A SYSTEMATIC APPROACH TO SECURE ACCESSING OF DATA USING CP-ABE AND MULTIFACTOR AUTHENTICATION IN CLOUD

[1]J.Mala, [2]A.N.Jayanthi, [3]S.Rajesh
jmala2004@gmail.com, jayanthi.ece@srit.org, rajesh.cse@srit.org
1.Assistant Professor, Department of Information Technology
2.Associate Professor, Department of Electronics and Communication Engineering
3.Assistant Professor, Department of Computer Science and Engineering
Sri Ramakrishna Institute of Technology ,Coimbatore, India, Tamilnadu.

Abstract:
This paper is specially targeted on the security mechanisms together with confidentiality and Multifactor Authentication. Data Confidentiality is completed via CP-ABE encryption technique. Multifactor Authentication is finished the usage of the aggregate of Image Based Password and Hash-MAC primarily based One-Time Password. Firstly, the Image Based Password Authentication is executed wherein authenticated user has been the usage of photo password that become already selected by using the consumer, accompanied with the aid of the Hash- MAC primarily based SHA-1 set of rules is used for the generating one-time password in a secure manner. This authentication method is rather comfortable. The SHA-1 algorithm is used for the calculation of HMAC.

Key words..Confidentiality, Cipher text Policy Attribute based Encryption (CP-ABE), Multifactor Authentication MFA, Image Based Authentication(IBA), One Time Password(OTP), Secure Hash Algorithm (SHA-1).

I.INTRODUCTION

Cloud computing can offer many blessings to the end users and company whilst the records must be shared inside the cloud. The organizations can be stored and shared their information inside the cloud, since the fee of replacing the data is very less in cloud when compared to manually exchanging the statistics. People are waiting for information sharing functionality on their computer systems, telephones and computer etc. Persons like to percentage their data with others along with circle of relatives, colleagues, buddies or the world. Scholars also get benefit whilst operating on crew tasks, as they're capable of team up with members and get work accomplished efficaciously. It allows higher efficiency compared to former strategies of often sending updated variations of a document to participants of the organization via e-mail attachments [3].

II.SECURITY REQUIREMENTS

The security requirements for facts sharing in cloud computing system are as follows:

a) Data security:

The company should make sure that their data outsourced to the cloud is comfortable and the issuer has to take security measures to guard their facts in cloud.

b) Privacy:

The company need to ensure that every one critical information is encrypted and that best legal users have get admission to facts in its entirety. The credentials and digital identities need to be relaxed as any facts that the company collects approximately purchaser interest in the cloud.

c) Data confidentiality:

The cloud customers need to ensure that their facts contents aren't made available or disclosed to illegal users. Only authorized customers can access the touchy statistics at the same time as others should not access any information of the information in cloud.

d)Fine-grained access control:

Data proprietor can restrict the unauthorized users to access the records outsource to cloud. The data owner offers specific get right of entry

to rights to a hard and fast of consumer to get entry to the facts, whilst others no longer allowed to get entry to without permissions. The get entry to permission need to be managed best with the aid of the owner in un-trusted cloud environments.

e) User revocation:

When a person receives back the get admission to rights to the records, it will not permit any other consumer to access the information at the given time. The user revocation has to not affect the other accredited users within the institution.

f) Scalable and Efficient:

The number of Cloud customers is extraordinarily large and the customers be part of and go away unpredictably, it's miles important that the system preserve efficiency in addition to scalability. A powerful data sharing in cloud computing gadget ought to fulfil all of the security requirements. [3]

A.Service models

i) IaaS:

Infrastructure as a provider is the one that gives hardware resources for extensive computing. These include some kind of garage services such as database or disk storage or digital servers [4].

ii) PaaS:

Platform as a Service is the only that includes provision of development systems which includes JAVA, Groovy, Pearl, and so forth. For builders on the cloud. The development platforms are generally non-compatible with each other. Hence, PAAS presents an included platform to expand, take a look at, set up, host and maintain applications over a unmarried environment. It offers Multi- tenant structure wherein more than one concurrent customers make use of the identical development software [4].

iii) SaaS:

Software as a carrier deals with provision of a set of softwares for users based on a skinny browser client. This version is regulated on a pay-per-use basis. Salesforce.Com has been a pacesetter for such an offering in on line Customer Relationship Management (CRM) area [5].

