Special Issue | August 2017 ISSN: 2320-9984 (Online)

International Journal of Modern Engineering & Management Research

Website: www.ijmemr.org

All India Seminar on

Futuristic Trends in Telecommunication Engineering & Telecom Panorama – Fundamentals and Evolving Technology, with Particular Reference to Smart City on 5th – 6th August 2017

Organized by

The Institution of Engineers (India)

Jabalpur Local Centre

Multi-Level Authentication and Data Privacy Technique for Accessing Cloud Services

Mukta Bhatele
Professor
Department of Computer Science & Engineering
Gyan Ganga Institute of Technology & Sciences
Jabalpur (M.P.), [INDIA]
Email: mukta_bhatele@rediffmail.com

Neha Bairagi
M. Tech. Research Scholar
Department of Computer Science & Engineering
Gyan Ganga Institute of Technology & Sciences
Jabalpur (M.P.), [INDIA]
Email: nehabairagi05@gmail.com

Abstract**—***Cloud computing, often referred to as simply "the cloud," is the delivery of on-demand computing resources— everything from applications to data centers over the internet on a pay-for-use basis. Cloud computing is now the hot spot of computer business and research. However cloud computing security issues have become more and more pronounced. To protect data confidentiality and integrity, making more reliable in cloud computing becomes priorities. Cloud computing security related to the survival of cloud computing, has become a key factor in the development of cloud computing. This paper presents a data security model for cloud computing, and introduces agents to data security module in order to provide more reliable services.*

Keywords:— *Confidentiality, OTP, MFA, Availability, Private Cloud.*

1. INTRODUCTION

Cloud, as explained roughly is the best thing in the new world; if you are on correct cloud with right services and using it in a right manner then you are definitely on cloud 9 and you can take the best shower of technology anytime, be anywhere; otherwise it is a nightmare. Cloud computing is also known as distributed computing since it has the capability to run many applications over a single resource on a network. This can be related with grid computing where idle processors within the network are used to resolve mission-intensive issues that are ineffectual for any autonomous machine. This makes cloud an ever-growing technique for organizations that follow the OPEX model so that the core business share can be utilized elsewhere and not on the infrastructure aspect. Thus infrastructure provision for multiple organizations is done under a single roof. It is also referred to as "a type of Internet based computing," where different services — such

as servers, storage and applications —are delivered to an organization's computers and devices through the Internet [1].

Data security is thus becoming a fundamental barrier in cloud computing since information of the client organizations are hosted under the same network.

The cloud is categorized basically into:

A. Service models

Infrastructure as a service is the one that offers hardware resources for intensive computing. These include some kind of storage services (database or disk storage) or virtual servers [2].

Platform as a Service is the one that involves provision of development platforms such as JAVA, Groovy, Pearl, etc. for developers on the cloud. The development platforms are usually non-compatible with each other. Hence, PAAS provides a integrated platform to develop, test, deploy, host and maintain applications over a single environment. It provides Multi-tenant architecture where multiple concurrent users utilize the same development application [2].

Software as a service (SaaS) deals with provision of a set of softwares for users based on a thin browser client. This model is regulated on a pay-per-use basis. Salesforce.com has been a leader for such an offering in online Customer Relationship Management (CRM) space [3].

B. Deployment models

Public cloud: This involves hosting a application at the cloud service provider's end and the customer has no knowledge about the infrastructure centre. Such a centre is shared among multiple organizations.

Private cloud*:* Organizations that build up their own cloud environments for organizational specific roles are termed as private clouds. Security is best offered in Private but at the expense of rise in cost. Private clouds are further categorized into: Externally Hosted and On-premise private clouds. The former one is hosted by some cloud service providers but are dedicated to one particular organization only which proves it is far more cheaper than the latter one [3].

Hybrid cloud: This type of environment is suitable for organizations that trade-off between Public and Private clouds. In this Hybrid model, private clouds are used for mission critical applications and public clouds for applications that require less security concerns. Such a combination is called hybrid cloud. Cloud Bursting is a similar term to Hybrid computing. In Cloud bursting, organizations use their own computing infrastructure for normal usage, but access the public cloud such as Salesforce cloud computing for peak load requirements. Such a type ensures that a sudden increase in computing requirement is handled gracefully [3].

