AUTHENTICATION - A PART OF IDENTIFICATION IN THE CLOUD ENVIRONMENT

Mrs. R. Anuratha[1], Dr. M. Ganagadurga[2]

[1]Research Scholar, Computer Science, Bharathiar University, Coimbatore, (India)
Asst. Professor, Mannar Thirumalai Naicker College, Pasumalai, Madurai, India.
[2]Research Supervisor, Computer Science, Bharathiar University, Coimbatore, (India)
Asst. Professor, Govt. Arts College for Women, Sivagangai (India)

ABSTRACT

Cloud Computing is a combination of traditional computing technology and network technology like grid computing, distributed computing, parallel computing and so on. Due to the migration of web applications to Cloud Computing platform, the privacy of sensitive data belonging to the consumers of cloud services has raised alarms. Identity Management has become a vital problem associated with the handling and management of sensitive identity credentials in the Cloud Computing environment. Authentication (verifying a user's identity) is one of the part to give access to the right person and to secure the system, application, data, (any computing resource) etc. This paper outlines digital identity, identity management system features and services. It also focuses on different methods of authentication and authentication attacks. Finally, concludes with Multi-Layer Authentication must deliver the high power of security in the public cloud environment, where the diverse nature of data level.

Keywords - Biometric Authentication, Digital Identity, Multi-factor Authentication, One Time Password (OTP) and Personally Identifiable Identity (PII)

I.INTRODUCTION

Cloud Computing, *"*an evolution of grid computing*"* has emerged as a leading paradigm for managing and delivering internet-based services, which itself is based on traditional distributed system concepts (Youseff et al. 2008). Cloud Computing offers many benefits to the IT industry by offering them unlimited storage and computing capacity. In addition, Cloud Computing is built on pay-as-you-use model that allows organizations to outsource their data and IT services (Mahmood 2011; Wang and Mu 2011). While cost and simplicity (self-service without the intervention of service provider) are the key advantages of cloud, trust and security are the main considerations of Cloud Computing users.

The invention of Cloud Computing information is stored in the cloud instead of local system. In the web world, one must prove his/her credentials like username, password to get access to the service. Managing the amount of sensitive personal information revealed to any one has become more and more important in terms of personal security. Identity Management (IDM) is the key to Cloud privacy and security.

The goals of security paradigm include Confidentiality, Data-Integrity, Authenticity, Authorization, Non-Repudiation, Availability, Audit and Control [1], [2], [3]. Key security challenges for cloud applications include authentication, authorization, security of data at rest, security of data in motion, data integrity and auditing [4]. The first step towards securing a computing system is that the ability to verify the identity of users. In most cases, people are still using username, passwords for authentication (verification). People use short passwords than long passwords because of inconvenience in remembering the password; which leads to forget or using the same password for multiple sites.

II.IDENTITY MANAGEMENT SYSTEM

2.1 Definition

Digital identity is the "Representation of an entity (or group of entities) in the form of one or more information elements which allow the entity(s) to be uniquely recognised within a context to the extent that is necessary (for the relevant applications)" [5]. Though an entity can be any object, in most cases it is a personal identity of people rather than of any object. Personal Identifying or Personally Identifiable Information (PII), which is "the information pertaining to any living person which makes it possible to identify such individual (including the information capable of identifying a person when combined with other information even if the information does not clearly identify the person)" [6]. PII is simply the attributes of a person, such as: their hair colour, sound of their voice, height, name, qualifications, past actions, reputation, medical records, etc.

Identity Management is "A set of functions and capabilities (e.g. administration, management and maintenance, discovery, communication exchanges, correlation and binding, policy enforcement, authentication and assertions) used for the following:

- assurance of identity information (e.g., identifiers, credentials, attributes);
- assurance of the identity of an entity (e.g., users/subscribers, groups, user devices, organizations, network and service providers, network elements and objects, and virtual objects);
- and enabling business and security applications" [7].

