contains two distinct modes for auditing: push mode and pull mode. The push mode refers to logs being periodically sent to the data owner or stake holder while the pull mode refers to an alternative approach whereby the user can retrieve the logs as needed [2]. The logger is the component which is strongly coupled with the user's data, so that it is downloaded when the data are accessed, and is copied whenever the data are copied. It handles a particular instance or copy of the user's data and is responsible for logging access to that instance or copy. The time to create a log file increases linearly with the size of the log file. But it not covers issues of data storage security which are a complementary aspect of the privacy issues. The attacks may steal the jar file in which logging policies are defined. Authentication cycle provide way to protect their client's data, especially to prevent the data from disclosure by unauthorized insiders. User-name and password doesn't match then user is not allowed to access their account [3]. And also in some case if hacker wants to hack the account of a particular user then in that case hacker gets only the fake database of the account is there to access the account by hitting the user-name and password, if limit become cross then hacker get's the fake database. It is very important in shared environment to properly and securely authenticate system users and administrators, and provide them with access to only the resources they need to do their jobs or the resources that they own within the system. It is also very important in a cloud environment to know who is doing what within the system, when they did it, and what exactly they did. Separating duties and enforcing least privilege applies for both the cloud provider and the customer. The cloud provider should ensure that only authorized administrators have access to resources. They should also provide the customer with a mechanism for giving internal administrators access to necessary resources. Text-based authentication is vulnerable to more complex attacks, such as Brute force attacks and packet sniffing. With Brute force attacks, an intruder tries to guess the users password, or uses a password hash file. Alternatively, an intruder can use easily downloaded packet sniffing technologies such as Ethereal (Akula).

VI. PROPOSED METHODOLOGY

Authentication is quite challenging and difficult in the case of Cloud Computing. In most applications, authentication is achieved through username and password only. With password cracking tools available free online, hackers take few minutes to identify the user's password [3]. Current authentication schemes suffer from many weaknesses. Textual passwords are widely used; howeverusers tend to choose meaningful words from dictionaries. This makes textual passwords easy to break and vulnerable to dictionary or brute force attacks. Smart cards or tokens can be lost or are prone to theft. To safeguard users against this threat, a new authentication scheme is required. Proposed model may provide a strong authentication process so that only authorized user can access the services. Our solution regards increasing security at the services access point level of cloud computing and also provide a status monitoring system with logger mechanism. The mechanism strongly coupled with user data and status monitoring system monitors access log of users. Then all these information is transfer with the request to the services according to that user can use the services of cloud.

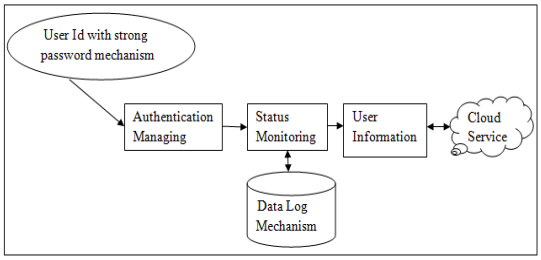

Fig2.Authentication System

VII. POSSIBLE OUTCOME AND RESULT

Our solution regards increasing security at the security access point level of cloud computing. Access policies that ensure only authorized users can gain access to sensitive information, so that even privileged users such as root user cannot view sensitive information. By providing data log mechanism focuses on keeping the data usage transparent and track able

VIII. CONCLUSION

Security features provided by service providers in a cloud computing is not totally trustful. This paper has presented some works on existing access control, security and privacy in the cloud computing environment. Information deemed

confidential needs to be protected, thus providers seeks technological innovations that guarantees protection and privacy of information users. This work has focused on the existing access control mechanisms in cloud computing environments and proposed an authentication system and status monitoring system with log mechanism. This framework ensures the user by keeping user's data privacy giving access policies.

FUTURE SCOPE

For future enhancement we would like to concentrate more on strong authentication techniques. Other mechanisms are still needed to improve access control, privacy of data, and secure sharing of information.

REFERENCES

[1] Syed MujibRahaman , Mohammad Farhatullah "A Framework For Preserving Privacy In Cloud Computing With User Service Dependent Identity" *International Conference On Advances In Computing, Communications And Informatics* VOL 978-1-4503-1196-0/12/08 , PP 133-136, AUGUST 2012.

[2] SmithaSundareswaran , Anna c. Squicciarini, Dan Lin "Ensuring Distributed Accountability for Data Sharing in the Cloud" IEEE *Transaction On Dependable And Secure Computing* VOL 9, No 4 , PP 556-568, JULY-AUGUST 2012.

[3] A. Elusoji, L.N. Onyejegbu, O.S. Ayodele "An Effective Measurement Of Data Security In A Cloud Computing Environment" IEEE *African Journal of Computing & ICT* VOL 6 NO2**,** PP67-76, JUNE 2013.

[4] Sandeep K. Sood "A Combined Approach To Ensure Data Security In Cloud Computing" *Elsevier Journal of Network and Computer Applications* VOL 33, PP 1831-1838, JULY 2012.

[5] Dev H. , Sen, T. ,Basak, M. Ali "An Approach to Protect the Privacy of Cloud Data from Data Mining Based Attacks" *High Performance Computing, Networking, Storage and Analysis (SCC),*VOL 978-1-4673-6218-4 ,PP 1106 – 1115 , 2012.

[6] Sugumaran, M. Murugan, B.Bala ; Kamalraj, D. "An Architecture for Data Security in Cloud Computing" *Computing and Communication Technologies (WCCCT),* VOL 978-1-4799-2876-7 PP 252 – 255 , 2014.

[7]Hsun, Chuang , Syuan-Hao Li , Kuan-Chieh Huang ,Yau-Hwang Kuo "Aneffective privacy protection scheme For cloud computing" *13th International Conference on Advanced Communication Technology (ICACT),* VOL 978-1-4244-8830-8 PP 260 – 265 , FEB 2011.

[8] Ram, C.P. Sreenivaasan, G. "Security as a Service (SasS): Securing user data by coprocessor and distributing the data" *Trendz in Information Sciences & Computing (TISC),*VOL 10.1109/TISC.2010.5714628 ,PP 152 – 155, 2010.

[9]Shaikh.F.B.; Haider.S. "Security threats in cloud computing" *International Conference on Internet Technology and Secured Transactions (ICITST),* VOL 978-1-4577-0884-8 ,PP 214 – 219,DEC 2011.

[10] Kulkarni, G. Gambhir, J.,Patil, T. Dongare, A. "A security aspects in cloud computing" *IEEE 3rd InternationalConferenc,*VOL10.1109/ICSESS.2012.6269525 , PP 547 – 550, JUNE 2012.