ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

An Analysis of Identity Management in Cloud Computing

Prof. Hiral M. Patel, Sweetyben Vishnukumar Patel

Assistant Professor, Dept. of Computer Engineering, SPCE, Sankalchand Patel University, Visnagar, Gujarat, India

Master of Engineering Student, Government Engineering College, Gandhinagar, Sector 28, Gujarat, India

ABSTRACT: The Cloud computing Concept has achieved much more popularity now-a- days because of its capability to provide extremely scalable resources at economical rates. Regardless of the very striking features that Cloud promises, the speed of journey towards Cloud is moderately slow, mainly because of the innate security challenges associated with this technology. Identity Management has become a very vital issue related to the handling and management of sensitive identity credentials in the cloud computing environment, where cloud providers have to control usernames, passwords and other information used to identify, authenticate and authorize users. In this paper, we have analyzed Cloud IDMSs to better be aware of the general as well as the security aspects .From the security viewpoint, we present a comprehensive list of attacks that occur frequently in Cloud based IDMSs . Comparisons of Identity Management paradigms and models have been also presented.

KEYWORDS: cloud computing, identity, identity management (IDM), service provider (SP)

I. Introduction

Due to innovation of cloud computing technology, novel and prominent exemplar for organizing and delivering internet oriented services comes into way of life. A cloud user provides sensitive personal information as Credentials to the service provider to prove correctness of their identity while using online services.

Handing sensitive data to cloud service provider is a serious security concern for the cloud user to trust on a cloud provider as well as it is crucial from cloud service provider's view point in achieving reliance from cloud users. Therefore IDM is come forward as a key to protect users' identities and hence providing cloud privacy and security but IDM in cloud is more complex than in traditional web-based systems since the users hold multiple accounts with different SPs or with a single SP [2]. In this paper different IDMs are analysed. Cloud based Identity Management Systems (IDMSs) differ from the traditional IDMSs in that they require dynamic governance of provisioning, de-provisioning, synchronization, entitlement, scalability and access control[3].

This paper is structured as follows: in section 2 depict center concepts of identity, Generic IDM architecture ,Current Technologies used to implement IDM with their strengths and limitations and Cloud identity as a service; section 3 discusses Identity Life Cycle Management; section 4 describes and Classification of identity management systems; section 5 represent the models of IDM;section 6 depict Comparison of IDM Models and Section 7 presents the conclusion.

II. Centre Concepts of Identity Management

1What is Identity management?

- An identity is a set of unique characteristics of an entity: an individual, a subject, or an object. A given identity may consist of one or more attribute(s).
- An identity used for identification purposes is called an identifier [4]. Identity has been defined as 'the distinct character or personality of an individual. Consists of traits, attributes, and preferences upon which one may receive personalized services [5].

DOI: 10.15680/IJIRCCE.2016. 0406246

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 [6]. The communication between users with IDMs and SPs is shown in Figure 1:

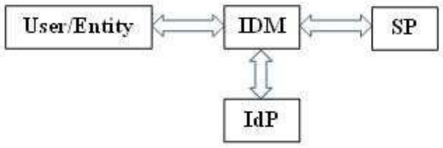

Figure 1 Identity Management System [7]

1) Identity provider (IdP): It issues digital identities. IdP essentially has to do two tasks, first it should put into practice services for users such as user registration, confirm truthfulness of user identity and user identity storage. Second, IdP must process requirements from SP and users for authentication.

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

3) User/Entity: User is the client of both SP and IdP. User must have a legal identity if it wants to use services. User could be a public organization, a human, a virtual entity like software, and so on. The only unique identity represents the user.

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

2. Generic IDM Architecture

The steps involved in acquiring access to a SP are mentioned here:

(1) The user login to the IDM provider with her pre-assigned username and password,
(2) The user requests to access cloud application/data from the SP,
(3) The SP asks for a token,
(4) The user requests a token from the IDM provider,
(5) The IDM provider generates a token and sends it to both the user and the SP,
(6) The user forwards the token received from the IDM to the SP,
(7) The SP compares the tokens received from the user and the IDM provider, and
(8) On successful comparison, the cloud allows the user to access the requested data or application [19].