An Identity management describes the management of individual identities, their authentication, authorization, roles, and privileges within or across system. An identity management system is the information system that can be used for Identity management [8].

The communication between users with IDMs and SPs are shown in Figure 1: [7]

1. Identity provider (IdP): IdP issues digital identities. First, IdP should put into practice services for users such as user registration, confirm truthfulness of user identity and user identity storage. Second, IdP must processes requirements from SP and users for authentication.

2. Service provider (SP): SP provides services to user/entities that have essential identities.

3. User/Entity: User is the consumer of SP and IdP. The only unique identity signifies the user. Anyone such as a

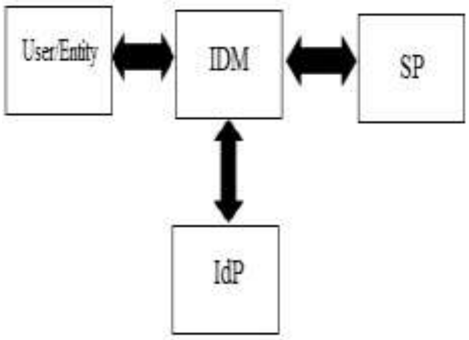

Fig 1: Identity Management System

public organization, a human, a virtual entity like software, and so on could be a User.

4. Identity Management (IDM): A trusted third party used to manage digital identities.

2.2 Functions

The goal of identity management is to improve productivity and security while lowering costs associated with managing users and their identities, attributes, and credentials. The identity management system stores information on all aspects of the identity management infrastructure. Using this information, it provides authorization, authentication, user registration and enrolment, password management, auditing, user self-service, central administration, and delegated administration.

2.3 Classification

Cloud Identity Management has to be characterized on the premise of their deployment architecture and functional behaviour [9].

2.3.1 Deployment based classification

This classification represents the primary architecture for the storage, management and flow of identity information. Isolated, centralized or federated identity management solutions are the instances of this category.

2.3.1.1 Isolated cloud IDMs

In Isolated cloud identity management system, only single server acts as a Service Provider as well as an Identity provider. Also, this single server deals with the storage of all the user’s credentials and all the user operations. There is no dependency on any third-party service for the credential issuance and verification.

2.3.1.2 Centralized cloud IDMs

In this kind of cloud identity management system, there is a separate identity provider for the storage, issuance and management of identity data. The only difference between isolated IDMs and Centralized IDMs is that it separates the functions of IdPs and SP.

2.3.1.3 Federated cloud IDMs

Federated cloud identity management is the realization of federated identity management model. In this model, multiple enterprises can use the same identification information for gaining the access to all the networks within a particular group of trusted enterprises. This identity management platform has received significant attention from the businesses because of its easy design that allows cross-domain access to its users that too without any need of creating additional user accounts.

2.3.2 Feature based classification of cloud IDMs

This category includes anonymous and user-centric identity management systems. These systems are entirely independent of underlying architecture.

2.3.2.1 User-Centric cloud based IDMs

In this type of cloud identity management platform, a user is the part of every identity provisioning transaction. In this kind of platform, CSC’s are responsible for the storage, management and retrieval of their personal identity information. In it CSCs are all responsible for every decision about the exchange of their identity credentials with other trusted third-party entities such as CSPs, IDPs or users. From the privacy point of view, User-centric IDMs consider user preferences prior to disclosing the identity information to the SPs.

2.3.2.2 Anonymous cloud IDMs

Anonymous identity management as the name refers offers anonymity as a feature in an identity management system. This anonymous identity management system is capable of keeping its entity(owner) secret from everyone else by assigning an anonymous identity to it. And this anonymous identity should be strong enough that make it hard to disclose the actual identity since data inferred may be connected with other information and can be reused.

