International Journal of Trend in Research and Development, Volume 6(1), ISSN: 2394-9333
www.ijtrd.com

Analysis of Cryptographic Technique for Securing Distributed Data Storage in Cloud Computing

Manjunatha Gowda
Department of Computer Science, M.G.R College (Arts & Science, Affiliated To Periyar University, Salem -11), Hosur, India

Abstract: In the internet era, the data storage sources are taken to a place where the user or enterprise has less control with respect to maintaining utilities, hardware, hypervisors and software applications. This place is called cloud which has many benefits like automatic resource scaling, sharing same resources with multiple tenants, billing similar to utilities, bringing various huge resources together and which can be accessed everywhere over the internet. However, cloud computing carries many risks along – like data security, infrastructure security, application security, jurisdictions based security and other daily operational based. In this research, security related to data in cloud has been considered where while moving or storing there is a chances of stealing it with various unauthorised manner. The proposal is to use encryption with multifactor authentication together which provides high security even will be double. The method of combining both technologyis described with scope for further future enhancement. While is multifactor even there is a touch of using biometric as one component which is unbeatable in this time.

Keywords: *Cloud Computing, Encryption, Security, Symmetric, multifactor*

I. INTRODUCTION

Since 2006 when the first cloud computing concept introduced by Amazon, there were various security methods evolved to protect the data within cloud from preying eyes in and around the world. Encryption is the primary security method came along cloud to protect the data while in movement and also at rest. There were various encryption algorithms developed over the period which was adopted in cloud computing. To name few AES, RSA, Blowfish, DES and Homomorphic encryption which is still under development which provides on the fly encryption mechanism of data not even being necessity to decrypt it. The methodology proposed here will make use of encryption with multifactor authentication, a method which adds second level protection to the data. While talking about multifactor, using of what we have (Normally it is password) and what we know (The code generated during the time of authentication). Normally when data is stored in cloud from the cloud user (An Enterprise or a User) technologies are there to encrypt data. ENCRYMUL mechanism boosts this process by adding a layer over the encryption by adding user's most unique identities like biometrics or token codes.

II. REVIEW OF CURRENT LITERATURE SURVEY IN THE CLOUD COMPUTING STORAGE

In the normal cloud architecture there are 4 deployment models – Private Cloud, Public Cloud, Hybrid Cloud and Community Cloud. All of these models threat of data loss and breach are common and different levels as

- **Private Cloud** – The cloud is owned by single organisation within its security boundary, need for data protection is for the data at rest most of the time
- **Public Cloud** – The Cloud is for use of public organisations, in this model the threat is more where resources might be shared between many users/companies as public cloud is shared architecture
- **Hybrid Cloud** – Again the risk is combination of above both model where a single organisation with its private cloud extends its storage to public for spike of utilization. Whenever there is a spike in utilisation the cloud will burst to public where the protection required is more
- **Community Cloud** – Most like private but here organisations of same community like banks or sister companies come together to form cloud, again the risk factor of protection required is same as above models

With deployment model there is a brief introduction required for service models where the threat modelling will be in a different angle. The Service models are;

- IaaS – Infrastructure are sold to customers with Processing, Storage and ability of building the servers and application are given to customer
- PaaS – Platforms with ready environment for development will be sold to customer with OS and base devops
- SaaS – Ready-made services like email (Office 365), CRM (Salesforce) are under this category

As mentioned above, the encryption mechanisms like DES are prone to brute force attack provided enough time to crack it. Over all cloud is open to various security threats in which the main are – Data breaches, Data loss, Data can be viewed by Government agencies without proper consent from the data owner, DDoS Attacks, Malicious Insider Users, Compliance and Various jurisdictions adding more restrictions, Insecure Access points and System Vulnerabilities. In the listed challenges all the majority of challenges are due to not properly able to protect the data which lead to those attacks and breaches. That is when the idea of ENCRYMUL has born which invokes 2nd level of authentication wherever data flows during transaction happens in cloud from user end. Now it is present in different strategies where the idea is to bring them together to get robust data protection with top most security.

In the current encryption methodology and key storage technique, there are various views. As per the standards, encryption keys should be held with the data controller/owner. It has to be safely handled by the data owners. If the keys are compromised, it is top most threat to the data of any company. Using those keys the entire data can be compromised and stolen.

Generally there are 3 methods of key handling in any encryption solution which is left to the data owner to decide which one to choose. Firstly key and data are storedalongside to provide faster retrieval of data. In this the processing speed of data is more as key is available within the data storage. But this is prone to vulnerable if the entire storage system gets co promised.

