Improving Identity Management on Cloud Computing using Upgraded Claim Based Method

Ravina Mangukiya[1], Gayatri Jain[2]
Department of Computer Engineering
[1, 2] LJIET, Gujarat, India

Abstract-*Cloud computing is the next stage in evolution of the Internet. The cloud in cloud computing provides the means through which everything — from computing power to computing infrastructure, applications, business processes to personal collaboration- can be delivered to you as a service wherever and whenever you need[1], but data preserve on cloud has several issues of security. So, Identity Management is way achieve end to end encryption, and also giving various functionalities like security management, authentication, encryption, data storage/manage, using that type of encryption method we can avoid data tampering, virtualization attack, account and password sniffing/phishing attacks etc. In this Paper, we propose various type models of Identity management that improve security issues in cloud web services.*

Keywords- Cloud Computing, Identity Management, Cloud Web Services, Encryption algorithms.

I. INTRODUCTION

Cloud computing is architecture for facilitating convenient, on demand network access to a shared pool of configurable computing resources. Those all resources are consist various network, servers, storages, applications and services that are rapidly provisioned and released with minimal management effort or clouds services provider interaction.

Figure 1. Cloud Computing [8]

Cloud computing also having some potential to enhance availability, accountability, scalability that all provide economic environment through optimization and efficiency in computing. In other word it can be define as remote server maintained by third party. All web applications like email,web conferencing, customer relationship management, businessman, data outsourcing and so many things can happen on cloud platform. One of the major problem faced during development of cloud computing technology is security issues. Client put their data on cloud but using various techniques client's personal data can be decrypted. So, in this paper it conclude various type of techniques that describe how to protect user's personal information and data can be secured. Using Identity management and various factor we provide more secure environment on cloud.

The paper is organized as follows. In next section description about Identity and Access management Control. In section 3, Survey of existing techniques and tools. In section 4, proposed Identity authentication is given. In section 5, scheme comparison is given. Finally we conclude our paper in section 5.

II. IDENTITY AND ACCESS MANAGEMENT

Identity as a Service (IDaaS) is the management of identities of the users in the cloud by third party vendors. IDaaS providers other than the organizations in identity management lead to challenges like, identity data locality, confidentiality, trust establishment, availability it also enable security system for accessing cloud application. In other word, Identity management System is use for providing security of user access, managing users, credential verification and check whether it is right person are access resource provider. Authentication of user are perform in different ways like username, password, biometric, token based or certificate based. Identity Management provide various functionalities and benefits like user attribute management, identity provisioning, audit and reports, password management, service account management, SSO and so on.

As well as Access management also providing some features like resource and roll mapping, work flow management, access governances etc.

III. SURVEY ON EXISTING TECHNIQUES AND TOOLS

Federated identity management assist in the administration of access to services and privacy of Personally Identifiable Information (PII). The cloud may impose some security issues, especially some threats to sensitive data such as PII. Therefore, we present a model that addresses privacy issues of PII, considering aspects of dynamic federations, different policies, data manipulation rules and encryption. Here we show various type of privacy features like, Transparency, Controllability, Minimization, Accountability, Data quality, User-friendly, Trust. Here, we show IDM model and sticky policies used for improving security. The flow comprises dynamic environments where thousands of users in different administrative domains interact through IdM. However, access control must be performed through a federated IdM system that considers preferences and access profiles of different users.