2.4 Generic IDM Architecture

1. The steps involved in acquiring access to a SP are mentioned here:
2. The user login to the IDM provider with her pre-assigned username and password,
3. The user requests to access cloud application/data from the SP,
4. The SP asks for a token,
5. The user requests a token from the IDM provider,
6. The IDM provider generates a token and sends it to both the user and the SP,
7. The user forwards the token received from the IDM to the SP,
8. The SP compares the tokens received from the user and the IDM provider, and
9. On successful comparison, the cloud allows the user to access the requested data or application.

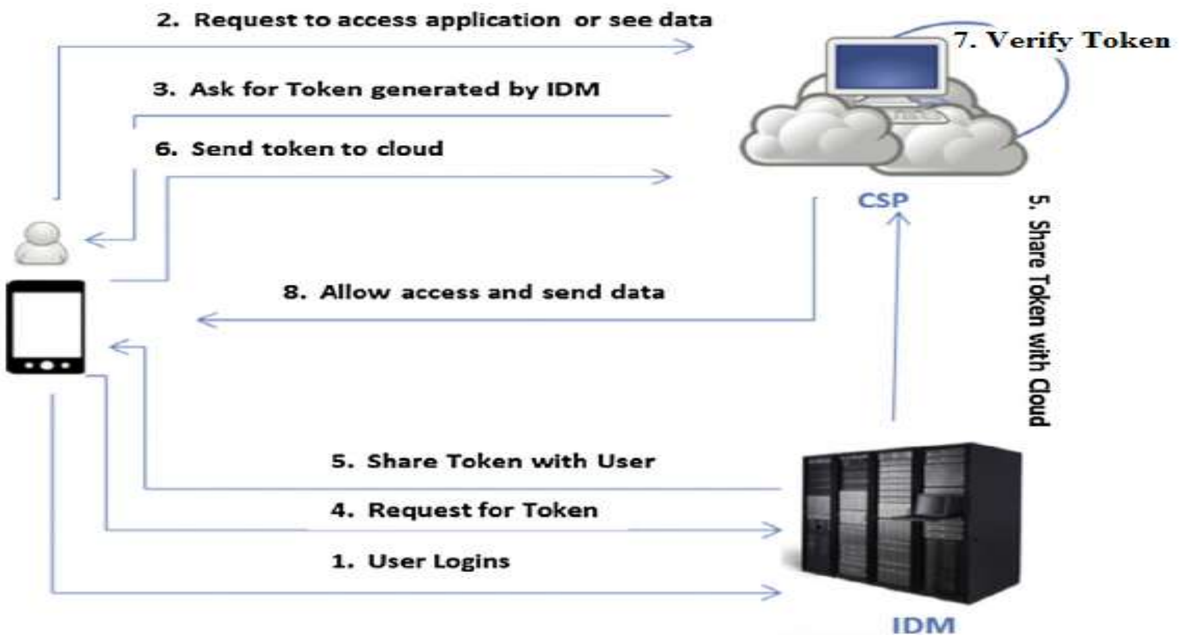
2. Request to access application or see data
7. Verify Token
3. Ask for Token generated by IDM
6. Send token to cloud
CSP
5. Share Token with Cloud
8. Allow access and send data
5. Share Token with User
4. Request for Token
1. User Logins
IDM

Fig 2: Generic IDM Architecture [10]

III. SECURITY AND PRIVACY CHALLENGES

Identity management is a broad domain that involves many open security issues and challenges including Openness, Identity Theft, Least Privileges, Elevated Privilege Control, Availability, Confidentiality, Integrity, Trust Management etc. Cloud Identity as a Service (IDaaS) is basically the management of identities in the cloud, outside the organizational boundary and applications that use them. The service is provided as third-party management of identity functions, including user life cycle management and single sign-on. Externalising any portion of identity management functions to third-party provider may raise several security and privacy challenges as well, which mainly includes identity, data locality, confidentiality, trust establishment, availability etc. [11].

Every enterprise will have its own identity management system to control access to information and computing resources. Privacy is a major concern to preserve the sensitive information (credit card number, identity information etc.) of the consumer. Such information can be retrieved by the unauthorized user who is following privacy issues like the lack of safety standards, unauthorized secondary storage, lack of user control and the unclear responsibility can be occurred [12].