B.Deploy mentmodels

i) Public cloud:

This includes web hosting an utility on the cloud service company's quit and the purchaser has no expertise approximately the infrastructure centre. Such a centre is shared among more than one corporations [5].

ii) Private cloud:

Organizations that increase their very own cloud environments for organizational specific roles are termed as private clouds. Security is excellent presented in Private but at the fee of rise in cost [5]. Private clouds are similarly classified into: Externally Hosted and On-premise non-public clouds. The former one is hosted by a few cloud service companies but are devoted to 1 specific enterprise only which proves it is some distance less expensive than the latter one [5].

iii) Hybrid cloud:

This type of surroundings is suitable for businesses that change-off between Public and Private clouds. In this Hybrid version, private clouds are used for project critical packages and public clouds for packages that require much less safety issues. Such a mixture is called hybrid cloud. Cloud Bursting is a similar term to Hybrid computing [5].

iv) Community cloud:

These cloud surroundings are beneficial for governmental groups wherein a single nation has all its statistics over a single virtual server [5].

III.RELATED WORK

i)One Time Password Token:

Access controls exist to save you unauthorized access. Companies ought to make certain that unauthorized access isn't always allowed and additionally legal customers can't make useless adjustments. The controls exist in a diffusion of forms, from Identification Badges and passwords to get right of entry to authentication protocols and security features [2]. There are mainly two types of password. They are Static password and Dynamic Password

Static password is the traditional password that is usually modified simplest when it's miles necessary: it's far modified while the user has to reset the password, i.e., either the consumer has forgotten the password or the password has expired. Static passwords are particularly at risk of cracking, due to the fact passwords used will get cached at the difficult drives [2].

To solve this, we developed One Time Password Token. Unlike a static password, dynamic password is a password which changes whenever the user logs in. An OTP is a hard

and fast of characters that may act as a shape identification for one time handiest. Once the password is used, it is no longer used for any further authentication. Even if the attacker gets the password, it's miles maximum possibly that it become already used as soon as, because it changed into being transmitted, hence vain to the attacker. This reduces the vulnerability of the hacker sniffing network site visitors, retrieving a password, and to correctly authenticate as a certified user. This password is used best for that consultation and when the user logins next time, any other password is generated dynamically [2].

ii) Image based authentication:

Image primarily based authentication is covered to offer extra protection included with OTP. With IBA, while the person performs first time registration on an internet site, he makes a choice of numerous secret classes of snap shots which can be smooth to take into account, together with pix of herbal scenery, cars. Every time the user logs in, a grid of randomly generated snap shots is presented to the consumer. The person identifies photos that had been formerly decided on. One-time get entry to code is generated with the aid of the chosen snap shots, making the authentication method greater comfy than using most effective a static text password. It's drastically less complicated and effective for the user due to the fact he has to don't forget only some classes to apprehend the chosen pictures [2].

Dhamija and Perrig [6] proposed a graphical authentication scheme based at the Hash Visualization approach [7]. In this method, the consumer is requested to pick out a sure quantity of photos from a set of random images generated by using application. Then the user can be authenticated by using figuring out the preselected pics. This approach fails to affect due to the fact the server has to keep the seeds of the portfolio photos of each consumer in plain text.

Akula and Devisetty's algorithm[8] is similar to the approach proposed by means of Dhamija and Perrig [6]. The distinction is that by way of the usage of hash set of rules SHA-1, which produces a 20 bytes' output, the authentication is greater at ease and requires less reminiscence. The authors recommended a probable future improvement by means of supplying continual storage and this may be deployed at the Internet, cell telephones and PDAs.

