A Dual Security and Protection Mechanism in Cloud Storage

AshishLadda [1]
[1]Assistant Professor in CSE Dept,
Dept, Balaji Institute of Technology & Science,

Sandhya Mekala[2]
[2]Assistant Professor in CSE
Balaji Institute of Technology & science,

Mamatha Kencha [3]
[3]Assistant Professor in CSE Dept,
Vasavi College of Engineering,

Abstract- *Cloud computing is rising technology which provide higher performance and may be use to supply forms of services like computer code as a Service (SAAS), Platform as a Service (PAAS) and Infrastructure as a Service (IAAS) at low price. The difficulty in providing SAAS is security of cloud user's knowledge once it's uploaded on cloud and authentication of cloud user before accessing the info. The plain knowledge isn't on top of things of cloud user once it's uploaded on cloud therefore it's prone to attack from cloud merchandiser itself associated an external aggressor. Additionally plain knowledge in transit is prone to attack. The projected methodology emphasizes on up knowledge security mechanism by implementing Two-factor authentication for shopper & provides encryption that shield knowledge from cloud merchandiser, associate aggressor and knowledge in transit additionally key sharing mechanism facilitate to share non-public knowledge with different cloud user.*

Keywords- Authentication, Cloud computing, Key sharing.

I. INTRODUCTION

Cloud computing refers to provision of procedure resources on demand via a electronic network. cloud computing provides varied services which has package as a service, platform as a service, infrastructure as a service. In ancient model of computing, user's laptop contain each knowledge and package; whereas in cloud computing there's no have to be compelled to contain knowledge and software solely the system desires software and browser. Cloud computing provides varied blessings that embrace economies of scale, dynamic provisioning, raised flexibility, low cost and lots of more[1]. As cloud computing share resources over the network, security is that the basic concern. knowledge house owners store their knowledge on external servers therefore knowledge confidentiality, authentication, access management area unit a number of the essential considerations. to shield user's privacy a method is to use authentication technique like username and watchword. Authentication is to envision user's identity, means that whether or not the person is same as he pretends to be. There area

unit varied authentication strategies and techniques [2]. it's additionally necessary to secure the access to all or any IT system and services. Access management could be a procedure that permits or denies access to a system or services. during this paper associate economical access mechanism mistreatment capability list is introduced. The identification of user's area unit done mistreatment an additional security layer i.e. 2 issue authentication mechanism so as to supply cloud access. the info area unit outsourced to cloud once encoding with trigonal key by the info owner. The CSP and user communicate with one another and generate a shared trigonal key mistreatment sturdy Diffie-Hellman rule. This solves the aim of secure communication between CSP and user's.