In view of the major IDMs security issues of Cloud Computing, there are several solution measures like Authentication and Identity management, Trust management Framework, Active Directory (LDAP), SSO (Single Sign On) and SAML (Security Assertion Mark-up Language), Privacy manager for Cloud Computing, PRIME (Privacy and Identity Management for Europe), Open ID are available.

IV.AUTHENTICATION

4.1 Basics of Authentication

Authentication is defined as the way of verifying or confirming the digital identity of a user. Everyone should be familiar with the standard three-factor authentication such as something you know, something you have and something you are. [13]

- Something you know: It is specific, secret information, such as a password or an answer to a secret question which perhaps others do not know. These are knowledge factors.
- Something you have: It is an item that is owned, such as a smart card or similar hardware device. These are ownership factors.
- Something you are: It is a physical attribute like fingerprint or voice, which can be identified. These are inherence/ behavioral factors.

More than one combination of authenticators (knowledge + object / knowledge + id / object + id) improve the security level better. This is called *multi-factor authentication*. ATM card is the common example of multi-factor authentication. The combination of an ATM card and PIN – two- factor authentication – is a better choice than a card alone, as the card can be stolen and used.

4.2. Methods of Authentication

Where password-only authentication is not adequate for an application, a number of alternative methods can be used alone or in combination to increase the security of the authentication process. A variety of methods are available for performing authentication. They are Password Authentication, Lightweight Directory Access Protocol (LDAP) Authentication, Biometric Authentication, PKI Authentication, Security Token Authentication, Smart Card Authentication and Wireless Authentication.

4.2.1 Password Authentication

A password is an un-spaced sequence of characters familiar to confirm that a user requesting access to a computer system is actually an authorized person. Password Authentication Protocol (PAP) is a simple user authentication protocol that does not encrypt the data and sends the password and username to the authentication server as plain text. PAP is extremely prone to being read from the Point-to-Point Protocol (PPP) data packets exchanged between the authentication server and also the user's machine.

Recently, graphical password authentication is familiar by select images in a specific order which is presented in graphical user interface. It requires more space than text password. Also, the registration and log-on process take too much of time.

4.2.2 Lightweight Directory Access Protocol (LDAP) Authentication

The Light-weight Directory Access Protocol (LDAP) is a directory service protocol that relies on a layer above the TCP/IP stack. It provides a mechanism used to hook up with, search, and modify Internet directories.

4.2.3 Biometric Authentication

Biometric Authentication is any method that validates the identity of a user who needs to sign into a system by measuring some intrinsic characteristic of that user. Biometric samples include finger prints, retinal scans, face recognition, voice prints and even typing patterns.

4.2.4 PKI Authentication

A public key infrastructure (PKI) is a set of roles, policies, and procedures required to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption.

4.2.5 Security Token Authentication

A security token (known as an authentication token) is a small hardware device that the owner carries to authorize access to a network service. The device is also in the form of a smart card or may be embedded in a commonly used object such as a key fob.

4.2.6 Smart Card Authentication

The CCID (Chip Card Interface Device) is a Universal Serial Bus (USB) protocol that permits a *smartcard* to be connected to a Computer, using a standard USB interface. This enables the smartcard to be used as a security token for authentication and data encryption such as Bit locker.

4.2.7 Wireless Authentication

Wireless security is that the prevention of unauthorized access or damage to computers using wireless networks. The most common types of wireless security are Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA). WEP is a notoriously weak security standard.

4.3. Authentication Mechanism

Single Sign-on (SSO) enables the user to access multiple systems with one set of login credentials (evidence of authority, status, rights entitlement to privileges). SSO saves time spent in authenticating with different applications for the same identity.

Security Assertion Mark-up language (SAML) is an XML based open standard data format for exchanging security information between an identity provider and a service provider.