Weinshall and Kirkpatrick [9] sketched numerous authentication schemes, consisting of photograph reputation, item popularity, and pseudo word reputation, and conducted some of person research. In the image reputation examine, a consumer is trained to understand a big set of photos (100 – 2 hundred images) selected from a database of 20,000 pictures. This look at found out that snap shots are the handiest a few of the three schemes discussed. Pseudo codes also can be used as an alternative however require right putting and education.

Jansen et al. [10-12] proposed a graphical password mechanism for cell devices. During the enrolment stage, a user selects a theme which consists of thumbnail snap shots after which registers a chain of photographs as a password. During the authentication, the person ought to enter the registered pix in an appropriate collection. One drawback of this approach is that since the variety of thumbnail pics is restrained to 30, the password area is less. Each thumbnail image is assigned a numerical price, and the series of selection will generate a numerical password. The end result depicted that the image series length is typically shorter than the textual password length. To address this hassle, images may be mixed to compose a brand new alphabet element, therefore increasing the image alphabet size.

Takada and Koike mentioned a similar graphical password technique for cell devices. This approach permits customers to use their favourite image for authentication [13]. The customers first sign in their favorite snap shots (pass- images) with the server. During authentication, a consumer has to go through numerous rounds of verification. At each spherical, the user both selects a pass-photo among several decoy-pictures or chooses nothing if no bypass-photograph is present. The software authorizes a user only if all verifications are a success. Allowing customers to register their very own pix makes it easier for person to recollect their password pix. This technique is an at ease authentication method in comparison with text-based passwords. Allowing customers to apply their own pix might make the password even greater predictable, particularly if the attacker is acquainted with the consumer.

Encryption is observed by Authentication to provide Data confidentiality and Data integrity. PKI (public key infrastructure) essentially encrypts the message for a specific receiver the use of his public key. Franklin and D. Boneh delivered Identity based encryption [14] which encrypts and decrypts information primarily based on some user identification. The public key used in this situation is a private identifiable statistic, for instance e-mail-id of the person instead of any random string which are utilized in PKI structures usually. IBE has an extended and advanced shape as ABE.

ABE added by water and sahai in 2005 makes use of a fixed of attributes (and not an atomic characteristic) for facts encryption. It is one of the public key encryptions in which User attributes together with telephone variety or any sort of personal identifiable facts is used to generate each the name of the game key as well as the cipher text [15]. There are varied roles in this scheme finished by means of the authority, the data proprietors (senders) and the records customers (receivers). The authority constructs keys for facts owners and customers to encrypt and decrypt data respectively. These keys are generated based at the attributes (i.e. Attributes of public key and master key) that need to be predefined (i.e. All of the attributes are listed on the way to be utilized in future). If any facts user who desires to get introduced to this gadget, and he owns the ones attributes that are not a part of the predefined ones, the authority then re-defines attributes and generates a new public key and grasp key again based on redefinition. The statistics proprietor on this scheme encrypts information with a public key and a set of descriptive attributes whereas a data consumer decrypts encrypted statistics with his personal key furnished by way of the authority, and only then can the obvious text be recovered.

For decryption, set of attributes in person's private key is checked by means of matching with the attributes in encrypted information. If the & quot; matching rating & quot; is at least a threshold price, the receiver's personal key is permitted to decrypt the encrypted records. For instance, for a hard and fast of descriptive attributes in the encrypted information, CCL, Rushikesh, Mayuresh, the edge value is two. If a receiver wants to decrypt the encrypted data, his wide variety of attributes in non- public key need to be or the greater than of attributes within the encrypted information, therefore, an information user that has a personal key with attributes, CCL, Mayuresh decrypts and obtains the records [16].

An essential protection component of ABE is collusion resistance: in which a contender that possesses n keys can examine the plain textual content if at least one of the n keys how a hit [7]. In quick, independently randomizing users' mystery keys limit customers to membership their mystery keys in decrypting the encrypted textual content. Hence a user that is unable to decrypt the use of his key will really be no longer capable of decrypt even on pooling keys of all of the customers of the system [17].

ABE has important versions such as KP-ABE proposed through Goyal and CP- ABE by sahai and water [18] respectively.