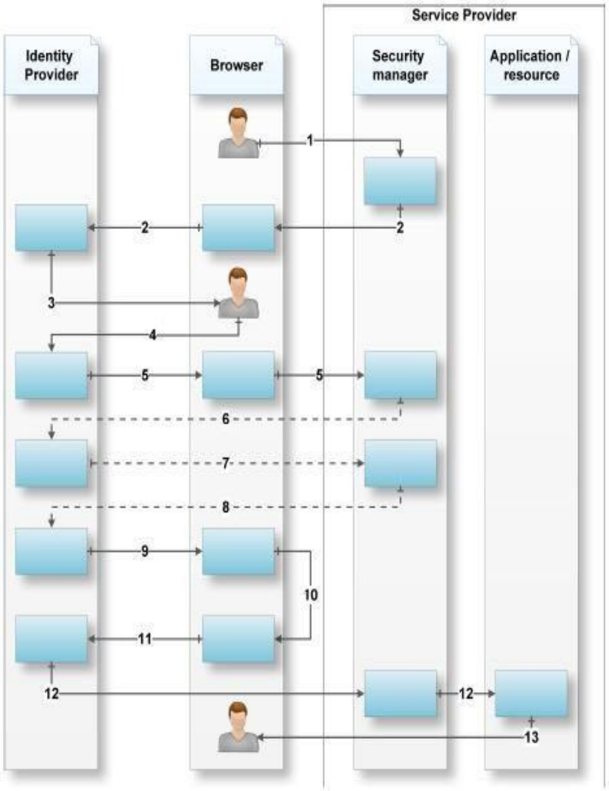


Figure 2. Adaptation of current federated identity management tools [2]

We propose that users encrypt attributes before sending them to the IdP, being able to choose only some of the attributes to be encrypted. The system maintains a recommendation to cipher all personally identifiable information. We define personally identifiable information as a set of basic attributes (name, email, identity documents, credit card numbers, telephone number and address).Also we obtain Adaptation of current federated identity management tools [2].

Decentralized system having several features like this system stores data on cloud in encrypted format, system modules manages to hide user identity from cloud. This system is decentralized one and hence divided into modules having different functionalities. System is solution for the bottle neck areas like multi user management on cloud, encrypted data on cloud, searchable encrypted data, data access protocols, user authentication by hiding his identity.

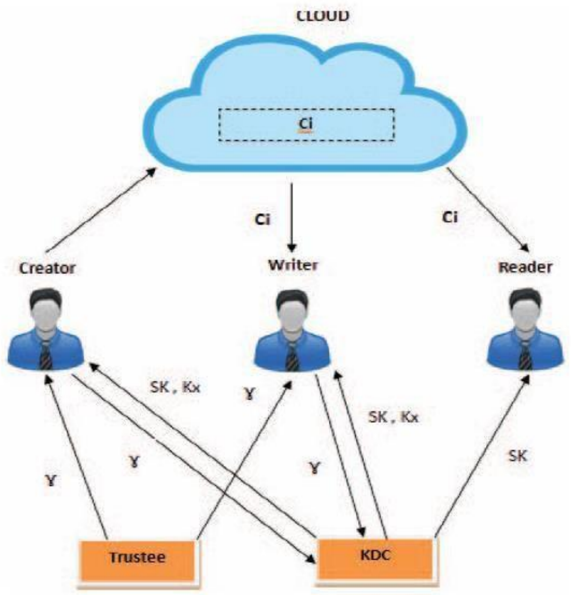
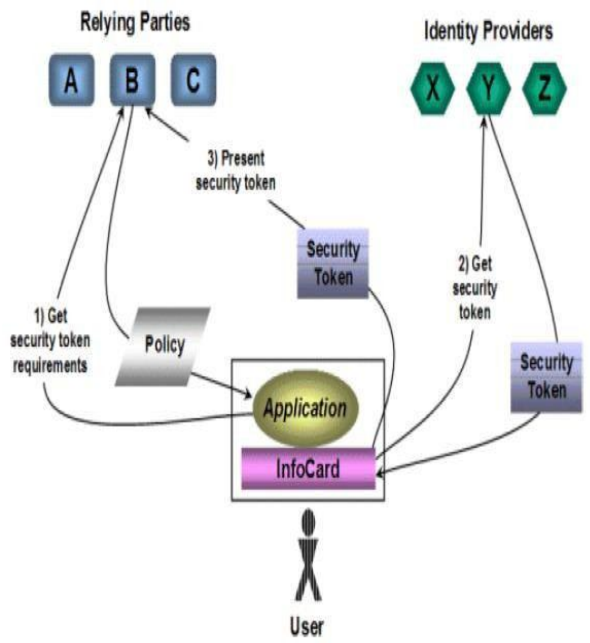


Figure 3. System Diagram [3]

Also this system effectively manages user revocation. A single KDC is not only a single point of failure but difficult to maintain because of the large number of users that are supported in a cloud environment. We, therefore, emphasize that clouds should take a decentralized approach while distributing secret keys and attributes to users. It is also quite natural for clouds to have many KDCs in different locations in the world.

