# A Multi-Factor Cloud Authentication And Access Control

**Himanshu Panadiwal[1], Chandra Prakash Patidar[2]**
[1, 2] Department of Information Technology

***Abstract-*** *The use of cloud computing and their relevant technology is growing rapidly. Due to this the need of new techniques for security and authentication is also rises in similar manner. In this presented paper a survey on the different existing techniques of authentication is explored and a new technique for securing the data storage of cloud server is proposed. The main aim of the proposed paper is review the different authentication schemes and recover most optimum technique for enhancing the ability of authorized persons data and sensitive information. The need of merchantable computing and storage switch the users to consume the services of cloud. Cloud computing technology provides both the prospective of computing. On one side it provides ease in computing new manner but the traditional manner of security is not much promising to work with it. Therefore need to enhance the security aspects of the cloud computing. In order to provide the effective security in computational cloud the proposed work is intended to find an optimized way of security using authentication and access control methodology. Thus new multi-factor authentication schemes are investigated and try to evolve for improving the security over the cloud storage data access.*

***Keywords****-* Cloud Computing, Security, Authentication, Survey, Multi-Factor Password, Password Management

## I. INTRODUCTION

The need of new computational manner is increases continuously and due to this new invention and security techniques are also increases in the similar ways. The authentication is one of the most essential parts of the security during the data access and sharing services. The requirement of data access is a party of privacy management techniques. Therefore for the sensitive or private data communication the authentication and access policies are collaborating each other, for reform the existing access control and authentication scheme.

Therefore in this presented study the authentication and privacy management technique is investigated and an improved authentication technique is proposed for improving the security and access of sensitive data in cloud environment. The proposed security and access control technique is based on the multi-factor authentication mechanism. In this technique the key user attributes and the system attributes are identified and utilized as key for validating the user and their role in the system. These attributes can be user behavior based access pattern or the application usage pattern. Additionally for more authenticity that is required to incorporate the system attributes with the user Behavior based key. The proposed work provides the promising approach for utilizing with the security and authentication technique which used control the access of data and also helps to manage the privacy concerns arises in the security of the data in computational cloud environment.

Cloud computing is a new generation computational infrastructure and used for scalable and efficient computing as well as storage requirements. Scalable term is used to denote the requirement based storage for the applications and the organizational databases. These techniques are also usages the concept of data outsourcing for managing data access and to reduce the complexity of the data management.

A number of cloud applications are consuming the sensitive and private data such as banking applications, social network and other applications. These applications collect these data on the storage and provide the access on demand to requested users. But the handing of the huge data can harm the privacy during the access therefore a strong cryptographic manner is required to keep in track the security as well as authenticity of data owner. In this approach there are two key issues are observed:

1. **Data and Data Owner Management:** during the data access and exchange that is required to keep the data secure from other participating user in same platform. Due to this data and their sensitivity remain during distribution of data and access.

2. **Secure Access of Data and Access Control of Data:** in further for securing the data access and control unauthorized access the user attributes as well as the system attributes are consumed for establishing the secure and authentic communication and access of private and sensitive data in un trusted environment or network.

The key issues of the proposed system is addressed in this section the next section provides the overview of the proposed technique and involved issues in the design of secure authentication and access control of the sensitive data in private cloud.

## II. BACKGROUND

### A. Authentications

Authentication is the act of confirming the truth of an attribute of a single piece of data claimed true by an entity. In contrast with identification which refers to the act of stating or otherwise indicative of a claim supposedly attest to a person or thing's identity, authentication is the process of actually validate that character. It might absorb validate the identity of a person by validating their identity documents, verifying the validity of a Website with a digital certificate, tracing the age of an artifact by carbon dating, or ensuring that a manufacture is what its packaging and labeling claim to be. In other words, authentication often involves verifying the validity of at least one form of identification [1, 8].

Or authentication is a process in which the credentials provide are measure up to those on case in a database of authorized users' information on a local operating system or inside an authentication server. If the certificate matches, the process is completed and the user is granted authorization for admittance. The permissions and folders return define both the environment the user sees and the way he can interact with it, together with hours of admittance and other rights such as the amount of allocated storage space.

The process of a supervisor conceding rights and the procedure of checking user account permissions for access to resources are both referred to as agreement. The rights and partiality granted for the authorized account depend on the user's permissions [9], which are either stored locally or on the authentication server. The settings defined for all these environment variables are set by an administrator.

### B. User Authentication vs. Machine Authentication

User authentication comes about within most human-to-computer relations other than guest accounts, automatically logged-in accounts and booth computer systems. In general, a user has to enter or choose an ID and provide their password to begin using a system. User authentication authorizes human-to-machine relations in operating systems and applications as well as together wired and wireless networks to enable admittance to networked and Internet-connected systems, applications and resources [2].