Community cloud: This cloud environment is useful for governmental organizations in which a single state has all its information over a single virtual server. For example, all Government organizations within the state of California may share computing infrastructure on the cloud to manage data related to citizens residing in California [3].

Security is a major concern in all the above models. Private clouds have better security aspect from all the above mentioned types.

The content of this paper is organized as follows: Section II provides a brief survey of the available security solutions for Cloud domain. Section III describes the proposed security solution over the existing ones mentioned in Section II.

System evaluation of the implemented solution is briefed in Section IV. The paper concludes in Section V giving a summarized view of the topic and some better approaches that could be experimented in future.

2. LITERATURE REVIEW

The deployment models of cloud have their own use cases. Usually organizations prefer Public cloud since they provide latest technology, such as the ones offered by Amazon. Google Drive with its Infrastructure and many applications, are also shared by many users worldwide. Even though Cloud Computing reduces the cost, provides flexibility and availability, which is the reason for companies to go for it, the security and availability issues still prevail in public clouds.

The companies worldwide also have a chain of security fundamentals that are followed hence directly opting for a public cloud is not the best solution. Organizations that need greater security thus invest in private clouds, with optimum availability and performance of services.

Various attack scenarios that are prevalent over the web are guessing attack, replay attack, stolen-verifier attack and modification attack. Thus to make cloud a secure model, generally, Authentication based on cryptographic techniques are used. Password-based method is the one that allows authorized users to access the resources in an uninterrupted manner. Research in this area has led to many password-based authentication schemes for entering into systems ;usually systems with web interfaces [4]. But static ones (Usernamepassword based) are prone to attacks since they can be bruteforced by malicious users given ample attempts and time.

MFA (Multi Factor Authentication) is the one which is based on more than one user credentials for authentication. These credentials are based on factors such as Possession, Knowledge, Inherence, Location and Time [5]. In 1981, Lamport proposed a onetime password (with factors Possession and Knowledge) authentication scheme using cryptographic hash functions [4]. The purpose of OTP is to make it more difficult to gain unauthorized access to restricted resources. The technique is much in demand since it uses physical resource for authentication. Hence, Dynamic (that are altered in intervals) or one time passwords hold greater security value than the static ones. OTPs are of basically two types: HOTP [RFC 4266] and TOTP [RFC 6238].

Other methodologies of MFA include:

- Security tokens (Hardware) in the form of smart cards or small devices with USB technology [17].
- Security tokens (Software) that generate a single-use login PIN has device based possession factor. For example, Google Authenticator [17].
- Mobile authentication such as SMS or calls for OTPs.
- Biometric authentication methods such as fingerprint, facial recognition uses Inherence factor. For example, Dell Defender [17].
- Smartphone with GPS uses location as a factor [17].

Hybrid methodologies include swiping a card, scanning a fingerprint and answering a security question all at once or attaching a USB hardware token to a desktop that generates a one-time pass code to login into a VPN client, etc for MFA [17].

Encryption is followed by Authentication to provide Data confidentiality and Data integrity. PKI (public key infrastructure) basically encrypts the message for a particular receiver using his public key. Franklin and D. Boneh introduced Identity based encryption [13] which encrypts and decrypts data based on some user identity. The public key used in this scenario is a personal identifiable information, for example email-id of the user rather than any random string that are used in PKI systems generally. IBE has an extended and advanced form as ABE.

ABE (Attribute based encryption) introduced by water and sahai in 2005 uses a set of attributes (and not an atomic attribute) for data encryption. It is one of the public key encryptions in which User attributes such as

phone number or any kind of personal identifiable information is used to generate both the secret key as well as the cipher text [6].