Using decentralized system information and execution rights are distributed over these several modules hence data tampering is avoided [3].

Using Cloud platform user feels unsafe about disclosing their identity on the Cloud environment because their information may be used with other application/users to generate knowledge about their activities.

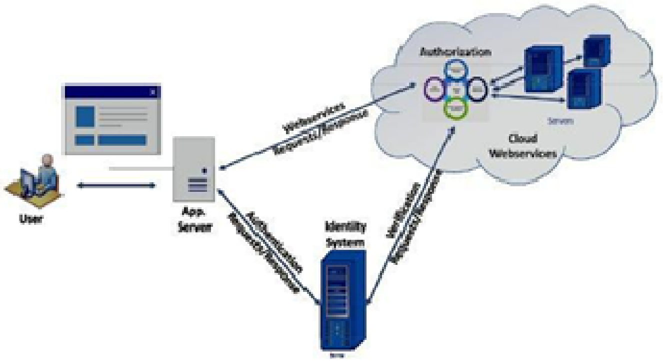


So, using Microsoft card space, OpenID and proxy encryption schema we enhance security level. We can here use novel identity schema for preserving data over cloud [4].

The combination of authentication and attribute based access control provides improved security to the cloud web service. The major problems in cloud web services are verification of eligible user's credentials, protection of credentials, Authentication, authorization, data protection, accountability, account hijacking and other security issues.

We can avoid this issue using integrated model of identity management and access management and this new schema known as integrity model.

Using this kind of model we can get more secure environment for any type of user wants it.


Authorization
Servers
Cloud Webservices
Webservices Requests/Responses
User
App. Server
Authentication Requests/Responses
Identity System
Verification Requests/Responses

The main concern is to monitor, protect, and verify the security of data at rest, in motion and in use in the cloud environment Most of the organizations are following Role based Authorization model. Role based Access Control (RBAC) concerns with the role of particular person in an organization.

When people move from web applications to cloud computing platform, their main concern point is how to raise privacy of user's sensitive data in cloud infrastructure. The traditional form of accessing cloud services is to use a username and password as a security token. During login/access time, new security risk may arise like virtualization attack, account/password sniffing, or phishing attack.

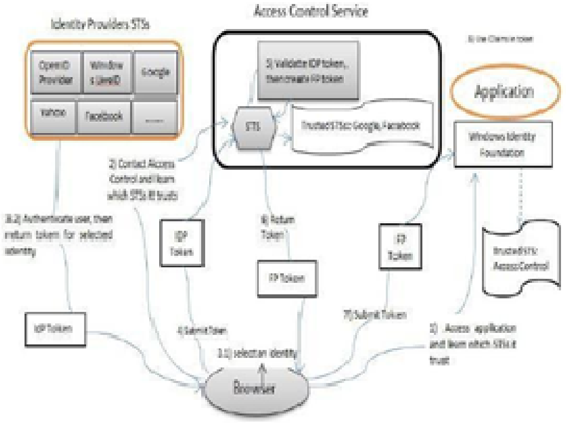

Identity Providers STSs
OpenID Provider
Windows LiveID
Google
Yahoo
Facebook
Access Control Service
5) Validate IDP token, then create FP token
STS
Trusted STSs: Google, Facebook
Application
Windows Identity Foundation
2) Contact Access Control and learn which STSs it trusts
3.2) Authenticate user, then return token for selected identity
IDP Token
6) Return Token
FP Token
FP Token
Trusted STS: AccessControl
IDP Token
4) Submit Token
3.1) selection identity
7) Submit Token
1) Access application and learn which STSs it trust
Browser

Figure 6. The access control service makes it easier for an application to accept identities from multiple cloud identity providers [6]

Using claim based technique for accessing resources that improve security level. The access control service makes it easier for an application to accept identities from multiple cloud identity providers.

For achieving an identity-based proxy re-encryption scheme has been adopted which allows a user to encrypt his data under his identity and to delegate his data management capability to the cloud.