Kerberos is an open authentication protocol used for authenticating client to service that communicate over an un-secure network with mutual authentication.

One Time Password (OTP) is valid for single use for a single session or transaction. OTP tokens are more secure and frequently used in on-line payment. SMS is the most common delivery mode of it. Time based OTP algorithm is used for generating OTPs.

There are two main steps that examine the procedure of secure and reliable user authentication in cloud environments:

- Investigating unique identifiers of users during the initial registration phase.
- User authentication and validating user legal identities and acquiring their access control privileges for the cloud resources and services during the service operation phase. [15]

4.4 Authentication Attack

Heterogeneous environment and the devices like smart phone, laptop, PDA, desktop is used to access applications by the users. This leads to the significant requirements of security. Cloud service providers need to ensure that only legitimate user is accessing their services and this point out to the requirement of a strong user authentication mechanism. But there exist numerous attacks that can create loop holes in the authentication mechanism and hence identifying the most secure authentication mechanism is a big challenge in the cloud environment.

V. MULTI-FACTOR AUTHENTICATION

Fast IDentity On-Line (FIDO) [14] specifications help multifactor authentication (MFA) and public key cryptography. The gain of FIDO-compliant authentication is that the users do now not need to use complex passwords and / or undergo recovery campaigns once they forget about a password. FIDO stores personally identifiable information (PII) consisting of biometric authentication records locally at the user's tool. FIDO's local storage of biometrics and other personal identity is intended to smooth utilization of personal statistics stored on an external server within the cloud.

FIDO helps the Universal Authentication Framework (UAF) protocol and the Universal Second Factor (U2F) protocol. With UAF, the client tool creates a new key pair all through registration with an internet service and keeps the private key; the public key is registered with the online service. During authentication, the customer device proves ownership of the private key to the service, which entails a user–friendly action such as providing a fingerprint, entering a PIN or speaking into a microphone. With U2F, authentication requires a robust second factor which includes a Near Field Communication (NFC) tap or USB security token.

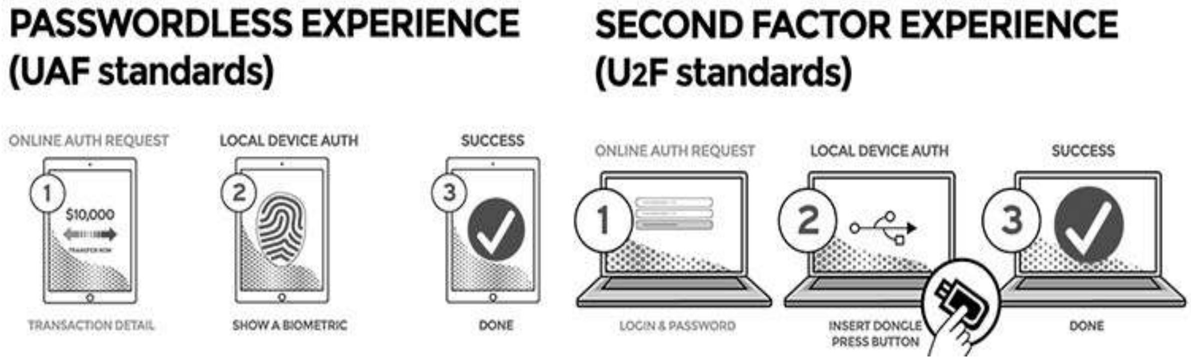

Fig 3: Fast IDentity On-line (FIDO)

VI. PROPOSED MULTI-LAYER AUTHENTICATION MODEL

In any application, one (user) should enrol or register or sign-up into the application by providing their personal information before getting access into it. Each user is allocated with role and permission for getting access to the resources. For this reason, the owner of the resources grouped the user with levels (User-level) according to their privileges. Also, the permission (access-rights) is given to the user according to the sensitivity of the actions like read/view, write/edit, delete, upload and download etc. This paper, introduces Multi-Layer authentication mechanism that provides better security in the Cloud environment to the user.