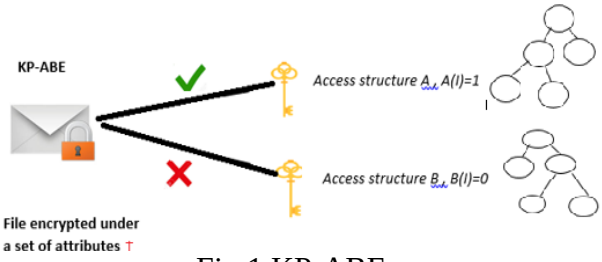

Fig.1.KP-ABE

In Fig.1.A consumer's organization of attributes are used inside the above KP- ABE scheme. The sender encrypts facts using a fixed of attributes. The receiver on the opposite facet is able to decrypt simplest if the get right of entry to structure he maintains is an aggregate of attributes of the sender. In the above diagram, receiver A is able to decrypt the records for the reason that get entry to structure satisfies the overall combination of attributes of the sender, whilst B does now not [19]. In this, the get admission to shape is infused into the person's secretive key, as an example, (P∧R) ∨S, and a cipher text that is fashioned the use of an characteristic set e.g., P,Q couldn't be decrypted via the person possessing the characteristic set of P,Q but the equal may be decrypted via a person with an characteristic with respect to P,R as the characteristic set [17].

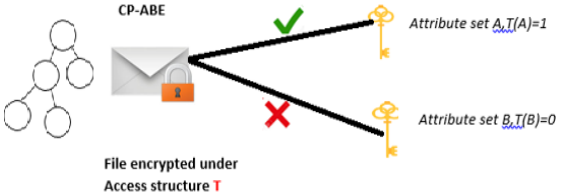

Fig.2.CP-ABE

In Fig.2. In CP-ABE, it isn't always the set of attributes that do the working but the regulations described over a set of attributes deliver the encryption method [19]. In this scheme, User's private key's primarily based on a group of attributes while the cipher text is based on the access shape described over machine unique attributes. A person is capable of decrypt a textual content, if his attributes satisfy the policy specified in the cipher text. Policies are described over attributes the use of conjunctions, disjunctions and n, m-threshold gates, i.e. N out of m attributes have to be present. For instance, the universe of attributes defined over the entire machine are P, Q, R, S and consumer Rushikesh gets a key with respect to attributes P, Q and user Mayuresh with appreciate to attribute S. If a cipher textual content is encrypted based totally on the policy (P∧R) ∨ S, then person Mayuresh is able to decrypt, even as user Rushikesh is not. In CP-ABE there may be no separate get right of entry to manage or authorization mechanism. It is integrated inside the encryption mechanism itself. Users may even gain their secret keys after information encryption the usage of the access shape is an essential upload-on. Hence, statistics can be encrypted even with no longer understanding the real user companies which could decrypt and only specifying the policy is quite sufficient. Future customers are given a key based totally on the attributes people who the policy satisfies and such users are only proper decrypts of the device [17].

IV.PROPOSED SOLUTION

The proposed work is to develop a cloud computing surroundings to provide secured information storage using Multi Factor Authentication for authentication and Cipher Text-Policy Attribute.

Sphurti Atram et al [20] supplied the new concept of ABE referred to as Cipher Text Policy Attribute Based Encryption (CP-ABE). In CP-ABE device, attribute policies are integrated with information’s and attributes are once more incorporated with keys. Only the ones secret keys that are related to the attributes fulfil the policy associated with the records are able to decrypt the statistics. In CP-ABE the cipher textual content is associated with a get right of entry to tree structure and every user mystery key's embedded with a hard and fast of attributes. In ABE, consisting of KP-ABE and CP-ABE, the authority runs the set of rules Setup and Key Generation to generate device MK, PK, and person secret keys. Only authorized users are capable of decrypt by using calling the algorithm Decryption. In CP-ABE, each consumer is related to a hard and fast of attributes. His secret key's generated based totally on his attributes. While encrypting a message, the encryption person specifies the edge access shape for his interested attributes. This message is then encrypted based on this access shape such that only the ones whose attributes fulfil the get right of entry to shape can decrypt it. With CP ABE technique, encrypted data may be kept confidential and comfortable against collusion attacks.