Machines need to authorize their automated measures inside a network too.

Machine authentication can be carried out with machine credentials much like a users' ID and password only submitted by the device in question. They can also use digital certificates issued and verified by a Certificate Authority (CA) as part of a public key communications to prove recognition though exchanging information over the Internet, like a type of digital password.

## III. LITERATURE SURVEY

The given section provides the different recent research trends and the efforts that placed in order to provide the strong authentication management for secure data access.

Along with the development of cloud computing, cloud-based RFID is getting more and more attentions of researchers and engineers. However, there is no investigate in which cloud computing is practical to RFID authentication schemes. Most current works lay emphasis on functionalities, lacking thought regarding security and privacy. Classical RFID authentication schemes fail to gather the special security and privacy supplies of cloud-based RFID. The basic postulates of traditional backend sever based RFID authentication, i.e. secure backend channel and entirely trustworthy database, and are no longer natively tenable in cloud-based RFID scenarios. In this paper Wei Xie et al [3], a virtual private network agency is suggested to build secure backend channels and to provide person who reads with anonymous access to the cloud. The cloud database is prepared as an encrypted hash table. The first cloud-based RFID authentication procedure preserving tag/reader privacy to database keeper is future.

Through the express developments of the IoT (Internet of Things) and the cloud computing, cloud-based RFID systems attract further thought. Users can reduce their cost of deploying and maintaining the RFID system by purchase cloud services. Conversely, the security threats of cloud-based RFID systems are more serious than those of traditional RFID systems. In cloud-based RFID systems, the connection between the reader and the cloud database is not secure and cloud overhaul supplier is not trusted. Therefore, the users have to encrypt their data stored in the cloud database to avoid the escape of solitude. In adding, the reader's location privacy must be protected to avoid its leak to the cloud provider. In this paper Qingkuan Dong et al [4], a cloud-based RFID mutual authentication procedure with no leak location privacy to the cloud is future. It provides real-time mutual verification between the reader and the tag and defends the reader's location seclusion by introducing the location retreat cloud. Compare with traditional backend-server based schemes and server-less schemes, the future scheme has evident advantages in deployment cost, scalability, concurrent authentication, and the tag’s computational complexity.

Security threats are considered the main difficulty that excluded possible users from reaping the forceful profit of the cloud computing model. Regrettably, traditional password authentication jeopardizes user privacy. Anonymous password authentication (APA) represents a promising process to preserve users’ privacy. However, the main handicap that faces the deployment of APA is the high computation cost and natural shortcomings of conformist password schemes. In the given scheme, Ali A. Yassin et al [5] present a new setting where users do not need to record their passwords to service provider. They are supplied with the required official document information from the data owner. In addition, for permit the service provider to identify the authorized users, data proprietor supplies the service provider with several secret identities information that is resulting from the pair (username/password) of each user. Given approach shows good results in terms of high scalability which makes scheme more suitable to the cloud situation, strong authentication that withstand dissimilar recognized attacks.

The cloud computing platform gives community the prospect for sharing income, services and information among the people of the whole world. In private cloud system, information is shared among the persons who are in that cloud. For this, security or personal information hiding process hampers. In this paper Kawser Wazed Nafi et al [6] have proposed new security architecture for cloud computing platform. This makes sure secure communication system and defeat information from others. This structure can be simply practical with main cloud computing skin texture, e.g. PaaS, SaaS and IaaS [13]. This model also includes onetime password system for user authentication process. Given work mainly deals with the security system of the whole cloud computing platform.

Cloud computing is a promising computing model which ease organizations and the IT industry. It helps them to reproduce or lessen their capital according to their operational requirements. However, the organizations are indisposed to store their responsive information on the cloud due to various privacy and identity tracking threats. In the past few years, a lot of research and development efforts have been made to define centralized and federated security mechanisms for the defense of identity in sequence in a cloud environment. However, to the best of knowledge none of the systems have been considered observance anonymity as the key component. Umer Khalida et al [7] describes an authentication and authorization procedure which draw the main features of anonymous [11] communication in the cloud. The resolution is an addition of offered standards making it easy to integrate and compatible with existing standards.

## IV. PROPOSED WORK

Cloud computing is comparatively new domain of the computing infrastructures thus a number of research issues and adaptation challenges are exists. Among the security, privacy and access control are primary issues in cloud adaptation. In different literature discussion and review of access policies the following issues are addressed for cloud based [10] access control.

1. The access control policies are not provide complete identity management for all kinds of applications
2. Generalization is not achieved in any access control model
3. User identity is not managed due to frequent access of data and information
4. Less secure and less trust worthy environment and authentication protocols

The proposed solution development for secure and authentic access control management the following solution is proposed.