The cloud, which could grant the access to an authorized user by transforming the cipher text encrypted with the data owner's identity to the one with the sharer's identity.

Module Description

The major modules of this project are as illustrated as following:

- Experimental Set up.
- Data Encryption.
- Data sharing.
- Proxy re-encryption.

- Data Access.

Experimental set up

In this phase, two important tasks are done.

- The system setup
- Key Generation.

The illustration is given in Figure. 1. In this the data owner uploads the encrypted file to the cloud. Then the cloud performs the Proxy- Re encryption using the sharer's identity and stores it in the database. Whenever the user wants to access the file he retrieves it by decrypting the file using his secret identity.

In the system set up, the system parameters are built up. The system is to guarantee the authorized sharers who can access the data. In the Key Generation phase a pair of keys is generated for the data owner using a public key cryptographic algorithm. Here adopted a public cryptography algorithm at the owner side.

A pair of keys (PUo, PRo) is generated. In this each user needs to register with the system using his identity to obtain a secret key corresponding to his identity. The data owner can share his public key (PUo) only with the identity of the registered user.

Here, we can show that how to generate secret key for encryption and decryption.

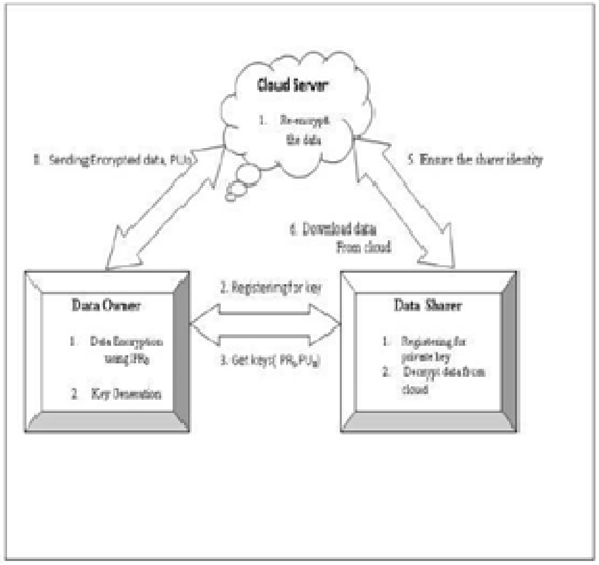

Cloud Server
1. Re-encrypt the data
8. Sending Encrypted data, PU₀
5. Ensure the sharer identity
6. Download data From cloud
2. Registering for key
3. Get keys(PR₀,PU₀)
Data Owner
1. Data Encryption using PR₀
2. Key Generation
Data Sharer
1. Registering for private key
2. Decrypt data from cloud

Figure 7 System model [7]