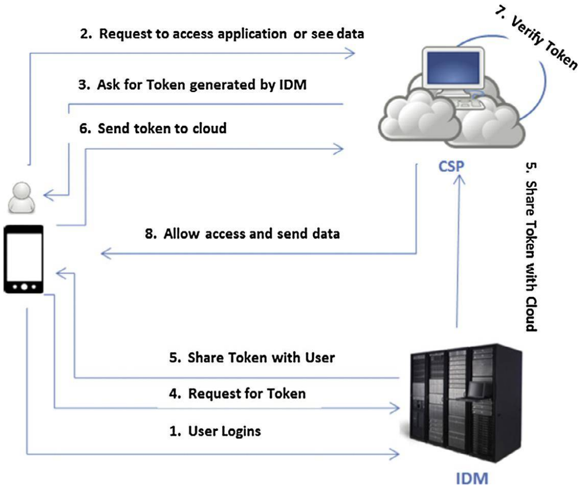
2. Request to access application or see data
7. Verify Token
3. Ask for Token generated by IDM
6. Send token to cloud
CSP
5. Share Token with Cloud
8. Allow access and send data
5. Share Token with User
4. Request for Token
1. User Logins
IDM

Figure 2: Generic IDM Architecture [19]

3 Current Technologies Used for IDM with their Strength and Limitation

Many technologies used for implementing IDM are Active Directory, Single sign-on(SSO), Security Assertion Mark-up Language(SAML), OpenID, Privacy and Identity Management for Europe(PRIME). Following Table 1 describes and list out limitations of each technology used to implement IDM.

Sr No.	Technology	Description	Strength	Limitation
1	**Active Directory**	-It is a directory service discovered by Microsoft for Windows domain networks that provides a strong set of capabilities to manage users and groups. It helps secure access to on-premises and cloud applications.	-It makes the task of network administration simpler by maintaining a central repository of information. -It provides a single destination to look out for information. -Highly secured access to data through the usage of security policies. Thereby it improves the management of data. -Easily scalable.	-increases the daily IT workload. -encourages bad behaviour and increases security risks
2	**SSO**	-SSO requires that users need to remember only one set of authentication credentials. - a user have to authenticate himself to a service one time and does not require to authentication again for other services of the system linked by the SSO framework.	-having only one set of credentials -It reduces clerical overhead in resetting forgotten passwords over multiple platforms and applications. -It reduces the time taken by users to log into multiple applications and platforms.	-Since user does not need to sign-in each time it access a new application. Then, anyone can use the first login and access any of the user's apps. -If the central account database is breached, an attacker would have access to multiple systems at once. -There is a single point of failure.
3	**SAML**	-It is an open standard protocol used to exchange authentication and authorization data between two different security domains which does not require password. Instead of password, application that use SAML, accepts secure tokens which only reveal what is needed to gain access to applications. When user access applications or secure content at the Service provider, the IDP generates a secure token to be sent to SP. The token grants accesses to applications and content, but does not pass any information that can be used by anyone else to access them[8]	-Platform neutrality -Loose coupling of directories/databases -Improved online experience for end users -Reduced administrative costs for service providers -Risk transference	-XML Signature Wrapping Attack[9] -In wrapping attack, the attacker attempt to insert the malevolent part in to message structure in Transport Layer Service(TLS) and after insertion, the forged content of the message is copied into the server and while executing, cloud server working is interrupted by the Attacker.
4	**OpenID**	-OpenID [11,12] is an open,	Its major advantages of are:	-suffers from “phishing

		decentralized, free framework for user centric digital identity management. -With Open ID multiple digital identities are controlled with a single username and password called OpenID. -user interacts with an relying parties that provides way to specify an OpenID for the authentication. -The user has formerly registered an OpenID with an OpenID provider (a TTP). -Upon being discovered by the RP, the OpenID provider authenticates and asks the user whether the RP should be trusted to receive the necessary identity details for the service. -If user accepts, then redirection to the relying party along with user identification, which need to be confirmed by the RP to provide service.	1. Highly distributed 2.Flexible -users can keep identity even when identity provider disappears by using delegation with their homepage URI as identity to different identity providers 3.Lightweight solution	attacks “[13]. –A malicious attack can be easily set up to attract users into entering their authentication information at a website that pretences as an OpenID provider website.
5	**PRIME**	-Privacy and Identity Management for Europe (PRIME) [10] provides privacy-preserving authentication using anonymous credentials. -The user-side component uses protocols for getting third party (IdP) endorsements for claims to relying parties. - Anonymous credentials are provided using an identity mixer protocol that allows users to selectively expose any of their attributes in credentials obtained from IdP, without enlightening any of their information. -The credentials are then digitally signed using a public key infrastructure.	-No Need to reveal all information for identity.	A major limitation of PRIME is that it requires both user agents and SPs to implement the PRIME middleware, which obstruct standardization.