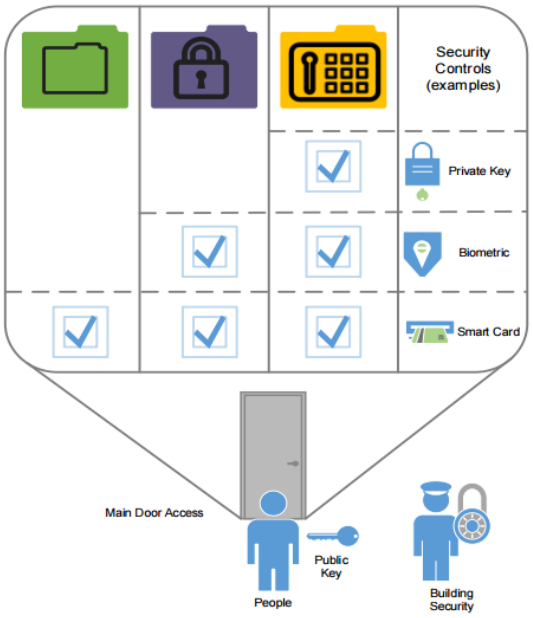

Fig 1: Protection levels

II. RELATED WORK

In the cloud storage mode, information is hold on in a very third-party cloud storage platform, from the information owner (Owner, O) control, that depends on the ISP safe level (Service supplier, SP). ancient information privacy protection methodology is to write user information hold on within the cloud server, like the literature [4-5] so on. Beneath these conditions, once the server-side leak or compromise, it might simply cause information integrity and user privacy speech act threat. Therefore, if the SP can not be trusty, the user has to think about the confidentiality, integrity and privacy protection mechanisms for cloud information storage, that has become a hot topic of analysis in recent years, cloud storage security and privacy protection [5-6]. [7] projected by the information key to write the information, so use the key to write information key. management is that the key during this theme by the key management of third-party managers, there area unit credible and cause key managers key compromise security risks. once the literature [8] Vanish system through the key threshold cryptography process, key slice distributed by Vanish system directly into DHT network. Thus, Associate in Nursing assailant will sniff attack [7] or jump attack [9] get enough key slice reconstructed key. [10] on the Shamir secret sharing rule [11] has been improved by extending the length of the key elements of the system to resist Vanish exist jump attack, mistreatment the RSA public key coding to shield against sniffing attacks. The program will higher solve the literature [7-8] safety defect exists, however in terms of potency and user privacy continues to be scarce. once massive amounts of knowledge hold on within the cloud server, the way to attain economical retrieval of encrypted information has become Associate in Nursing imperative downside to be solved . Song et al projected a searchable initial encrypted security model [12], uses a two-story structure of the encrypted file keywords encrypted.

afterwards, Goh et al projected a good safety index model Z-IDX [13], the model uses a pseudo-random perform, and Bloom filters (Bloom Filter, BF). what is more, Curmola [14] and Chang [15], World Health Organization conjointly use an identical methodology index, during this methodology, every file Associate in Nursing encrypted hash table index, Associate in Nursing index table for every keyword Associate in Nursing consists of an encrypted file that contains the keyword represent a collection of identifiers. Bloom filter methodology by criteria established for every file hash index, and within the cloud server, the tactic will effectively scale back the index terms of cupboard space to store them. supported DHT network, proposes a theme for information security shared cloud storage system, the program combines homomorphism key negotiation mechanism, Shamir secret sharing rule, Bloom Filter combined with the B + tree search rule, Rsync information update rule provides User privacy protection theme supported information sharing beneath a non-public cloud storage conditions. Its main blessings area unit as follows: initial, the key into the key and also the information key, key to write information mistreatment the information by dominant key coding key data. By simplifying the classification key management, increased security keys; 2, mistreatment RSA key negotiation with the state to get the key, the knowledge is complete interactive cipher text, avoiding unreliable thanks to user privacy SP speech act issues; Third, the employment of secret sharing methodology for information cipher text and key cipher text process, multiple cipher text fragment sent to the DHT network, avoiding the fragmentation caused by harm to or loss of knowledge unrecoverable issues. Fourth, by finding rule BF and B + combining the employment of BF rule is economical area utilization and B + tree quickly pinpoint characteristics, are able to do the information for economical storage access, and quickly and accurately find; 5, mistreatment Rsync synchronization update rule, DHT network node dynamically updated information, we tend to propose a DHT node information effectively extend the validity of the new mechanism to effectively forestall the information thanks to DHT network disturbance and loss.

III. EXISTING SYSTEM

Now a days Cloud storage is understood as a promising resolution for providing convenient, universal, and on demand access to bigger amounts of knowledge shared on the net. In existing system, they introduced a two-factor security protection mechanism for information keep within the cloud. System is predicated on Identity-Based cryptography (IBE) mechanism. The sender needs solely the identity of the receiver to send associate encrypted information. Sender send cipher-text through the cloud to the receiver then receiver will transfer cipher text at any time. Existing system accommodate two-factor encryption protection technique. Encrypted information keep during a cloud, receiver accessed encrypted information and convert into decrypted information that point it'll needed 2 things: very first thing, user secret key that is send by sender through a secure channel (e.g., email). Second issue, user desires distinctive personal security device to attach the pc like USB. The system user needed a security device then it'll request for security device to the protection device establishment (SDI) suppose device is stealing or loss then user report back to SDI, subsequently establishment revoked personal security

device of user and afford a brand new distinctive or personal security device to user.