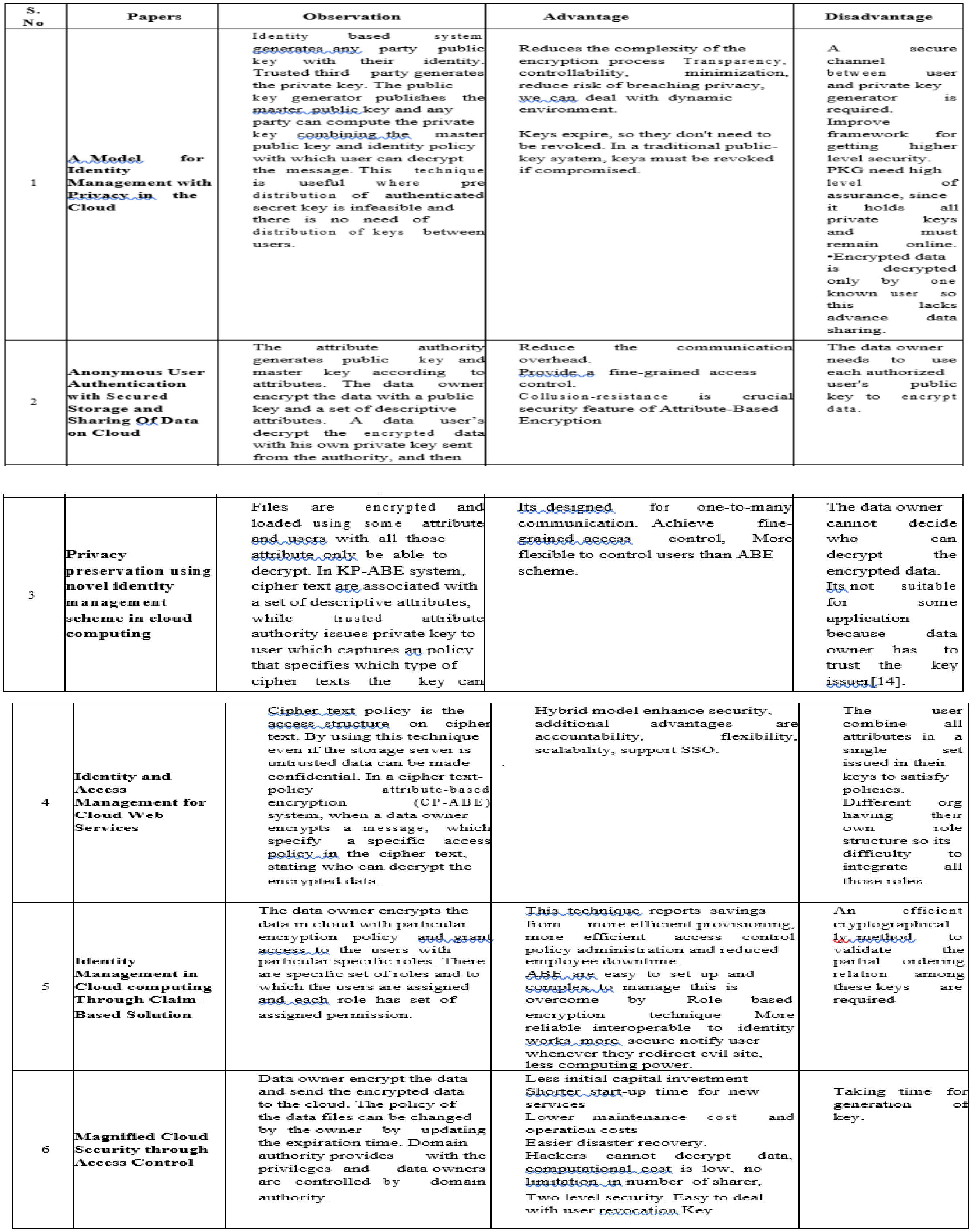
As the keys are generated only by the administrator there will be no abuse of keys. Each user has an identical key based on their identity there will be no duplicates. Each user is registered with the Administrator and the secret key is only known to the user and owner there will be no unauthorized access. As the data is forwarded to the cloud in encrypted format, it does not have any knowledge about the data.

In the data encryption phase the data owner runs the Encrypt algorithm which convert the plain text M(F) into cipher text C(F) using his private key(Pro). As mentioned in the previous phase the keys for encryption are generated whenever the data owner choose a file for uploading. The data owner performs a first level encryption using a public key cryptographic algorithm with his private key (PRo) after that the cipher text can be transformed to the cloud where a second level encryption (IB-PRE) is performed.

C(F)=Encrypt(M(F),Pro))

Whenever the data owner encrypted the data. It will be uploaded in the cloud. Thus, way we can implement proxy re-encryption schema using various type of algorithms