There are varied roles in this scheme performed by the authority, the data owners (senders) and the data users (receivers). The authority constructs keys for data owners and users to encrypt and decrypt data respectively. These keys are generated based on the attributes (i.e. attributes of public key and master key) that need to be predefined (i.e. all the attributes are listed which will be used in future). If any data user who wants to get added to this system, and he owns those attributes that are not part of the predefined ones, the authority then re-defines attributes and generates a new public key and master key again based on redefinition. The data owner in this scheme encrypts data with a public key and a set of descriptive attributes whereas a data user decrypts encrypted data with his private key provided by the authority, and only then can the plain text be recovered. For decryption, set of attributes in user's private key is checked by matching with the attributes in encrypted data. If the "matching score" is at least a threshold value, the receiver's private key is permitted to decrypt the encrypted data. For example, for a set of descriptive attributes in the encrypted data, {CCL, Rushikesh, Mayuresh}, the threshold value is 2. If a receiver wants to decrypt the encrypted data, his number of attributes in private key should be two or the more than two of attributes in the encrypted data, hence, a data user that has a private key with attributes, {CCL, Mayuresh} decrypts and obtains the data [7]. An important security aspect of ABE is collusion resistance: in which a contender that possesses n keys can read the plain text if at least one of the n keys prove successful [7]. In short, independently randomizing users' secret keys restrict users to club their secret keys in decrypting the encrypted text. Hence a user that is unable to decrypt using his key will definitely be not able to decrypt even on pooling keys of all the users of the system [16].

ABE has two important variants such as KP-ABE proposed by Goyal and CP-ABE by sahai and water [14] respectively. {n, m}-threshold gates, i.e. n out of m attributes have to be present. For example, the universe of attributes defined over the entire system are {P,Q,R,S} and user Rushikesh gets a key with respect to attributes {P,Q} and user Mayuresh with respect to attribute {S}. If a cipher text is encrypted based on the policy (P∧ R) ∨ S, then user Mayuresh is able to decrypt, while user Rushikesh is not. In CP-ABE there is no separate access control or authorization mechanism. It is incorporated in the encryption mechanism itself. Users can even obtain their secret keys after data encryption using the access structure is an important add-on. Hence, data can be encrypted even with not knowing the genuine user groups which can decrypt and only specifying the policy is quite enough. Future users are given a key based on the attributes those that the policy satisfies and such users are only genuine decrypters of the system [16].

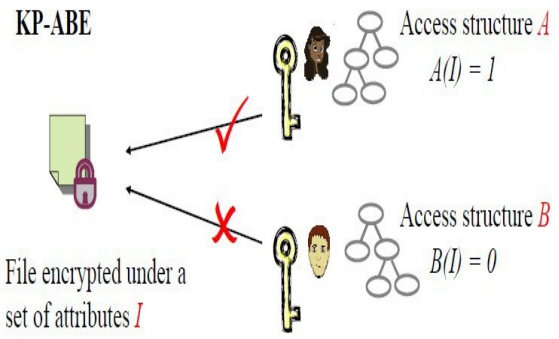

Figure 1. KP-ABE Scheme [15]

A user's group of attributes are used in the above KP-ABE scheme. The sender encrypts data using a set of attributes. The receiver on the other side is able to decrypt only if the access structure he/she maintains is a combination of attributes of the sender. In the above diagram, receiver A is able to decrypt the data since the access structure satisfies the overall combination of attributes of the sender, while B does not [15]. In this, the access structure is infused into the user's secretive key, for example, (P∧ R)∨ S, and a cipher text that is formed using an attribute set e.g., {P,Q}

could not be decrypted by the user possessing the attribute set of P,Q but the same could be decrypted by a user with an attribute with respect to {P,R} as the attribute set [16].