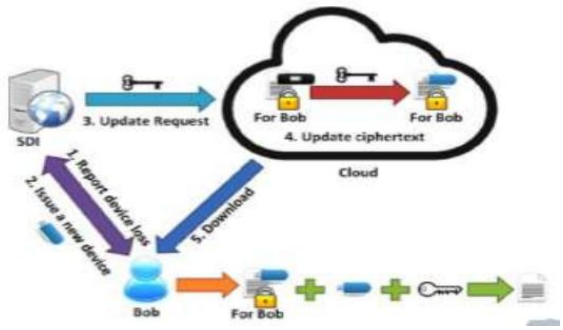

Fig2: Existing system overview

IV. PROPOSED IMPLEMENTATION SYSTEM

This section focus on detailed explanation of proposed system which helps in tacking security issues of authentication, privacy of user data.

A. REGISTRATIONAND AUTHENTICATION MECHANISM

In a typical word authentication theme, the server has the power to permit or forestall any remote user supported username and word. The weakness of word authentication system is, it will be break and really abundant susceptible to attack. Passwords have suffered from attacks like lexicon or brute-force attacks. In registration mechanism, new users aren't asked to submit Associate in Nursing documents to open an account. they will submit on-line registration type which has user info in conjunction with email-id, even as we have a tendency to off whereas gap Associate in Nursing email account. Then user info can get keep in cloud wherever word gets keep in hash format so if any attack on word would be ineffective. when registration consumer should manifest with the CSP at the time of victimization service.

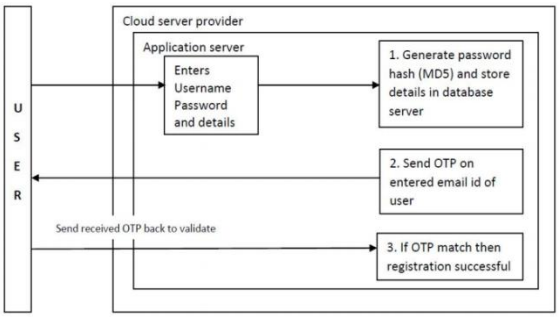

Fig 3: Registration mechanism

Authentication factor 1 In this client has to provide username and password which client has entered at the time of registration. Authentication factor 2 In this level CSP send OTP on clients registered email-id. After two authentication levels are cleared then only client is allowed to access cloud service.

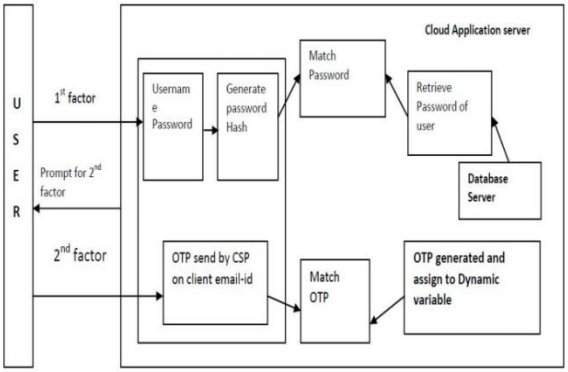

Fig 4: Two factor authentication mechanism

B. STORING AND ACCESSING OWN DATA

Once user is echo to the Cloud Server, user will access the file storage and may transfer any sort document within the cloud storage. Here the file is 1st encrypted before uploading and also the same is decrypted at the time of downloading. Or user will easy store original format get in common folder that he/she needs to share with alternative each user directly without concern regarding key sharing

mechanism Uploading encrypted file If user is each then cloud server can load module to purchasers finish to perform coding operation. Here consumer transfer encrypted file on cloud server non-public folder mistreatment bilaterally symmetrical key coding technique. At the time downloading encrypted file user can raise to supply the coding key if secret's valid then solely file can get downloaded at purchasers finish. This coding and coding of information are done at consumer aspect by creating use of a bilaterally symmetrical key thus it's unfeasible for CSP to achieve access to key thus notwithstanding the info hold on is in write in coded format and also the algorithmic rule wont to encrypt it's offered to cloud, it's tough to rewrite it. User is assured regarding security of information hold on in cloud. This ensures information privacy of personal compartment. Uploading plaintext file At the time of uploading plain computer file user needn't worry regarding coding. Here cloud can load Emodule to purchasers finish upon request so user will choose file to transfer. User will store file to either common folder or non-public folder. At the time of downloading the file user will merely request file without concern regarding coding key.

C. DATA SHARING BETWEEN CLOUD USERS

In this scheme cloud user can share file which is stored in private folder with other authenticated cloud user.