Secondly "Key Escrow" service where a third party whose job is to handle all the keys related to customer or data owner where he will be solely responsible for all the encryption keys but data will be stored in the cloud provider. Here the cloud provider has no idea of the key and hence data is mostly protected but if the key escrow service is compromised, then the data can be stolen.Also if the key escrow will have full access to data if they wish to attack. This way is to keep the keys with data owner in the on premise key server. Here the challenge is to maintain the server, if the server is crashed, access to entire data is gone! Hence chances of data loss or breach are more

Again where is this secure? Once someone authenticates and get the encryption key for the data, they have unlimited access to the data that is protected. In any encryption model they uses a 2-shared key, where the first factor (password) is generating key1, then the second factor, like a OTP authenticator, is used to authenticate at the administrator, and key2 (the token) is generated. Then the 2 keys are combined in a way, like key1 XOR key2, and gives key3. Key3 gives access to data.

Any hacker who want to break the system, could ensure the real user authenticates successfully. After this, key1 and key2 is copied, and thus the two-factor authentication is bypassed as the entire information is available in the same session.

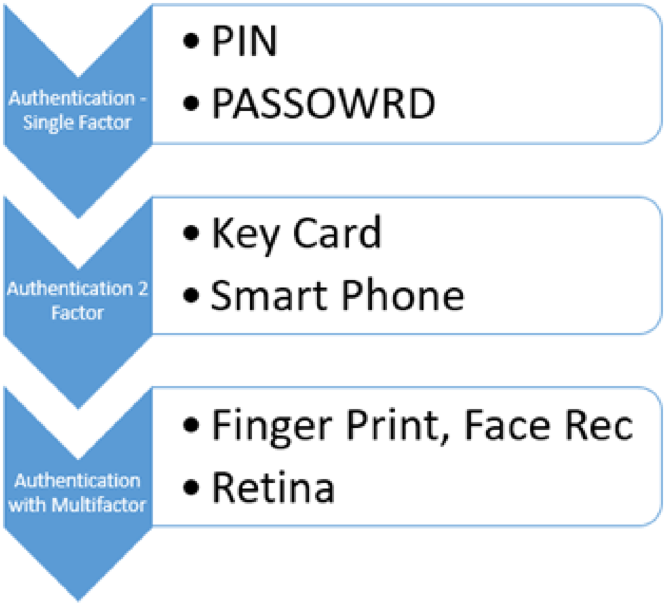
For two-factor to be really two-factor, the physical second-factor must have a property, ensuring that the secret key cannot be extracted, rather disk data has to be fed through the second factor. In other Words, like a HSM. This ensures that the two-factor requirement is enforced at all times, and that you could even lend out the second factor to someone that needs temporary access, and once the access is revoked, the second factor is taken back and then the hacker is guaranteed to no longer have access to the data.

A smart card is too slow, which need some disk encrypting solution that uses some sort of high capacity HSM (Hardware Security module) that is inside a little key that is inserted. For the "what you know" factor, a PIN can be used. Using a Smart card or HSM, that stores a "master key" securely, but is used to decrypt a "disk key" that is later used to decrypt data, isn't secure either, since a hacker could just ask the smart card or HSM to decrypt the disk key for them and then they have full access, even when they lost access to the Smart card or HSM.

Authentication flow in any client – cloud server model while beginning any transaction. Example of an Multifactor encryption is Microsoft BitLocker which supports TPM + PIN unlock, whereby a combination of a decryption key stored in the hardware (something you have) and a password / PIN entered at start-up (something you know) are together used to decrypt the boot volume.

Clearly full-disk encryption requires authenticating users before the OS boots, so interactive challenge-response protocols involving a remote host won't work. But I don't see any insurmountable obstacles to implementing a secure, pre-boot one-time password mechanism.

Proposed Method:

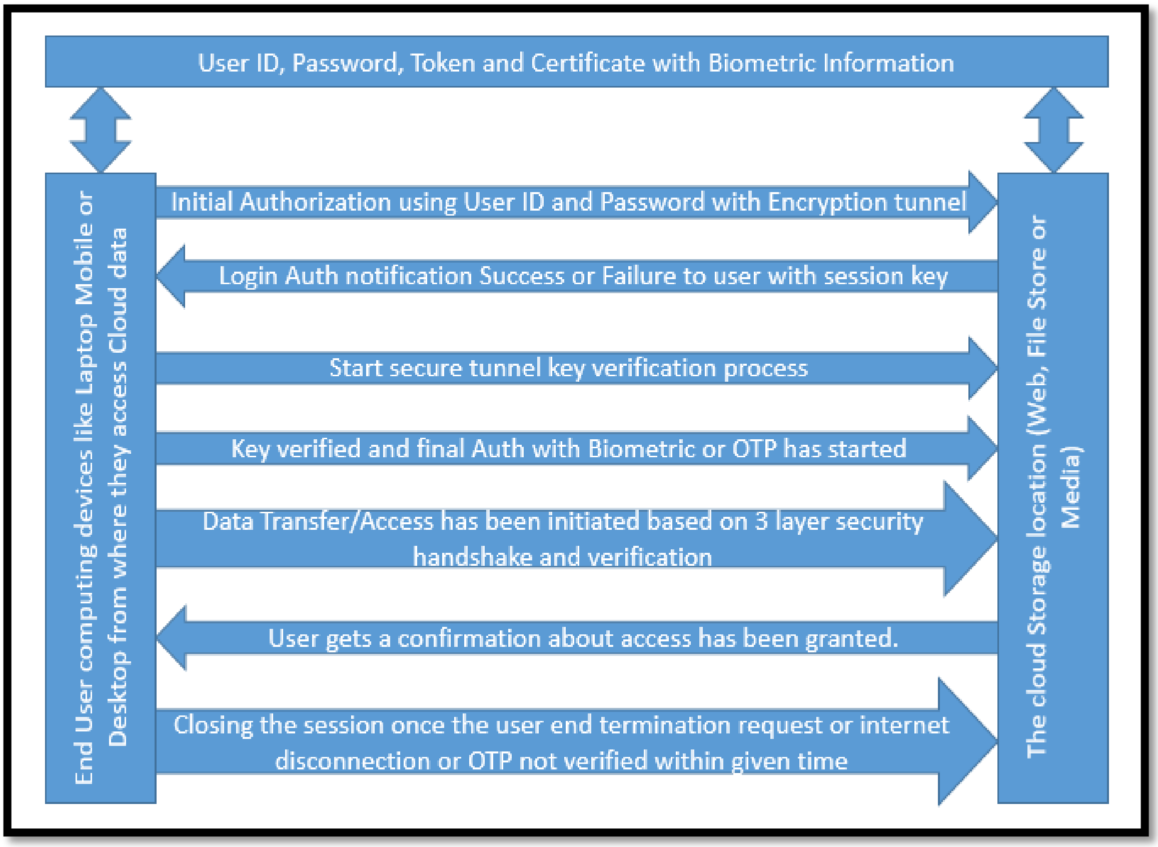


In the proposed method there are 3 layer security has been proposed to over come different deployment, service model or location of data. First level is to encrypt data with symmetric key combination. In this the key will be stored in a HSM device (Hardware Security Model) which is the most secured model till today.

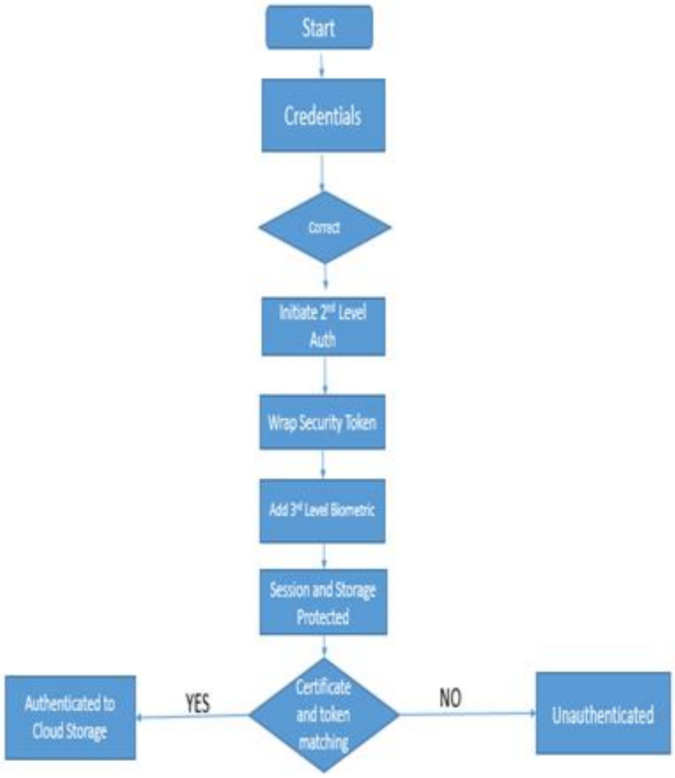
Steps are as follows which will be used to securely access data in a single session. Where;

1. User opens session by entering URL or any client from his end using computer to access cloud to get any kind of data (Text, Document, Video or Audio)
2. When prompting for password user enters his user ID and password – Level 1
3. The credentials are passed to cloud server where the encrypted data requests 2nd layer security either biometric token or OTP based
4. The server then hand shake with biometric and send the token to HSM for double check
5. Based on the pre-loaded key in HSM, it requests final verification token chain from user which is a RSA or OTP which will be instant key to verify and start session
6. Once the session is open data transmission happens either on a certificate or continuously varying biometric sequences to stop any kind of hijacks if at all
7. 2 layers will be continuously transmitting the data while th e 3rd layer will be continuously varying and stopping hacker not to gain any session hijacks.
8. Stopping sessions and transmission so that no active session left for providing 3rd party any option to crack

When the session is over the client disconnects every transmission signal to the server to avoid any kind of left over information which might get compromised. Based on the availability of data and session the time will be calculated for live activity.