1. The proposed solution prepares a multi-factor authentication scheme for granting access to the cloud storage
2. The multi-factor authentication [14] approach first identifies the user behavior attributes and combines with the system attributes to generate the authentication keys
3. The generated keys are used for authentication and access management for the cloud storage
4. During change in user attributes and properties of the system, cloud verifies the trust using one time pad
5. Change in the system behavior and user behavior is efficient animatedly and automatically to the attendant authenticator and further used for access management. The proposed work provides the multi-factor authentication scheme for securing the data as well as providing the effective access control [15, 16] of the data. Therefore there are three main factors are estimated for utilization:

1. User attributes: these attributes are recovered from the original data which is provided by user for registration purpose and among them some selected attributes are used for preparing the authentication key as the first factor.
2. Data attributes: a number of different kinds of data is used by the end user such as images, some text files and other

contents. Thus a part of original data is used as second factor which is request by the user for access.

3. System Attributes: In this phase the system properties are extracted to use with the authentication technique development. Thus the system property by which the request is made or data is uploaded is also considered as the factor for the authentication.

After recovering the attributes to use for secure data access and authentication that are used with the system for providing the access control of the sensitive and private data. The proposed system provides the security [17] in the following manner as given in the figure 1.The given figure demonstrates the proposed authentication methodology for the secure and authentic data access. The participating attributes and the components of the system are provided as:

1. **User Registration:** In order to keep in track the security and access control first need to register the user. During the registration the user provides some personal and professional details to prepare the profile of user. When the user need to access the data the profile of the user is required for match them during request.
2. **User Input Attributes:** The user input data for completing the user profile need to provide some input for profile using the input attributes the registration process is performed.

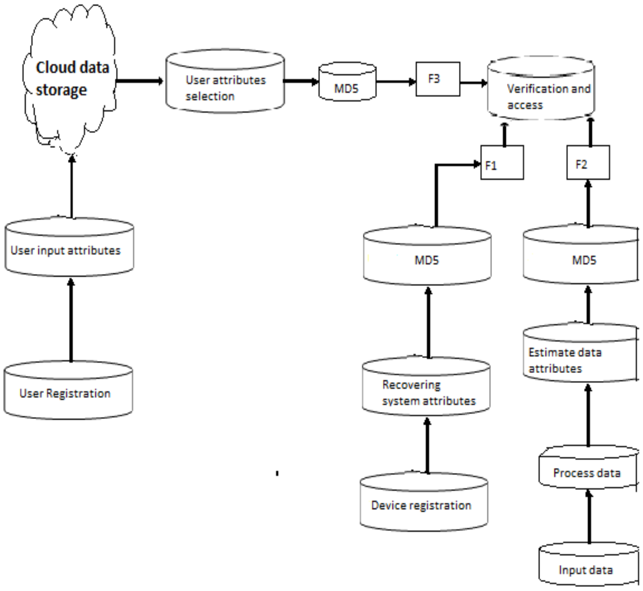

Figure 1 Proposed Authentication Model

3. **Cloud Data Storage:** That is the basic cloud data base which is prepared to make user profile, basically these attributes are not directly participating with the authentication process therefore the storage on the server is not affecting the security of the user authentication.
4. **User Attributes Selection:** That the profile based attribute selection process, that perform by selecting the random attributes from the user profile. For example if a user have the user name, age, salary and other parameters to provide for completing their profile only two or three attributes are get selected from the data base in random manner and user with authentication.
5. **Device Registration:** That is responsible to construct the system side attributes and for second factor. Therefore the system properties are extracted using the application and some random factors are utilized for authentication thus not all the user have the same features of the system and may have the different keys as factor for secure validation of data access and recovery.
6. **Recovering System Attributes:** In this phase the extracted system parameters are evaluated and selected only two parameters from recovered different features of the system.
7. **Input Data:** That can be any kind of file in different format such as image or any kind of text which is required to preserve on the targeted server.
8. **Process Data:** In order to prepare the third factor of the authentication the input data is evaluated using an additional process where from text file or image file some attributes are recovered and used as the attribute of the data.
9. **Estimate Data Attributes:** The extracted data features are minimized or prepare the similar size of attributes for utilizing the data as key for authentication.
10. **MD5:** That is a hash generation technique which accept any size of data to produce a fixed length of key thus different recovered features from the data is processed using the MD5 algorithm that generates the fixed length of string as key for cryptographic data security and also can be used for validating the user data access.
11. **F1, F2, and F3:** The different kinds of obtained attributes from the user, system and the data are used with the cryptographic hash function. These functions are generating the factors for authentication.
12. **Verification and access Control:** The recovered factors are combined together and used to develop a key for the following
    1. Authentication during the system access
    2. Data preservation and storage
    3. On demand data exchange and sharing
    4. Privacy preserving [12] data and data owner management.