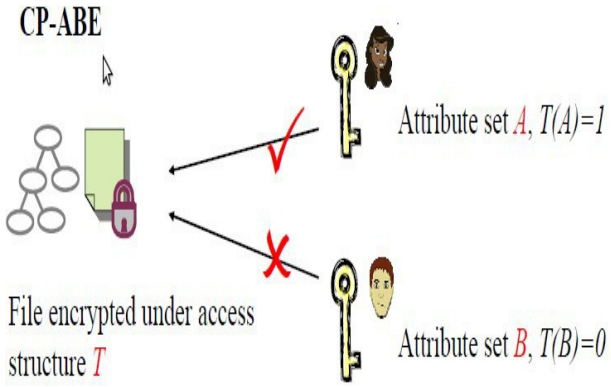

Figure 2. CP-ABE Scheme [15]

In CP-ABE, it is not the set of attributes that do the working but the policies defined over a set of attributes carry the encryption process [15]. In this scheme, User's private key is based on a group of attributes whereas the ciphertext is based on the access structure defined over system specific attributes. A user is able to decrypt a text, if his attributes satisfy the policy specified in the cipher text. Policies are defined over attributes using conjunctions, disjunctions and

3. PROPOSED SOLUTION

The proposed solution aims in developing a private cloud and providing secure storage service using MFA (for authentication) and CP-ABE(for data Confidentiality). The private cloud is developed using open source technologies like Apache Ambari [8], Oracle VM Virtual box [9], Vagrant [10], Putty. For the cloud system, CentOS operating system - a Linux distribution is used.

Figure 3 shows actual flow of the system. The user registers and logs in with its credentials, enters OTP, this OTP is in a token form which is provided by Google Authenticator application in Mobile devices. To enter into the cloud environment, user's personal credentials as well as Token(using TOTP algorithm) provided by the Service provider is needed.

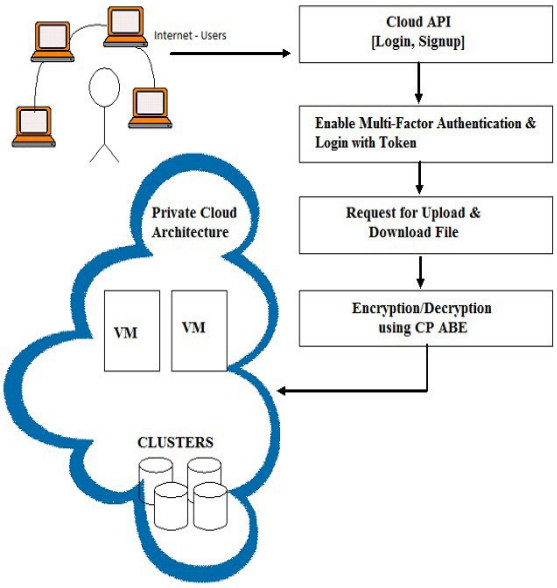

Figure 3. Architecture of the system.

```
session_key = decrypt_session_key(sctxt, mpk, msk, attributes)
enc = encrypt(plaintext, mpk, session_key)
```

For uploading a file, User provides the file as input and the cloud service encrypts it using CP-ABE algorithm. The detailed working of CP-ABE is seen further. The encrypted file is stored on cloud. The cloud contains the clusters for storage. To download file from the cloud, user again has to login with its credentials and OTP generated by Cloud Service.

Then it selects the file from cloud which he wants to download. Cloud service based on user's demand to retrieve the encrypted file or the decrypted file does the processing. If decrypted file is to be fetched, the Cloud service using CPABE decrypts the file and sends it to user, otherwise the file is downloaded in encrypted format and is sent to the user. An additional layer of security is available for files that need to be decrypted and downloaded, i.e. attributes are to be filled by the users (as provided in the registration phase) into the verification page. If verification is successful, file is downloaded in a plain-text format, else download fails.

A) Authentication levels provided are as follows:

1. Static username and password.
2. OTP using new tokens or default tokens.

B) Data Confidentiality

The CP-ABE encryption technique is used to provide confidentiality and access control. It has four algorithms such as setup, encryption, key generation, & decryption. The process with its pseudo- code is shown below.

