Journal of Data Acquisition and Processing
ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.98549455

COMPARATIVE STUDY AND SECURE DATA SHARING TECHNIQUES FOR CLOUD COMPUTING STORAGE

N.Krishnaveni[1], Jayakumari. C[2]
[1]Research Scholar, Department of Computer Science, Bharathiar University, Coimbatore.
E-mail-krishnavenivalliappan@gmail.com
[2]Associate professor, Department of Computing, Middle East College, Oman.
E-mail-jayakumari@mec.edu.om

ABSTRACT

Cloud based communication is a tremendous growth in the world and which provides the services through virtualized resources with support of internet. In cloud computing, optimized storage techniques require to store the huge amount of data. Eliminating the redundant data file from the optimized storage, which results the minimizing the bandwidth and reduces the cost and disk usage. In Existing approach, the most of the research work are using Attribute Based Encryption to prevent the data security. However, the security protection issues during the Attribute Based Encryption are considered as challenging task. In the traditional method of cloud data storage, the data are usually encrypted in the server side and then securely stored in remote server. Many researchers proposed many algorithms in which it makes easier for user's convenience so that it makes them fulfil their requirements. In, this proposed work detailed comparative study for data Sharing techniques in cloud storage are analysed. The results indicate that the cloud computing allows the users to perform the limited outsourcing performance of computational task with extraordinary server. Our proposed Sharing scheme enhances to improve a secured connection for attribute-based encryption for an emerging source to use and it proved the secured against the application system.

Keyword: Cloud Communication, data Sharing, Encryption, Authentication, optimized storage.

I. INTRODUCTION

In last few years, people and objects have been communicating with one another using a new technology called Cloud Computing Technology. The operations in Cloud Computing technology has quickly developed nowadays. The Information Technology organization is not similar like other industries because, it is a sector which is of high priority where the customers expect very high level of quality, integrity, security and service. But, till now this did not satisfy the expectations socially even though it is allocated with large percentage of budget. With the rapid technology development, the cloud computing plays the vital role in many applications such as Information Technology Industry, Healthcare technology and so on. In cloud computing, clients will provide the data for storage and other business purpose, from this acted as the trusted commercial enterprise. Cloud-based services such as Platform as a Service (PaaS) and Software-as-a-Service (SaaS). The other cloud industry provider services are IBM's Blue Cloud and Amazon's Elastic Compute Cloud (EC2). These cloud service providers allow users to access the several applications based upon cloud services on demand. In general, the Cloud Computing offers to compute as a service. It shares the resources, software and data through the network or internet. The testing applications specifically implemented to run on the cloud platform. The Cloud Computing model promising to improve the reliability, availability, collaboration, agility and scalability in both academia and industry.

In cloud Computing, Data Sharing scheme provides the optimized storage data. So, the performing the Sharing scheme over the encrypted data considered as challenging task. The methodology of data Sharing is illustrated in Figure 1. The data Sharing methodology categories into division of data, location of data and Time data.

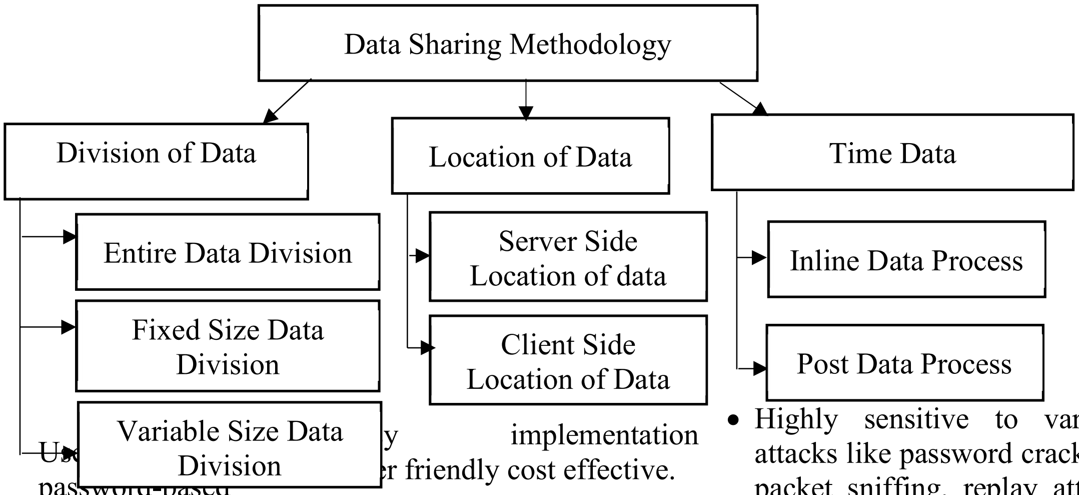


Figure 1. Data Sharing Methodology

A. Data Division – The process of splitting the data into blocks in order to avoid redundant data known as data division. It can further divide into three categories,
   a. Entire Data Division – This strategy is based on mathematical hash indexed operations to avoid the redundant data without splitting the data.
   b. Fixed Size Data Division – This strategy is based on mathematical checksum technique to avoid the duplication data by splitting the data in equal block.
   c. Variable Size Data Division – This strategy is done by without fixing the boundary values and good for backup purpose.