For importing a document, User affords the report as input and the cloud carrier encrypts it the use of CP-ABE algorithm. The detailed running of CP-ABE is seen further. The encrypted file is saved on cloud. The cloud carries the clusters for storage.

a)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.

i)SETUP:

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".

ii) Key Generation:

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.

iii) Encrypt:

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.

Fig.4. gives schematic representation of encrypted session key.

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

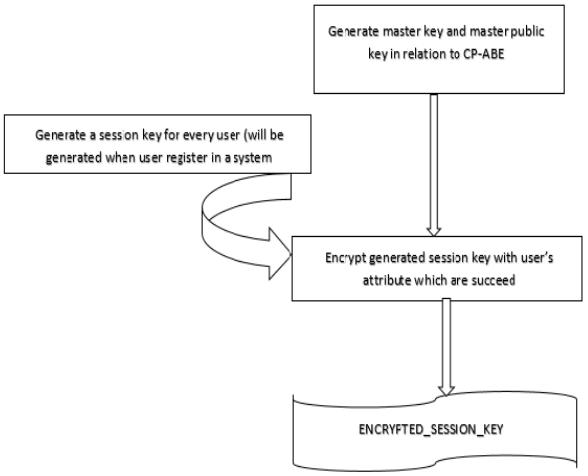

Fig.4.CP-ABE Key generation

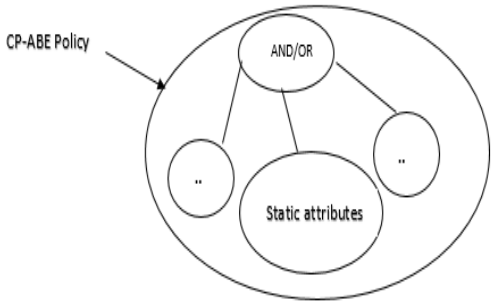

Fig.5.CP-ABE Access policy Scenario

iv)Decrypt:

In this decryption code, PK, a cipher text, which contains a 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. Here, encryption and decryption of contents is achieved using AES algorithm, whereas CPABE encrypt decrypt is used for session key encryption and decryption respectively.

Fig.6. indicates the glide of the encryption and decryption of the file. Step 1 is used to decrypt the consultation key and use this session key for AES encryption of information, however in the get admission to coverage context i.e. The session key context. For decryption, AES decryption of contents is performed the usage of session key for each consumer. Session key decryption is feasible handiest if the attributes in dec_key (within the Key_gen segment) matches the attributes within the access coverage.

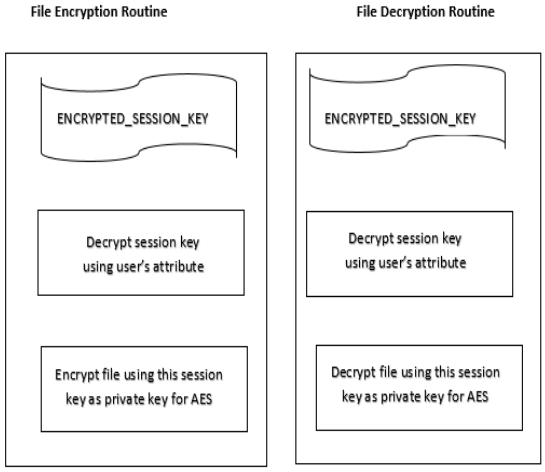

Fig.6.Encryption and Decryption Routine

The proposed machine makes use of attributes for get right of entry to policy introduction in CP-ABE method. The device gives customization in wide variety of attributes for CP-ABE i.e. Variety of attributes can be accelerated or decreased for protection provision. In different phrases, for a superset of attributes five, a person can enter any quantity of attributes (most 5), and encryption of information is accomplished based on enter range of attributes [1].

b)Multifactor Authentication:

The proposed answer includes two strategies: picture primarily based authentication and an OTP based approach.

i Image Based Password Authentication

ii) HMAC- Based One-Time Password

i)Image Based Authentication

The Image-based totally authentication is primarily based on Recognition Techniques. When the consumer registers for first time in an internet web site they pick out set of pics that are smooth to take into account, which includes natural surroundings, cars and many others. Every time the consumer logs into the website, they may be supplied with a grid of pics this is randomly generated. The person can pick out the pics that were previously selected with the aid of him. It is significantly simpler for the person because they need to take into account some simple snap shots simplest.