Usually, registration process is done by getting information from user like first name, last name, mail-id, phone number, date-of-birth etc. Input validation method is taken into account for better security during registration. Simultaneously, access-rights also assigned to the user according to the privileges. After registration, user can login and get access to the resources after authentication.

U = $\{g_0, g_1, g_2 \ldots g_n\}$ ----- Users are grouped into 0 – n levels.

F = $\{f_0, f_1, f_2 \ldots f_n\}$ ----- Functions like read, write, update, modify, delete etc.

P = {Grant, Denial} ----- Permission - Grant (give rights), Denial (cancel rights).

Multi-Layer Authentication (UFP) is proposed for better security that motivates the time saving concept while log-in. User personal identifiable information (PII), during registration is stored in Security Index Database (SID). Randomly selected information is given while log-in process instead of password. This Multi-Layer approach is described in the following:

Layer - 1

Step 1: Student select department and year. Simultaneously student can select their reg.no also.

Step 2: Every log-in randomized field (date-of-birth, mobile no, mail-id etc.) is given from SID instead of password.

Step 3: One Time Password (OTP), Captcha can be used for better security (optional).

After getting into the application all the users can view the details in the application. But submitting assignment, file download, copying/modifying content can be done in another layer of authentication approach.

Layer – 2

Bio-metric authentication like finger-print, voice recognition and photo verification are done in this layer. Location/Time/Session constraints are also included in this layer.

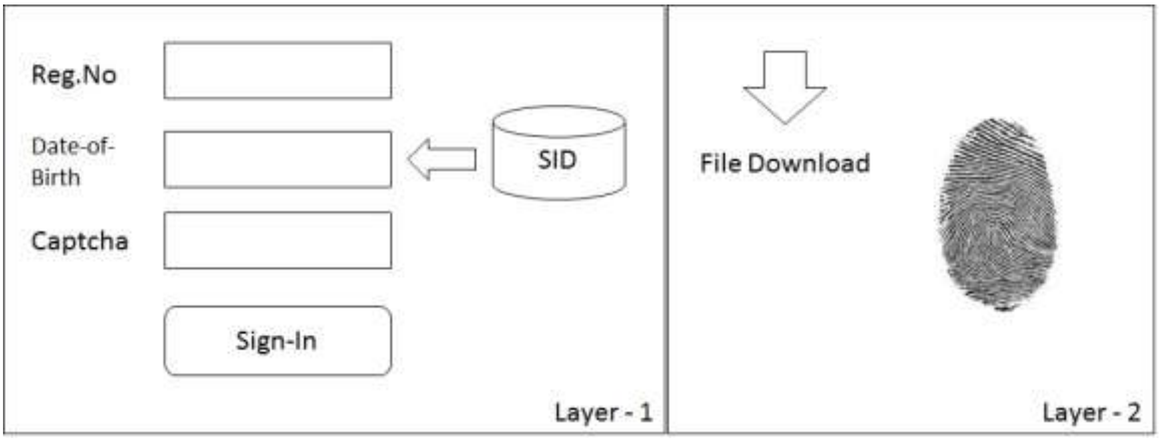

Fig 4: Multi-Layer Authentication

Hybrid Access model [16] which consists of combination of any two methods/ models like rule and role based access control ensures the security which can be implemented in Multi-level, Multi-phase and Multi-factor models for the security of data in Cloud environment. The basic components like user or group, function (process like read, write, upload, download, transfer, copy and alter), location, device, session, resource and permission are clearly defined depending upon the nature of the data/information (unclassified, confidential, secret and top secret).

Multi-Layer Authentication must deliver the high power of security in the public cloud environment, where the diverse nature of data level.

VII. CONCLUSION

This paper presents some essential process of Cloud Computing and the classification of Identity Management. It is the most significant thing to secure one's personal data as well as corporate sensitive information which travels from one data center to another without the user's knowledge. Authentication plays a significant role in information security in confirming identity proof to get system access. Despite of various mechanisms from vendor to vendor, multi-factor authentication can give more benefits to an enterprise. Along with password or PIN is the baseline authentication standard, there is other layers of security like USB tokens.