SETUP(ʌ;U)- The setup algorithm has security parameter and attribute universe as input. It generates public parameters "pk" as "mpk" and one master key which is "mk" as "msk" [11].

```
def CPABE_setup():
    group = PairingGroup('SS512')
    cpabe = CPabe_BSW07(group)
    return mpk,msk
```
(1)

Key Generation (MK; S) - In key generation, MK and set of attributes S are taken as input that describe the key. It gives "SK" i.e. "dec_key" which is decryption key and used only for decryption of session key [11].

```
dec_key = cpabe_keygen(group, msk, mpk, attributes)
```
(2)

```
def cpabe_keygen(group, msk, mpk, attributes):
    return CPabe_BSW07(group).keygen(mpk, msk, attributes)
```
(3)

Encrypt (PK; M; A) - This algorithm uses the PK, a message M, and structure of attributes A (access structure or access policy) over a universe of attributes. It encrypts message and produces a cipher text CT which is only decrypted by a user that has a set of attributes that satisfies the combination of attributes in the access structure [11]. value that is generated for each user whereas Session key context is combination of session key and access policy.

Figure 4 gives schematic representation of encrypted session key. Figure 5 shows a general sample of CP-ABE access policy which can have AND (OR) combination of attributes in the system. The CP-ABE policy in the proposed solution is

ANDing of attributes such as username, email-id, DOB and mobile number.

```
def decrypt_session_key(session_key_ctxt, mpk, msk, attributes):

    dec_key = cpabe_keygen(group, msk, mpk, attributes)
    session_key = cpabe.decrypt(mpk, dec_key, session_key_ctxt)

    return session_key
```
(5)

```
def encrypt(message, mpk, session_key):

    group = PairingGroup('SS512')
    cpabe = CPabe_BSW07(group)

    message = pad(message)
    iv = Random.new().read(AES.block_size)
    cipher = AES.new(sha(session_key)[0:32], AES.MODE_CBC, iv)
    return iv + cipher.encrypt(message)
```
(6)

Decrypt (PK; CT; SK) - In this decryption code, PK, a cipher text, which contains an structure of attributes A, and a private key are taken as input which is a private key for a S set of attributes. If the S set of attributes is equivalent to A i.e. if dec_key matches the attributes in policy within the session key context scenario, session key for that user is decrypted. This session key is then used to decrypt the cipher text and give the original message [11].

```
session_key = decrypt_session_key(sctxt, mpk, msk, attributes)
dec = decrypt(ciphertext, mpk, msk, session_key)
```
(8)

```
def decrypt(ciphertext, mpk, msk, session_key):

    iv = ciphertext[:AES.block_size]
    cipher = AES.new(sha(session_key)[0:32], AES.MODE_CBC, iv)
    plaintext = cipher.decrypt(ciphertext[AES.block_size:])
    return plaintext.rstrip(b"\0")
```
(9)

In (6) and (9), encryption and decryption of contents is achieved using AES algorithm, whereas CPABE encrypt/decrypt is used for

session key encryption and decryption respectively.