IBA is primarily based on a consumer's a hit identity of his set of pix. When the consumer logins for the first time, the website displays a grid of snap shots, which includes photos from the person's password set blended with different images. The consumer is authenticated through effectively identifying the password pictures. Performing brute force assaults or different

assaults on such systems may be very tough. A set of various images are decided on to authenticate the person. The Image Identification Set (IIS), for each user is then saved at the Authentication System. When a person logins, the IIS for that person is retrieved and used to authenticate that unique person. The machine does no longer keep the pix but the class of the pictures are saved in IIS as images are massive documents. This technique is likewise greater secure and requires much less memory. If this step is successful, next OTP is generated and send to the consumer electronic mail-id.

ii) HMAC-Based One-Time Password Algorithm

This paper describes a set of rules which is used to generate Time-synchronized OTP values, based on SHA-1 based totally Hash Message Authentication Code (HMAC) or HMAC-Based One-Time Password because here OTP is created based on HMAC. One-Time Password is manifestly one of the simplest and maximum popular kinds of two-thing authentication that can be used for securing get admission to money owed. One-Time Passwords are often referred to as a relaxed and stronger varieties of authentication, and letting them set up throughout a couple of machines inclusive of domestic computers, cellular telephones and so forth. When the user selects the pre-selected pix to login an OTP is generated and sent to the consumer's e- mail identity. The user is then directed to subsequent page where the user is requested to go into the OTP. The consumer receives the OTP the usage of the e-mail account and enters it. If the OTP is demonstrated the user succeeds in logging within the system.

c)Algorithm Requirements:

A-The algorithm must be time synchronized.

B - The algorithm would be reasonable to implement with the aid of reducing the amount of hardware required.

C - The set of rules need paintings with any kind of code generating tokens.

D - The price displayed on the token or any mail message have to be easy to read and entered by way of the consumer. For this the OTP value have to be of affordable duration along with an eight-digit cost. It is appropriate for the OTP fee to be a numeric digit so that it could be easily entered.

E - User-pleasant mechanisms have to be available to resynchronize the time.

d)Algorithm Notation Used:

The notations used in OTP algorithm

Symbol	Represents T is the Time value.
Key	Shared secret key among purchaser and server
Digit	Number of digits in an HOTP value.

e)Description:

The OTP algorithms are primarily based on an increasing time cost characteristic and a static symmetric key recognized best to customer and server. In order to create the OTP price, a HMAC- SHA-1 algorithm is used. Since the output of the HMAC SHA-1 calculation is a 160 bits, we have to truncate this cost to a smaller digit in order that it may be easily entered. Here truncate is used to convert the value of HMAC SHA-1 to an OTP value. OTP (Key,T) = Truncate(ToHex(HMAC- SHA-1(Key,T)))

f) Generation of OTP Value

The algorithm can be defined in three steps:

Step 1: Produce the HMAC-SHA-1 value

Let HMK = HMAC-SHA-1(Key, T) //

HMK is a 20byte string

Step 2: Create a hex code of the HMK.