Table 1: IDM Strength and Limitation

4 Cloud identity as a service: IdaaS

Cloud Identity as a Service (IDaaS) is fundamentally the management of identities in the cloud, exterior to the organizational periphery 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. The terms IDaaS is quite wide, and covers all service layers of Cloud computing including software, platform, or infrastructure; and for together public and private clouds. Hybrid solutions may also exist, whereby identities can still be managed internally within an organization, while other mechanism like authentication, authorization etc. are externalized through Service Oriented Architecture (SOA). IDaaS moreover providing desired identity management services offers all of the Cloud benefits as well, including reduced hardware cost, easy management with wide range of integration options etc[14,15]. Due to this cause most of the organizations are moving their existing enterprise IDMSs to Cloud based services.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

III.IDENTITY LIFE CYCLE MANAGEMENT

Figure 3 shows the lifecycle of identity management in a cloud computing environment. These tasks are performed by two basic components: provision and administration. Provision components manage identities and user profile information while administrative component mainly handles access management [16].

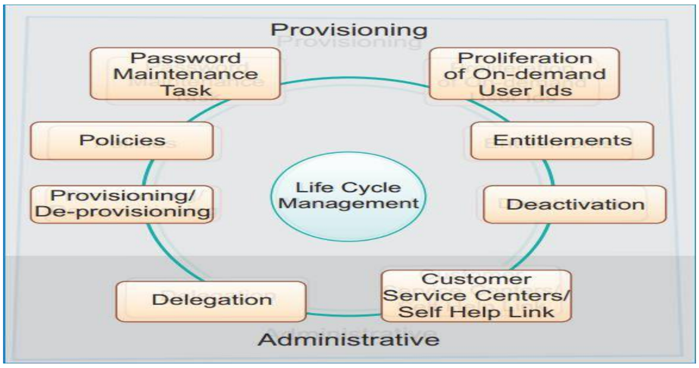
Provisioning
Password Maintenance Task
Proliferation of On-demand User Ids
Policies
Entitlements
Life Cycle Management
Provisioning/ De-provisioning
Deactivation
Delegation
Customer Service Centers/ Self Help Link
Administrative

Figure 3: Identity Lifecycle Management [17]

An identity manager is supposed to have the subsequent capacity to deliver identity services in cloud computing [18]:

- **Identity provisioning/de-provisioning**: An identity manager should be able to assign and repeal the identity of an entity in the cloud in a secure and just-in-time manner.
- **Authentication:** This is the process of verify the fact of an argue an entity makes about an identity.
- **Authorization and Entitlement:** Entitlements are a set of attributes which specify the access rights of an entity. Authorization uses these attributes to conform or refuse a request.

After identity is established, and procedures are defined, Identity Lifecycle Management should be specified. Identity Lifecycle Management is the process of managing accounts, policy changes, and entitlement, and tracking policy compliance. It includes the following features:

Work flow: Steps in identity lifecycle management should be automated in order to decrease administrative efficiency and reduce security risks by reducing human interference.

- **Delegation:** Delegation is the process of granting permission to an application or entity to carry out certain tasks in the future. Delegation is necessary in cloud as the majority of tasks and processes are volatile and short-lived.
- **Entitlement:** Access control attributes should be clearly defined.

IV.CLASSIFICATION OF IDENTITY MANAGEMENT SYSTEMS

Various Cloud identity management solutions exist and in order to highlight their strengths, weaknesses and suitability for Cloud, we have characterized them on the basis of their deployment architecture and functional behaviour. Figure 4 presents the classification of identity management systems followed by a brief description for each of these systems [1].