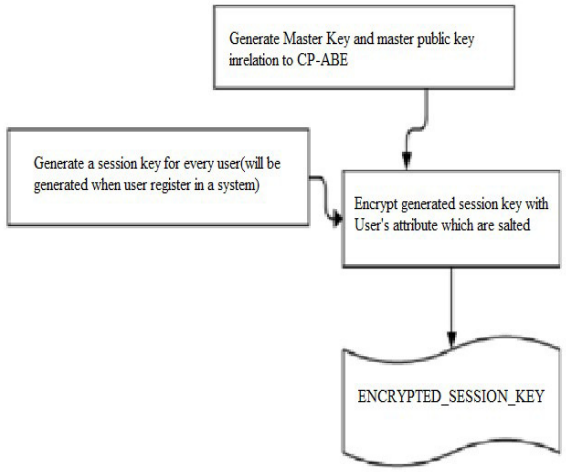

Figure 4. CP-ABE Key generation

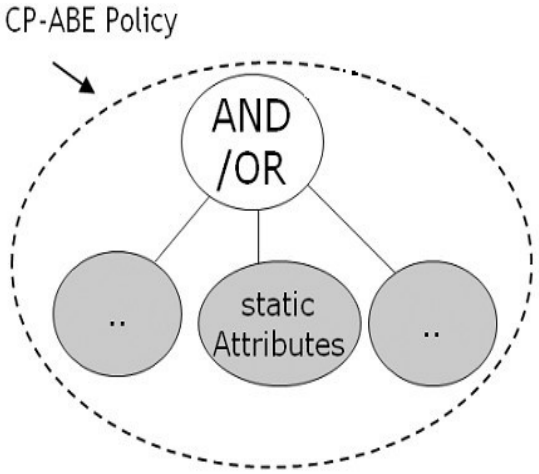

Figure 5. CP-ABE Access policy scenario

Figure 6 shows the flow of the encryption and decryption of the file. Step 1 is used to decrypt the session key and use this session key for AES encryption of data, but within the access policy context i.e. the session key context. For decryption, AES decryption of contents is done using session key for each user. Session key decryption is is possible only if the attributes in dec_key (in the Key_gen phase) matches the attributes in the access policy.

5. SYSTEM EVALUATION

The proposed system provides Cloud Storage security using MFA and Encryption technique. The performance and security check of the implemented module is done as follows:

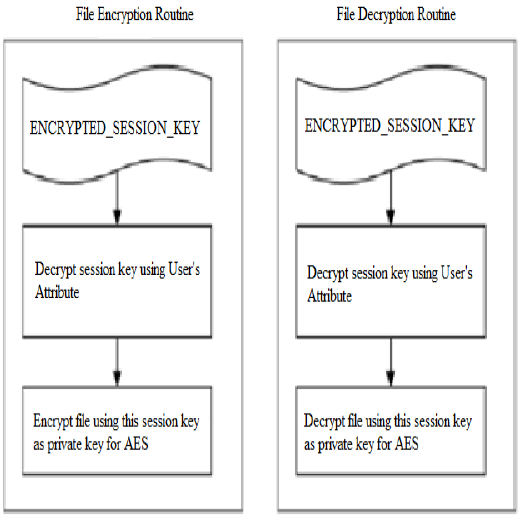

Figure 6. Encryption and Decryption Routine

A. Performance

Case- Number of attributes per user in the system are increased and time required for Encryption key generation, to encrypt the file, Decryption time, and time taken to decrypt the file from ciphertext to plaintext is calculated. A file size of 10426 bytes is used for the test.

Observation-

Figures 7 and 8 show that the time taken for key generation and encryption-decryption process increases with increase in number of attributes.

The security level also increases with increase in attributes for encryption.

B. Security Check

The security implementation can be verified as- Level 1 check- A malicious User logs in using authorized user's username and password, still is unable to gain access to the system. This is because even though initial security level is bypassed the next level of security depends on physical device. Only after getting access to the device can a user be eligible to enter into the cloud system.

Level 2- A malicious User steals the authorized user's physical device (mobile phone) and uses user's tokens for authentication.

But even this does not let the malicious user access the authorized user's account. This is possible because there is again a verification page that matches the initial registration page entries with the newly submitted entries (i.e. user's attributes such as DOB and mobile number). Hence security of authenticated user is preserved.