User ID, Password, Token and Certificate with Biometric Information
End User computing devices like Laptop Mobile or Desktop from where they access Cloud data
Initial Authorization using User ID and Password with Encryption tunnel
Login Auth notification Success or Failure to user with session key
Start secure tunnel key verification process
Key verified and final Auth with Biometric or OTP has started
Data Transfer/Access has been initiated based on 3 layer security handshake and verification
User gets a confirmation about access has been granted.
Closing the session once the user end termination request or internet disconnection or OTP not verified within given time
The cloud Storage location (Web, File Store or Media)

While encryption is the core while protecting data in our solution it is used with multifactor and certificate based key protection preferably using a HSM.



CONCLUSION

As discussed above the protection of cloud data with single factor of authentication and one level of encryption is out of date now. Hence the ENCRYMUL technique of combining encryption with session key and verifying the data transmit with help of another layer of security like biometric or certificate based is proposed. As always there is scope for further enhancement of the technology to speed up data access with on the fly decryption technology which is already incorporated by many cloud vendors in their test environment.

References

[1] O'Hara, B. and Malisow, B. (n.d.). CCSP (ISC)2 certified cloud security professional.

[2] Cloud Security Alliance. (2018). CSA Security Guidance for Critical Areas of Focus in Cloud Computing v4.0 - Cloud Security Alliance. [online] Available at: https://cloudsecurityalliance.org/guidance/ [Accessed 1 Sep. 2018].

[3] NIST. (2018). Final Version of NIST Cloud Computing Definition Published. [online] Available at: https://www.nist.gov/news-events/news/2011/10/final-version-nist-cloud-computing-definition-published [Accessed 1 Sep. 2018].

[4] Tresorit Blog. (2018). Experts on the GDPR #4. Storing encrypted personal data in the cloud. [online] Available at: https://tresorit.com/blog/gdpr-storing-encrypted-personal-data-cloud-secure-option/ [Accessed 1 Sep. 2018].

[5] CEBIT. (2018). How to Delete Data from the Cloud - Cloud Applications. [online] Available at: https://www.cebit.de/en/news-trends/news/how-to-delete-data-from-the-cloud-1050 [Accessed 1 Sep. 2018].

[6] Owasp.org. (2018). Category:OWASP Top Ten Project - OWASP. [online] Available at: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project [Accessed 1 Sep. 2018].

[7] Cloud Security Alliance. (2018). The Notorious Nine: Cloud Computing Top Threats in 2013 - Cloud Security Alliance. [online] Available at: https://cloudsecurityalliance.org/download/the-notorious-nine-cloud-computing-top-threats-in-2013/ [Accessed 1 Sep. 2018].

[8] Ntt-review.jp. (2018). Cryptographic Techniques that Combine Data Protection and Ease of Utilization in the Cloud Computing Era | NTT Technical Review. [online] Available at: https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201210fa3.html [Accessed 1 Sep. 2018].

[9] Nikolova, I. (2018). Data Security Challenges in Cloud Computing. [online] Patecco.com. Available at: https://www.patecco.com/en/blog/data-security-challenges-in-cloud-computing [Accessed 1 Sep. 2018].

[10] Skyhigh. (2018). Only 9.4% of Cloud Providers Are Encrypting Data at Rest. [online] Available at: https://www.skyhighnetworks.com/cloud-security-blog/only-9-4-of-cloud-providers-are-encrypting-data-at-rest/ [Accessed 1 Sep. 2018].

[11] Tresorit Blog. (2018). Experts on the GDPR #4. Storing encrypted personal data in the cloud. [online] Available at: https://tresorit.com/blog/gdpr-storing-encrypted-personal-data-cloud-secure-option/ [Accessed 1 Sep. 2018].

[12] Lifehacker.com. (2018). [online] Available at: https://lifehacker.com/the-best-cloud-storage-services-that-protect-your-priva-729639300 [Accessed 1 Sep. 2018].

[13] Combining Two Factor Authentication and Public Key Encryption to Ensure the Authentication in Cloud Computing. (2018). International Journal of Recent Trends in Engineering and Research, pp.118-121.