A unified security model for a typical cloud infrastructure is under research. We suggest a framework to enhance confidentiality in Cloud environment by using Authentication, Access Control and Auditing (AAA). This Hybrid Multi-Layer Access Control (HMLAC) model is focused to strengthen Cloud security.

VIII.ACKNOWLEDGEMENT

I take this privilege to express my gratitude and respect to the Principal, Management of Mannar Thirumalai Naicker College, Bharathiar University and my special thanks to my Supervisor.

REFERENCES

[1] Chauhan N.S. and Saxena. S, “Energy Analysis of Security for Cloud Application,” in Proc. Annual IEEE India Conference, pp. 1-6, 2011.

[2] Liu W., “Research on Cloud Computing Security Problem and Strategy,” in Proc. IEEE 2nd Int. Conference on Consumer Electronics, Communications and Networks, pp. 1216-1219, 2012.

[3] Yu. X and Wen Q, “A view about Cloud data security from data life cycle, (2010),” in Proc. IEEE Int. Conference on Computational Intelligence and Software Engineering, pp. 1-4, 2010.

[4] Arshdeep Bahga, Vijay Madisetti, “Cloud computing”, Universities Press, New Delhi.

[5] ITU-T. “Baseline capabilities for enhanced global identity management trust and interoperability”. Draft New Recommendation ITU-T X.1250 (X.idmreq), Feb 2009.

[6] ITU-T. “NGN identity management framework”, Recommendation Y.2720.

[7] Ardi BENUSI, “An Identity Management Survey”, International Journal of Computing and Optimization, Vol. 1, Issue no. 2, pp.63-71, 2014.

[8] Rizwana Shaikh, M Sasikumar, “Identity Management in Cloud Computing”, International Journal of Computer Applications (0975 –8887), Volume 63, Issue No.11, pp.17, February 2013.

[9] Prof.Hiral M. Patel, Sweetyben Vishnukumar Patel, “An Analysis of Identity Management in Cloud Computing”, International Journal of Innovative Research in Computer and Communication Engineering Vol. 4, Issue 6, June 2016 ISSN(Online): 2320-9801.

[10] Issa Khalil, Abdallah Khreishah, Muhammad Azeem, “Consolidated Identity Management System for secure mobile Cloud Computing”, Computer Networks, Elsevier, vol. 65, pp. 99–110,2014.

[11]. Prabhusekar A.M., “Cloud Identity Management Security Issues and Countermeasures”, International Conference on Explorations and Innovations in Engineering & Technology (ICEIET – 2016, ISSN: 2348 – 8387) pp. 192-195.

[12] Smita Saini, Deep Mann “Identity Management issues in Cloud Computing”, International Journal of Computer Trends and Technology (IJCTT) – Vol 9 No 8 – Mar 2014.

[13] Dwiti Pandya, Khushboo Ram Narayan, Sneha Thakkar, “An Overview of Various Authentication Methods and Protocols”, International Journal of Computer Applications (0975 – 8887) Volume 131 – No.9, December 2015.

[14] http://searchsecurity.techtarget.com/definition/FIDO-Fast-Identity-Online.

[15] Fatemi Moghaddam F, Gerayeli Moghaddam S, Rouzbeh S, Kohpayeh Araghi S, Morad Alibeigi N and Dabbaghi Varnosfaderani S, “A Scalable and Efficient User Authentication Scheme for Cloud Computing Environments,” in Proc. of IEEE Region 10 Symposium, 2014, pp. 508–513.

[16] Anuratha. K, Dr. Ganagadurga. M, “Analysis of Data Security in Cloud Computing Using Access Control Technique”, International Conference on Global Talent Management in the Digital Era, ISBN: 978-93-86537-95-9, September, 2017.