Table1.Techniques and its Advantage & Disadvantage



S. No	Papers	Observation	Advantage	Disadvantage
1	**A Model for Identity Management with Privacy in the Cloud**	Identity based system generates any party public key with their identity. Trusted third party generates the private key. The public key generator publishes the master public key and any party can compute the private key combining the master public key and identity policy with which user can decrypt the message. This technique is useful where pre distribution of authenticated secret key is infeasible and there is no need of distribution of keys between users.	Reduces the complexity of the encryption process Transparency, controllability, minimization, reduce risk of breaching privacy, we can deal with dynamic environment. Keys expire, so they don't need to be revoked. In a traditional public-key system, keys must be revoked if compromised.	A secure channel between user and private key generator is required. Improve framework for getting higher level security. PKG need high level of assurance, since it holds all private keys and must remain online. •Encrypted data is decrypted only by one known user so this lacks advance data sharing.
2	**Anonymous User Authentication with Secured Storage and Sharing Of Data on Cloud**	The attribute authority generates public key and master key according to attributes. The data owner encrypt the data with a public key and a set of descriptive attributes. A data user's decrypt the encrypted data with his own private key sent from the authority, and then	Reduce the communication overhead. Provide a fine-grained access control. Collusion-resistance is crucial security feature of Attribute-Based Encryption	The data owner needs to use each authorized user's public key to encrypt data.
3	**Privacy preservation using novel identity management scheme in cloud computing**	Files are encrypted and loaded using some attribute and users with all those attribute only be able to decrypt. In KP-ABE system, cipher text are associated with a set of descriptive attributes, while trusted attribute authority issues private key to user which captures an policy that specifies which type of cipher texts the key can	Its designed for one-to-many communication. Achieve fine-grained access control, More flexible to control users than ABE scheme.	The data owner cannot decide who can decrypt the encrypted data. Its not suitable for some application because data owner has to trust the key issuer[14].
4	**Identity and Access Management for Cloud Web Services**	Cipher text policy is the access structure on cipher text. By using this technique even if the storage server is untrusted data can be made confidential. In a cipher text-policy attribute-based encryption (CP-ABE) system, when a data owner encrypts a message, which specify a specific access policy in the cipher text, stating who can decrypt the encrypted data.	Hybrid model enhance security, additional advantages are accountability, flexibility, scalability, support SSO.	The user combine all attributes in a single set issued in their keys to satisfy policies. Different org having their own role structure so its difficulty to integrate all those roles.
5	**Identity Management in Cloud computing Through Claim-Based Solution**	The data owner encrypts the data in cloud with particular encryption policy and grant access to the users with particular specific roles. There are specific set of roles and to which the users are assigned and each role has set of assigned permission.	This technique reports savings from more efficient provisioning, more efficient access control policy administration and reduced employee downtime. ABE are easy to set up and complex to manage this is overcome by Role based encryption technique More reliable interoperable to identity works more secure notify user whenever they redirect evil site, less computing power.	An efficient cryptographical ly method to validate the partial ordering relation among these keys are required
6	**Magnified Cloud Security through Access Control**	Data owner encrypt the data and send the encrypted data to the cloud. The policy of the data files can be changed by the owner by updating the expiration time. Domain authority provides with the privileges and data owners are controlled by domain authority.	Less initial capital investment Shorter start-up time for new services Lower maintenance cost and operation costs Easier disaster recovery. Hackers cannot decrypt data, computational cost is low, no limitation in number of sharer, Two level security. Easy to deal with user revocation Key	Taking time for generation of key.

IV. PROPOSED MODEL

Each technique has its own pros and cons and used according to requirement. Among all we choose claim based method to explore its method.From literature survey here we can show that in the traditional form of accessing cloud services is to use a username and password as a security token. During login/access time, new security risk may arise like virtualization attack, account/password sniffing, or phishing attack. Hence, cloud service provider does not provide a complete security. Even though existing authentication scheme have addressed various security properties, there is still need of a secure authentication mechanism. So it’s important to introduce security to cloud platform along with claim based Authentication model, so we decided to improve its method by introducing new modified RSA algorithm.

Key generation:

Modified RSA Algorithm is as follows:

1. Choose 4 large prime numbers p, q, r and s randomly and independently of each other. All primes number should be of equivalent length.
2. Compute n, m, φ , λ :- • n= p x q • m= r x s • φ= (p-1) x (q-1) • λ=(r-1) x(s-1).
3. Choose an integer e, $1 < e < \varphi$ such that Gcd (e, φ) =1
4. Compute the secret exponent d, $1 < d < \varphi$, such that e x d mod φ =1.
5. Select an integer g=m+1.
6. Compute the modular multiplicative inverse: μ=λ-1 mod m. The public (encryption) key is (n, m, g, e). The private (decryption) key is (d, λ , μ)

Encryption: Let F be a data to be encrypted where the contents of data are taken into string S. Select random number r, where r < m. Compute cipher text as C = gs^e mod n * rm mod m2

Decryption: Compute original message: S = (((cλ mod m2 -1) / m) * μ mod m)d mod n.