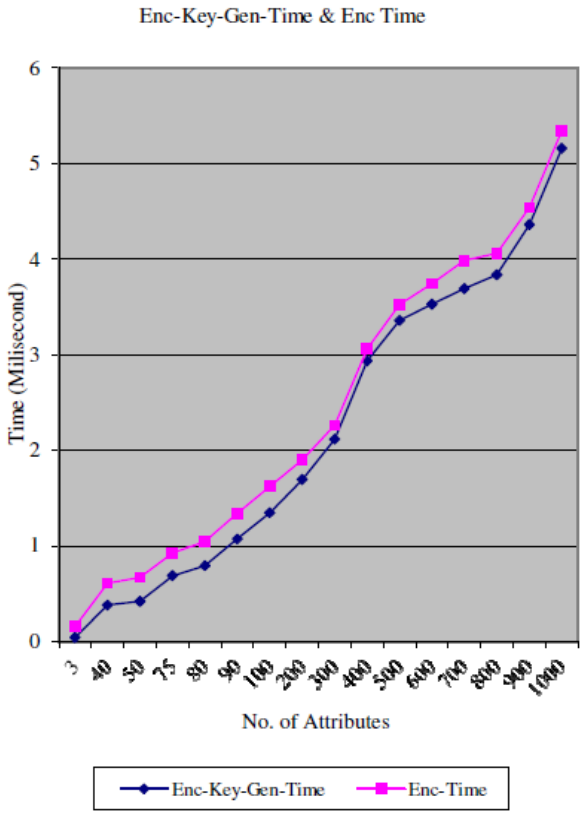

Figure 7. Encryption- Key generation & Encryption time for CP-ABE

C. TOTP Vulnerability

There are some weaknesses in the authentication system as well which cannot be ignored. The TOTP is a vulnerable system which has issues as the TOTP device gets discharged or the clock gets de-synced or at times even the device gets stolen. Security related weaknesses of TOTP that are found are attackers can view TOTP codes since they are available over the screen itself, TOTPs are also prone to malware attacks.

D. Service Offered

Private Cloud deployment has benefits of customization in services as per Business needs. This paper focuses on the customized services and data protection mechanisms offered by the proposed solution, such as :

1. Automatic Resource Scaling

Users are provided with dedicated resources as per their needs. Based on User demands, resources are scaled or removed, this prevents resource locking up, when Users leave the system.

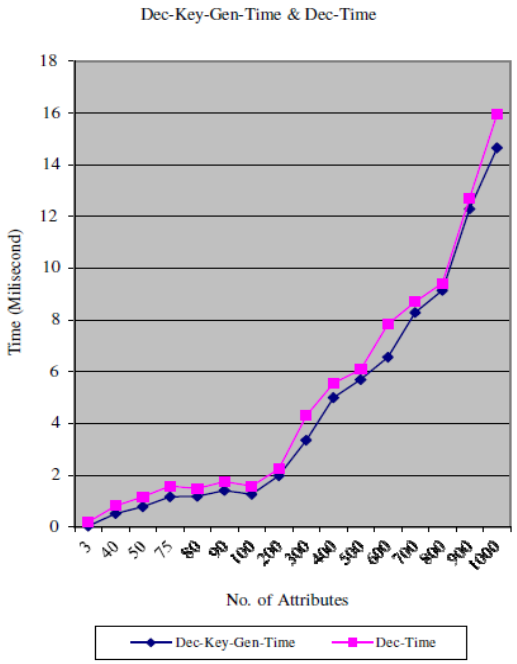

Figure 8. Decryption- Key generation & Decryption time for CP-ABE

2. Managed Virtual Environment

Design and Hardware can be customized and configured as per Business needs.

3. Customization in Security a) MFA

The solution uses static username-password and QR code based tokens as the MFA mechanism. Authentication using SMS or E-mail as the second factor is also a available option, based on requirements.

b) Availability

Tokens generated by QR code is the second factor of authentication in the proposed solution. But, for authorized users, there is a provision of backup tokens, for situations where QR code scanning is not possible. This preserves availability for genuine users.

c) CP-ABE

The proposed system uses attributes for access policy creation in CP-ABE technique. The system offers customization in number of attributes for CP-ABE i.e. number of attributes can be increased or decreased for security provision. In other words, for a superset of attributes 5, a user can input any number of attributes (maximum 5), and encryption of data is achieved based on input number of attributes.

d) Administrative interference

Files encrypted using CP-ABE technique cannot be viewed in plain-text even by the system administrator. Therefore, administrative interference is null.

4. Application Domains

The proposed solution offers robust security features, enabling mission-critical and financial applications as the best served application domains.

5. Backup services

Private cloud infrastructure deployment is set up using a 3- node cluster architecture, out of which only one remains active.

In the events of failure, other nodes in the cluster can be used as backup servers. Hence, snapshots of backup and redundant nodes are offered as backup solutions.

6. Administrative and Management console

The system provides ways for monitoring and management of system resources, such as RAM, storage space, etc. In a way, User management and Cluster management is also possible.