HexHMK=ToHex (HMK)

Step 3: Remove the 8-digit OTP cost from the string OTP = Truncate (HexHMK)

The Shorten function in Step three does the dynamic truncation and reduces the OTP to 8-digit.

g) Operation

```
MessageDigest md =
MessageDigest("SHA1")
md.update(Key, T)
output = md.digest()
buf = hexDigit((output >> 4) & 0x0f)
otp=buf.toString()
otp=otp.substring(0,7)
```

V.CONCLUSION

This paper offers the cloud to achieve better customization in offerings and data safety methods. Major protection mechanisms are measured on this paper is confidentiality and Multifactor Authentication. Data Confidentiality is accomplished through CP-ABE encryption method. Multifactor Authentication is finished using the combination of Image Based Password and Hash-MAC based totally one-time password. This authentication technique is tremendously

comfortable. The SHA-1 is used for the calculation of HMAC. SHA-1 is most extensively common cryptographic hash function due to its high safety in comparison to other cryptographic hash capabilities which includes MD5 adds to the security of HMAC. Recovery of lost password based totally on secret query and solutions can be a future enhancement

REFERENCES

[1] Rushikesh Nikam and Manish Potey," cloud storage security using multi-factor authentication" IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE- 2016), December 23-25, 2016, Jaipur, India.

[2] Himika Parmar, Nancy Nainan anSumaiya Thaseen," Generation of Secure One-Time Password Based on Image Authentication", Computer Science & Information Technology(CS & IT) –CSCP, pp. 195–206, 2012.

[3] J. Mala, Dr.A.N. Jayanthi, S. Rajesh," A Survey on Secure Data accessing and Sharing Using Cryptographic Algorithms in Cloud Computing Environment ",International Journal of Scientific Research and Engineering Development-– Volume 2 Issue 3, May 2019,pp.452-455.

[4] Nitin, Durg Singh Chuhan, Vivek Kumar Sehgal, Ankit Mahanot," Security Analysis and Implementation of *JUIT– Image Based Authentication System using Kerberos Protocol", Seventh IEEE/ACIS International Conference on Computer and Information Science, pp. 575-580.

[5] Balkis Hamdane, Ahmed Serhrouchni, Adrien Montfaucon, Sihem Guemara." Using the HMACBased One-Time Password Algorithm for TLS Authentication" 978-1-4577-0737-7/11/ ©2011 IEEE.

[6] R. Dhamija and A. Perrig, "Deja Vu: A User Study Using Images for Authentication," in Proceedings of 9th USENIX Security Symposium, 2000.

[7] A. Perrig and D. Song, "Hash Visualization: A New Technique to Improve Real-World Security," in Proceedings of the 1999 International Workshop on Cryptographic Techniques and E-Commerce, 1999.

[8] S. Akula and V. Devisetty, "Image Based Registration and Authentication System," in Proceedings of Midwest Instruction and Computing Symposium, 2004.

[9] D. Weinshall and S. Kirkpatrick, "Passwords You'll Never Forget, but Can't Recall," in Proceedings of Conference on Human Factors in Computing Systems (CHI). Vienna, Austria: ACM, 2004, pp. 1399-1402.

[10] W. Jansen, "Authenticating Mobile Device Users Through Image Selection," in Data Security, 2004.

[11] W. Jansen, S. Gavrila, V. Korolev, R. Ayers, and R. Swanstrom, "Picture Password: A Visual Login Technique for Mobile Devices," National Institute of Standards and Technology Interagency Report NISTIR 7030, 2003.

[12] W. A. Jansen, "Authenticating Users on Handheld Devices," in Proceedings of Canadian Information Technology Security Symposium, 2003.

[13] T. Takada and H. Koike, "Awase-E: Image-based Authentication for Mobile Phones using User's Favorite Images," in Human-Computer Interaction with Mobile Devices and Services, vol. 2795 / 2003: Springer-Verlag GmbH, 2003, pp. pp. 347 - 351.

[14] 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

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

[16] 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

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

[18] 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.

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

[20] Sphurti Atram, N. R. Borkar," A Review Paper on Attribute-Based Encryption Scheme in Cloud Computing," International Journal of Computer Science and Mobile Computing, Vol. 6, Issue. 5, May 2017,260 – 266.

[21] John Bethencourt, Amit Sahai, and Brent Waters. Ciphertext-policy attribute- based encryption. In IEEE Symposium on Security and Privacy, pages 321-334, 2007.