## V. CONCLUSION AND FUTURE WORK

The given paper is a proposal and review for the securing the cloud storage service for preventing the unauthorized data and information access. Therfore different variety of authentication schemes are explore and thr recent efforts on improving the technique of authentication is also reviewed. Finally using the concluded techniques a new method for effective authentication is proposed. The future arhitecture for secure the cloud based strogae is also demonstrated in this paper. In near future the proposed model is implemeted through the relevent technology and their performance and the limitations are discussed.

## ACKNOWLEDGMENT

The preferred spelling of the word ―acknowledgment‖ in American English is without an ―e‖ after the ―g.‖ Use the singular heading even if you have many acknowledgments.

## REFERENCES

[1] Robert Havighurst, "User Identification and Authentication Concepts", 2007 by Taylor & Francis Group, LLC

[2] Richard L. Zunkel, "HAND GEOMETRY BASED VERIFICATION.

[3] Wei Xie, Lei Xie, Chen Zhang, Quan Zhang, Chaojing Tang, "Cloud-based RFID Authentication", 2013 IEEE International Conference on RFID (RFID)

[4] Qingkuan Dong, Jiaqing Tong, and Yuan Chen, "Cloud-Based RFID Mutual Authentication Protocol without Leaking Location Privacy to the Cloud", Hindawi Publishing Corporation International Journal of Distributed Sensor Networks Volume 2015, Article ID 937198, 9 pages

[5] Ali A. Yassin, Hai Jin, Ayad Ibrahim, WeizhongQiang and DeqingZou, "Efficient Password-based Two Factors Authentication in Cloud Computing", International Journal of Security and Its Applications Vol. 6, No. 2, April, 2012

[6] Kawser Wazed Nafi, Tonny Shekha Kar, Sayed Anisul Hoque, Dr. M. M. A Hashem, "A Newer User Authentication, File encryption and Distributed Server Based Cloud Computing security architecture", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 3, No. 10, 2012

[7] Umer Khalida, Abdul Ghafoor, MisbahIrum, Muhammad Awais Shibli, "Cloud based Secure and Privacy Enhanced Authentication & Authorization Protocol", 17th International Conference in Knowledge Based and Intelligent Information and Engineering Systems - KES2013

[8] Marcos A. P. Leandro, Tiago J. Nascimento, Daniel R. dos Santos, Carla M. Westphall, Carlos B. Westphall, "Multi-Tenancy Authorization System with Federated Identity for Cloud-Based Environments Using Shibboleth", ICN 2012 : The Eleventh International Conference on Networks

[9] Mr. Ankush Kudale, Dr.Binod Kumar, "Protected Authentication by Login Credential and OTP for Cloud Based Application", International Journal of Computer Application (2250-1797) Volume 5– No. 3, April 2015.

[10] SaeidAbolfazli, ZohrehSanaei, Ejaz Ahmed, Abdullah Gani, Rajkumar Buyya, "Cloud-Based Augmentation for Mobile Devices: Motivation, Taxonomies, and Open Challenges", IEEE Communications Surveys & Tutorials, Accepted For Publication.

[11] Ruj, Sushmita, Milos Stojmenovic, and Amiya Nayak, "Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds." Parallel and Distributed Systems, IEEE Transactions on 25, no. 2 (2014): 384-394.

[12] Bharathy, S. Divya, and T. Ramesh. "Securing Data Stored in Clouds Using Privacy Preserving Authenticated Access Control." (2014).

[13] Nguyen, Dang, Jaehong Park, and Ravi Sandhu, "Adopting provenance-based access control in Open Stack cloud IaaS", In Network and System Security, pp. 15-27, Springer International Publishing 2014.

[14] Lee, Keunwang, and Haeseok Oh, "Research on access control method by user authority using two-factor authentication" In Proceedings of the 1st International Conference on Convergence and its Application (ICCA'013), vol. 24, pp. 172-175. 2013.

[15] Kabir, M.E., Wang, H., and Bertino, E. (2012), "A Role-involved Purpose-based Access Control Model", Information Systems Frontiers, 14(3), 809-822

[16] Nguyen, Dang, Jaehong Park, and Ravi Sandhu "A provenance based access control model for dynamic separation of duties." In Privacy, Security and Trust (PST), 2013 Eleventh Annual International Conference on, pp. 247-256, IEEE, 2013.

[17] Wazan, Ahmad Samer, Gregory Blanc, Hervé Debar, and Joaquin Garcia-Alfaro. "Attribute-based Mining Process for the Organization-Based Access Control Model" In Trust, Security and Privacy in Computing and Communications (TrustCom), 2013 12th IEEE International Conference on, pp. 421-430, IEEE, 2013.