V. CONCLUSION AND FUTURE WORK

This paper presents private Cloud deployment so as to achieve better customization in services and data protection methods as stated above. Security levels taken into consideration are Confidentiality, access control. Data Confidentiality is achieved through CP-ABE encryption technique. Access control and availability is maintained using Multifactor Authentication principle. Multifactor authentication involves using static username-password as the first factor and OTP based on MFA as the second. The extended work lies in providing MFA to cloud environment using Artificial intelligence.

Factors in MFA range from Possession, Knowledge and Inference. For mobile or users that change their numbers frequently, possession factor does not seem feasible. The proposed MFA technique that uses Knowledge factor works fine in intermittent network conditions, but seems to be unstable when time sync between the mobile device and the system to be authenticated is not correct.

Therefore, a novel MFA technique, that incorporates, Inherence factor-Fingerprint, with Knowledge and Possession factors, is planned in future. This aims to achieve a level of security, which is difficult to break, because, Passwords can be changed, but the human anatomical characteristics tend to change very rarely.

REFERENCES:

[1] "What is Cloud Computing? A Webopedia Definition", 2015. [Online]. Available: http://www.webopedia.com/TERM/C/cloud_computing.html

[2] Rackspace Support, "Understanding the Cloud Computing Stack", October 2013, http://www.rackspace.com/knowledge_center/whitepaper/

understanding-the-cloud-computing-stack-saas-paas-iaas

[3] N. Garbani, "Private, Public, Hybrid Clouds," 2014. [Online]. Availbale:http://thecloudtutorial.com/cloudtypes.html

[4] L. Lamport, "Password Authentication with Insecure Communication", Communications of the ACM, Vol. 24, pp. 770-772, 1981.

[5] Niharika Gupta, Rama Rani, "Implementing High Grade Security in Cloud Application using Multifactor Authentication and Cryptography", International Journal of Web & Semantic Technology (IJWesT) Vol.6, No.2, April 2015

[6] "Attribute based Encryption" 2016 [Online]. Availbale: http://gleamly.com/article/introduction-attribute-based-encryption-abe

[7] Cheng-Chi Lee, Pei-Shan Chung, and Min-Shiang Hwang, "A Survey on Attribute-based Encryption Schemes of Access Control in Cloud Environments", International Journal of Network Security, Vol.15, No.4, PP.231-240, July 2013

[8] Apache software foundations, "Apache Ambari", 2016 [online] https://ambari.apache.org/index.html

[9] Margaret Rousey, "Hypervisor", October 2006. [online]. http://searchservervirtualization.techtarget.com/definition/hypervisor

[10] Gajda, Włodzimierz. "Getting Started with Vagrant." Pro Vagrant. Apress, 2015. 1-19.

[11] John Bethencourt, Amit Sahai, and Brent Waters. "Ciphertext-Policy Attribute-Based Encryption". In IEEE Symposium on Security and Privacy, pages 321-334, 2007.

[12] Grace Ramamoorthy, "Distributed systems and Cloud computing", April 2011 [online], http://www.resumegrace.appspot.com/pdfs/DistributedSystemsandCloudComputing.pdf

[13] D. Boneh and M. Franklin. Identity-based encryption from the weil pairing. In CRYPTO '01: Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology, pages 213–229. Springer-Verlag, 2001.

[14] V. Goyal, O. Pandey, A. Sahai, and B. Waters. "Attribute-based encryption for fine-grained access control of encrypted data." In CCS '06: Proceedings of the 13th ACM conference on Computer and communications security, pages 89–98, New York, NY, USA, 2006. ACM.

[15] Nabeel Yousuf, "ABE and its two Flavours", 2012 [online]. http://mohamednabeel.blogspot.in/2012/03/aattribute-based-encryptionabe-and-its.html

[16] "What is Attribute Based Encryption", [online]. http://crypto.stackexchange.com/questions/17893/what-is-attributebased-encryption.

[17] Margaret Rouse, "Multi-Factor Authentication", 2015 [online], http://searchsecurity.techtarget.com/definition/multifactorauthentication-MFA.