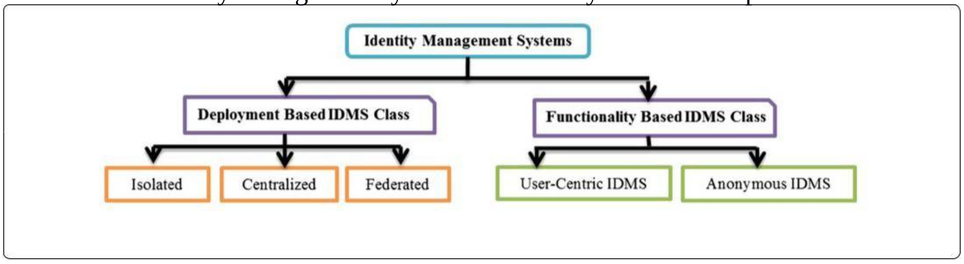
Identity Management Systems
Deployment Based IDMS Class
Functionality Based IDMS Class
Isolated
Centralized
Federated
User-Centric IDMS
Anonymous IDMS

Figure 4: Classification Of Identity Management systems [1]

DOI: 10.15680/IJIRCCE.2016. 0406246

V. Models of IDM

Deployment Based IDMS:

- **Isolated Identity Management Systems.**
  The isolated model is on the whole the simplest identity model. In isolated model, SP plays the role of both service provider and identity provider that means identification and authentication are directly done at the service provider. Other tasks of the identity management system like creating, maintaining and deleting identities can only be handled by this specific service provider. If a user wants to access services of any more service provider then it needs to register at the new service provider's identity management system yet again. This necessitate that every individual service provider has to store up and preserve the identity data and credentials of the user independently [20]. This identity management system does not depend on a Trusted Third Party for the credential issuance and verification.
  With the explosive growth of online services, users have to deal with more and more identities information. More and more credentials such as usernames and passwords should be managed properly by users. This approach increases security risks, as users often choose the same password for all their accounts.

- **Centralized Identity Management Systems.**
  In this model, user identity storage and user authentication is both implemented in the same servers called IdP. But unlike isolated model, this model detaches functions of SP and IdP. SPs don't store user identities locally, instead every identity is sent to the centre IdP intended for storage and following authentication. All SPs use the global unique IdP. when the SP need to authenticate an user, it will send the user information to the IdP to finish the process.
  This model is appropriate for the requirements of managing a bundle of users, but it has many short -comes, stock up all identities in single IdP typically gets the adversity of privacy and security. It can't support user privilege allocation and cross domain access as well.

- **Federated Identity Management Systems.**
  To eradicate credential redundancy and prevent disjointed login, a new approach for federating identity management of service providers has been anticipated. Federation can be defined as the set of agreements, standards and technologies that enable a group of SPs to recognize user identities from other SPs with in a federated trust domain [21]. In this model identity data are not stored in a central storage area but are rather stored scattered across different identity and/or service providers. The distributed identity data of a particular user are connected with a common identifier. Every identity provider and service provider, which are involved in such a federation, share a common trust relationship amongst each other. Once the user authenticates to an IdP, it need not have to execute the authentication procedure again when accessing another SP within the circle of trust in the current working session [16].

Functionality Based IDMS :

- **User-Centric Identity Management Systems.**
  In user-centric model all identity data are stored directly in the user's domain like on a secure token such as a smart card. The most important benefit of the model is with the intention of the user always remains the owner of his/her identity data and stays under their full control [23]. Identity data can only be transferred by an identity provider to a service provider if the user explicitly provides his/her approval to do so. Compared to the central model, this tremendously increases users' privacy.

- **Anonymous Identity Management Systems.**
  Identity management systems that put forward anonymity as a characteristic is termed as an anonymous identity management system. An Anonymous identity management system is proficient of keeping its entity top secret from everyone else [24, 25, 26].Anonymous identity should be well-built enough to make it hard, if not impractical, to expose real identity because data inferred ultimately may be coupled with other information and can be republished [24, 25]. However, anonymous identity management as well has several weaknesses, such as not have faith between user and SP.

VI. COMPARISON OF IDM MODELS

The Comparative analysis of deployment based various IDM models depends on the individual criteria like number of service providers and Identity providers require, kind of service provided by models, whether access to other domain allowed or not, where the identity information stored, whether user having control on identity, type of privacy, single sign on present or not, cost effectiveness, scalability and extensibility is clearly mentioned.

In the following we discuss the various models based on the individual criteria.