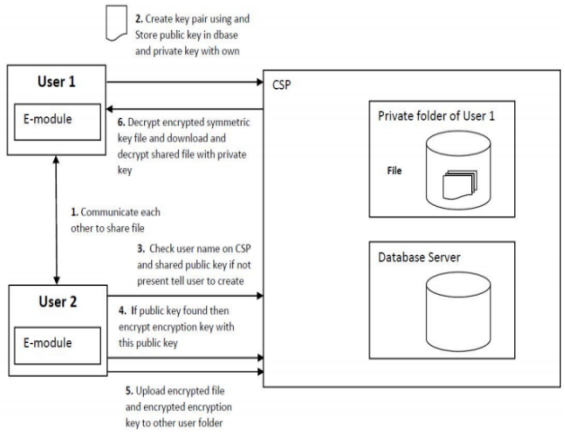

Fig 5: data sharing between cloud users

Here first cloud user request file to second cloud user by using any communication media which is possible. Then first user creates sharing key and store that in folder created on cloud. Then second user check sharing key and encrypt that encryption key with sharing key then second user send requested encrypted file and encrypted encryption key to first user. On the first user side when he receives the encrypted file and encrypted encryption key then he first decrypt the encryption key with own private key then he get encryption key which can be use for decryption of encrypted file

V. CONCLUSION

This paper conferred a group of security procedures to secure the information of an information owner in cloud. The combined approach of access management and cryptography is employed to safeguard outsourced information. Our theme conferred a capability primarily based model for access management mechanism. additional layer of security is provided for users and cloud victimization 2 issue authentication approach. therefore the planned theme make sure that solely the registered users might access the requested service victimization

mobile phones as an additional accessorial security. sturdyDiffie- dramatist procedure to access outsourced information expeditiously and firmly from CSP.

REFERENCES:

[1] Gartner, "Newsroom: Consumers Will Store More Than a Third of Their Digital Content in the Cloud by 2016," Press Release, 2012.

[2] CSA, "Top Threats to Cloud Computing V1.0," 2010. s

[3] CSA, "Cloud Computing Vulnerability Incidents : A Statistical Overview," 2013.

[4] GTISC and GTRI, "Emerging Cyber Threats Report 2014," 2013.

[5] F. Sabahi, "Cloud computing security threats and responses," 2011 IEEE 3rd Int. Conf. Commun.Softw. Networks, pp. 245–249, May 2011.

[6] F. Bashir Shaikh and S. Haider, "Security Threats in Cloud Computing," 6th Int. Conf. Internet Technol. Secur.Trans. Abu Dhabi, UAE, no.December, pp. 11–14, 2011.

[7] YashpalsingJadeja, KiritModi, "Cloud Computing - Concepts, Architecture and Challenges", 2012 International Conference on Computing, Electronics and Electrical Technologies [ICCEET], pages 877-880, 2012

[8] Christian Baun, Marcel Kunze, "Building a Private Cloud with Eucalyptus" Steinbuch Centre for Computing, Karlsruhe Institute of Technology 2010

[9] Mahatebba, Said EL Hajji, Abdellatif EL Ghazi ,"Homomorphic Encryption method applied to Cloud Computing", Network Security and Systems (JNS2) Conference IEEE, Pages 86-89, April 2012

[10] Sunil Sanka, ChittaranjanHota, MuttukrishnanRajarajan, "Secure data access in cloud computing", 978-1-4244-7932- 0/10/$26.00 ©2010 IEEE

[11] Yubo Tan , Xinlei Wang, "Research of Cloud Computing Data Security Technology" , 978-1-4577-1415-3/12/$26.00 ©2012 IEEE, pages 2781-2783,2012

Authors:

AshishLaddais 4+ years experienced Assistant Professor in the Department of Computer Science & Engineering, BALAJI INSTITUTE OF TECHNOLOGICAL SCIENCES-NARSAMPET, Warangal, India and his Research area includes Cloud Computing , IoT, Data Mining , Network Security etc.,

SandhyaMekalais 4+ years experienced Assistant Professor in the Department of Computer Science & Engineering, BALAJI INSTITUTE OF TECHNOLOGICAL SCIENCES-NARSAMPET, Warangal, India and her Research area includes IoT, Networks, Network Security etc

MamathaKencha is Assistant Professor in the Department of Computer Science & Engineering, Vasavi college of engineering, Hyderabad.