Block diagram

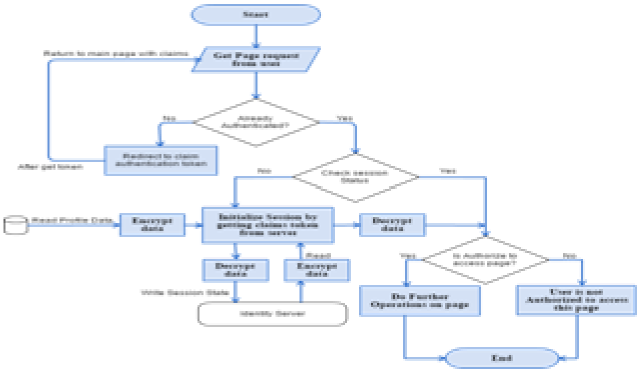

Start
Get Page request from user
Return to main page with claims
Already Authenticated?
No
Yes
Redirect to claim authentication token
After get token
Check session Status
No
Yes
Read Profile Data
Encrypt data
Initialize Session by getting claims token from server
Decrypt data
Decrypt data
Encrypt data
Read
Write Session State
Identity Server
Is Authorize to access page?
Yes
No
Do Further Operations on page
User is not Authorized to access this page
End

Fig 8. Flow of modified RSA Algorithm

In phase 1, when user request for a page it will check again for authentication. If user is already authenticated then on phase 2, it will check session status for further authorization process for a specific page which is requested by user. If user does not have a session with server then it has to get session from identity server and claims based token server. During this process by accessing user profile data which is encrypted goes to claim based token server, which will use identity server for getting session state information which is also encrypted. After confirming available session which then assign to specific user forspecific page request.

In Phase 3, if the user has authorize to access the page then it can perform further operation on it otherwise it will end session if it is not authorize to use the specific page.

V. CONCLUSION

From literature survey here we can show that in the traditional form of accessing cloud services is to use a username and password as a security token. During login/access time, new security risk may arise like virtualization attack, account/password sniffing, or phishing attack. Hence, cloud service provider does not provide a complete security. Even though existing authentication scheme have addressed various security properties, there is still need of a secure authentication mechanism. So it’s important to introduce security to cloud platform along with claim based Authentication model.

REFERENCES

[1] www.wileyindia.com/cloud-computing-principles-and-paradigms.html

[2] Jorge Werner, Carla Merkle Westphall, “A Model for Identity Management with Privacy in the Cloud”, 2016 IEEE Symposium on Computers and Communication (ISCC), DOI: 10.1109/ISCC.2016.754 3782. (Volume-1 to 6)

[3] Manisha D Karad, Milind B Vaidya" Anonymous User Authentication with Secured Storage and Sharing Of Data on Cloud"In Advance Computing Conference (IACC), DOI10.1109/INFOP. 2015.748937 8 2015 IEEE International. (Volume-201 to 205)

[4] Dishant Soni, Hiren Patel., Anthony Theodore Chronopoulos "Privacy preservation using novel identity management scheme in cloud computing" In International Conference on Data Science & Engineering (ICDSE), 2015, DOI: 10.1109/ICDSE. 2014.6974610

[5] Shobana, G.; Geetha, M.; Suganthe, R.C."Identity and Access Management for Cloud Web Services" Information Communication and Embedded Systems

[6] Ashish Singh, Kakali Chatterjee" Identity Management in Cloud computing Through Claim- Based Solution" Information Communication and Embedded Systems (ICICES), 2064, (Volume- 524 to 529) DOI: 10.1109/ICICES.2014.7033816

[7] K.Ganagavalli , P.Saravanan, V.Krishnamoorthy "Magnified Cloud Security through Access Control" Human Computer Interactions (ICHCI), 2016 International Conference on, 2015,(Volume-1 to -4) DOI:10.1109/ICHCI-IEEE.2013.6887799

[8] http://cloudnewsdaily.com/wp-content/uploads/2015/03/ cloud-computing-security.jpg