Number of SPs: In Isolated Model SP and Idp are the same body, the identity provider can only serve one service where as other model have multiple service providers.

Number of IdP: Only federated models are able to deal with various connected identity providers. Whereas others just include one identity provider.

Number of Trust domains: The federated models support authentication across multiple trust domains, whereas others support authentication in single domains only.

Service Type: Isolated model provides service solely, whereas centralized model offers multiple services but within single domain and Federated models provides multiple services in different domains.

Access to Cross Domain: Federated model can have access to other domain, whereas others do not having such type of access.

Identity Storage Location: identity data are stored at service provider in isolated model and in centralized model identity data are stored at cloud identity provider, whereas federated model stores identity data on both SP and Idp.

User Control on Identity: User does not having any kind of control on identity in isolated model, whereas remanning two models have it.

Privacy Protection: Isolated model nearly has no privacy protection, centralized model has some mechanisms in privacy protection but not that strong whereas federated model provides strong privacy protection mechanisms.

SSO: All models that can handle multiple service providers are primarily applicable to support single sign-on.

Scalability: The Centralized Model has the lowest scalability, as an external identity provider is usually not designed for dealing with high load activities. Whereas in isolated model an external identity provider has not that flexibility or elasticity that an identity provider deployed in a cloud has. Hence, we rated it with medium level scalability. While in federated model can additionally be distributed to other identity providers and thus achieve the highest scalability

Extensibility: The Isolated Model can't be extended because service provider and identity provider are the same entity. The Centralized Model can be ex-tended to integrate additional service providers. Nevertheless, the federated model has the best extensibility because of its support to multiple service providers and identity providers.

Cost: The Federated models have the highest cost effectiveness because multiple identity providers can be connected and re-used. Due to the reuse of existing external identity providers, costs can be saved. Whereas all other models have medium cost effectiveness, as the identity provider is set up in the cloud but no existing identity providers can be re-used.

Model	Number Of SP	Number Of IdP	Number Of Trust domains	Service Type	Access to Cross Domain	Identity Storage Location	User Control on Identity	Privacy Protection	SSO	Scalability	Extensibility	Cost
Isolated	One SP is IdP	One IdP is SP	One	Solely	No	SP	No	Weak	No	Medium	Low	Medium
Centralized	Multiple	One	One	Multiple services but in one domain	No	IdP	Yes	Weak	Yes	Low	Medium	Medium
Federated	Multiple	Multiple	Multiple	Multiple services form different domains	Yes	SPs as well as IdPs	Yes	Strong	Yes	High	High	High

Table 2: Comparative Analysis Of IDM Models

VII. CONCLUSION

This paper represents the core concepts pertaining to identity, identity management and summarizes the current technologies used for IDM by listing out strength and limitations. Identity management issue is critical for cloud computing environment and has turn into burning spot of research. Various identity management systems are discussed and analyzed by considering various parameters. Nevertheless, the effort done in this area of cloud computing is yet in its embryonic stage, and the upcoming extent of effort will be towards developing a framework for an even improved Identity management in cloud computing.

REFERENCES

1. Habiba et al.," Cloud identity management security issues & solutions: a taxonomy. Complex Adaptive Systems Modeling", doi:10.1186/s40294-014-0005-9,vol.2,Issue No.5,2014.
2. P. Angin, B. Bhargava, R. Ranchal, N. Singh, L. Ben Othmane, L. Lilien, M. Linderman, "An Entity-Centric Approach for Privacy and Identity Management in Cloud Computing", 29th IEEE Symposium on Reliable Distributed Systems, 2010.
3. Gopalakrishnan A," Cloud computing identity management",SETLabs Briefings,vol.7,pp.45–54., 2009.
4. S. Rieger, "User-Centric Identity Management in Heterogeneous Federations", Fourth International Conference on Internet and Web Applications and Services, 2009.
5. T. E. Maliki, J.Seigneur, "A Survey of User-centric Identity Management Technologies," In International Conference on Emerging Security Information, Systems and Technologies, Valencia, 2007.
6. Rizwana Shaikh, M Sasikumar," Identity Management in Cloud Computing",In International Journal of Computer Applications (0975 – 8887), Volume 63,Issue No.11,pp.17, February 2013.
7. Ardi BENUSI," An Identity Management Survey ",In Int. Journal of Computing and Optimization,Vol. 1, Issue no. 2,pp.63-71, 2014.
8. J. Hughes, E. Maler, "Security Assertion Markup Language (SAML)", V.2.0 Technical Overview, http://www.oasis-open.org/committees/documents.php?wg_abbrev=security,2005.
9. Pawel Krawczyk, "Secure SAML validation to prevent XML signature wrapping attacks", Open Web Application Security Project(OWASP).
10. S. Fischer-Hubner, and H. Hebdom," PRIME - Privacy and Identity Management for Europe", accessed in Aug. 2010.
11. P.Angin,B.Bhargava,R.Ranchal,N.Singh,M.Lin derman,L.B.Othmane,L.Lilien,"An Entity-centric Approach for Privacy and Identity Management in Cloud Computing",29th IEEE International Symposium on Reliable Distributed Systems,2010.
12. T.A. Johansen,Ivar Jorstad,D.van Thanh,"Identity managment in mobile ubiquitous environments",The Third International Conference on Internet Monitoring and Protection,2008.
13. C. Sample and D. Kelley,"Cloud Computing Security: Routing and DNS Threats", http://www.securitycurve.com/wordpress/,2009.
14. Rimal BP, Choi E, Lumb I, "A taxonomy and survey of cloud computing systems", In INC, IMS and IDC NCM'09 Fifth International Joint Conference on.Piscataway, New Jersey, United States, IEEE,pp.44–51, 2009.
15. Subashini S, Kavitha V," A survey on security issues in service delivery models of cloud computing", J Netw Comput Appl ,Elsevier ,vol. 34,pp.1–11,2011,.
16. Mohammad Sadegh Faraji," Identity and Access Management in Multi-tier Cloud Infrastructure", A thesis, Graduate Department of Electrical and Computer Engineering, University of Toronto
17. Anu Gopalakrishnan.,"Cloud Computing Identity Management.",SETLabs Briengs, vol.7,pp.7-45, 2009.
18. Antonio Celesti, Francesco Tusa, Massimo Villari, and Antonio Pulia to," Three-phase cross-cloud federation model: The cloud sso authentication", In Advances in Future Internet (AFIN), Second International Conference ,IEEE, pp. 94-101,2010.
19. Issa Khalil, Abdallah Khreishah , Muhammad Azeem," Consolidated Identity Management System for secure mobile cloud computing", in Computer Networks,Elsevier,vol. 65,pp. 99–110,2014
20. Jøsang, A. and Pope, S.," User centric identity man-agement", AusCERT, 2005.
21. Federated identity, http://en.wikipedia.org/wiki/Federated_identity
22. Cao, Y. and Yang, L.," A survey of Identity Manage-ment technology", IEEE ICITIS 2010, pp. 287– 293,2010.
23. Dbrowski, M. and Pacyna, P.," Overview of Iden-tity Management.", Technical report, chinacommunications.cn,2008.
24. Bhargav-Spantzel A, Camenisch J, Gross T, Sommer D,"User centricity: a taxonomy and open issues", J Comput Secur 2007, IOS Press vol.15,pp.493–527, 2007.
25. Conrado C, Kamperman F, Schrijen GJ, Jonker W," Privacy in an identity-based DRM system", Proceedings of Database and Expert Systems Applications, 2003, 14th International Workshop on Piscataway, New Jersey, United States, IEEE,pp.389–395,2003.
26. McCallister E," Guide to Protecting the Confidentiality of Personally Identifiable Information", Collingdale, PA, United States,Diane Publishing, 2010.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

BIOGRAPHY

Hiral M. Patel is an Assistant Professor in the CE Department Of Sankalchand patel college of Engineering since 2005. She received Bachelor of Engineering degree in 2004 from CKPCET, Surat, and Gujarat. Her area of interest are Data Structure and algorithms, Cloud Computing, Big Data Analytics , Compiler Design, Operating Systems etc.

Sweety V. Patel is a Master of engineering student at government engineering college, gandhinagar, Gujarat. She received Bachelor of Engineering degree in 2012 from UVPCE, Kherva, Gujarat Her area of interest are operating system ,data mining ,cloud computing, computer networks etc.

DOI: 10.15680/IJIRCCE.2016. 0406246