B. Location of Data – In Cloud, the data are stored in two locations named as client side location and server side location. By this Sharing scheme is done.
   a. Client Side Location of Data – This strategy is based on spectral program to avoid the redundant data in Client side. The main purpose of this process is minimizing the bandwidth.
   b. Server Side Location of Data – This strategy is based on Sorting process to detect the Sharing data in server side.

C. Time Data – For Computing and processing the data in Cloud computing, the time complexity considers as important factor. It can be categories into two types based on time complexity named as Inline and Post data process.
   a. Inline Data Process – This strategy also known as before sorting process. This can be done on client side location of data.
   b. Post Data Process – This strategy also known as after sorting process. This can be done on server side location of data.

Method	Benefits	Challenges
Username & password-based authentication	• Easy implementation • User friendly cost effective. • Commonly used in various web applications.	• Highly sensitive to various attacks like password cracking, packet sniffing, replay attack, identity theft, pattern recognition etc.
One time pass-code authentication	• Strong against Man-in-the-middle attack. • Provides complete protection during login phase.	• Vulnerable to masquerading (stealing the password from the storage location attack.
Biometric authentication	• User need not to remember any cryptographic words. • Sole property of an individual	• Selection of human organ is very important.
Certificate based authentication	• Minimal involvement of the user. • No extra hardware is required. • Highly compactable.	• Performance degradation due to large user groups (SSL SPIKES). • Not suitable for bulk file transfer.

In this paper, authentication mechanism of secure data Sharing in cloud storage is analysed. This manuscript is organized as follows, Section 2 illustrate the literature survey works with comparative detailed study, Section 3 describes the proposed methodology work flow, followed by results are narrated in section 4, conclusion is described in section 5.

II. RELATED WORKS

The Table 1. Describes the Comparative study of Sharing schemes through Encryption process. Table 2. Describes the Analysis of the authentication schemes for Sharing techniques.

Table 1. Comparative study of Sharing schemes through Encryption process

S. No	Author & Year	Focused Area	Considered Parameter	Encryption Method used	Sharing Techniques used	Environment	Tool Used
1	Vishalakshi et al., (2017)	Secure Sharing in convergent based encryption for cloud storage	Security, Bandwidth & storage capacity	Authorized duplicate check Encryption	At File level	Cloud Environment	Java
1	Bellare et al., (2013)	Secure Sharing in message based encryption for cloud storage	Security & Storage space	Locking Message Encryption	At File level	Cloud Environment	Java
2	Chen et al., (2015)	Secure Sharing in message based encryption for cloud storage	Security	Locking Message Encryption	At Block level	Cloud Environment	Java
3	Miguel et al., (2015)	Secure Sharing in homomorphic encryption for cloud storage	Security	Encryption based on homomorphic	At File level	Cloud Environment	Java

4	Bellare et al., (2013)	Secure Sharing in server based encryption for cloud storage	Security & Privacy	Prevents the brute force attack by message based encryption	At File level	Cloud Environment	Java
5	Puzio et al., (2013)	Secure Sharing in convergent based encryption for cloud storage	Security & Efficiency	Encryption based on convergent mechanism	At File level	Cloud Environment	Java
6	Li et al, (2015)	Secure Sharing for improving the reliability in cloud storage	Security, Bandwidth & Reliability	Secret sharing Encryption	Both File and Block level	Cloud Environment	Java

Table 2. Analysis of the authentication schemes for Sharing techniques

Method	Benefits	Challenges
Username & password-based authentication	• Easy implementation User friendly cost effective. • Commonly used in various web applications.	• Highly sensitive to various attacks like password cracking, packet sniffing, replay attack, identity theft, pattern recognition etc.
One time pass-code authentication	• Strong against Man-in-the-middle attack. • Provides complete protection during login phase.	• Vulnerable to masquerading (stealing the password from the storage location attack.
Biometric authentication	• User need not to remember any cryptographic words. • Sole property of an individual	• Selection of human organ is very important.
Certificate based authentication	• Minimal involvement of end user. • No extra hardware is required. • Highly compactable.	• Performance degradation due to large user groups (SSL SPIKES). • Not suitable for bulk file transfer.

Shashi Mehrotra Seth & Rajan Mishra (2019) studied the detailed comparative analysis of encryption techniques in cloud storage. The performance metrics of memory usage, computation time and output bytes for encryption techniques is analysed and evaluated.

The demerits of the previous research works are understood clearly from this literature study and hence suitable computational techniques are to be developed and justified with performance metrics.

III. PROPOSED METHODOLOGY

In recent years, health care research based on a cloud-based system of health information that leads to concerns of privacy and protection. Safe sharing of health information in a cloud environment among individuals remains an open challenge. This research focuses on security systems and privacy protection mechanisms to resolve this problem in the cloud environment to ensure safe sharing of personal health information in the cloud to avoid the Sharing data. The Figure 2. illustrate the Framework workflow for Encryption-Based Secured Data Sharing in Sharing technique.

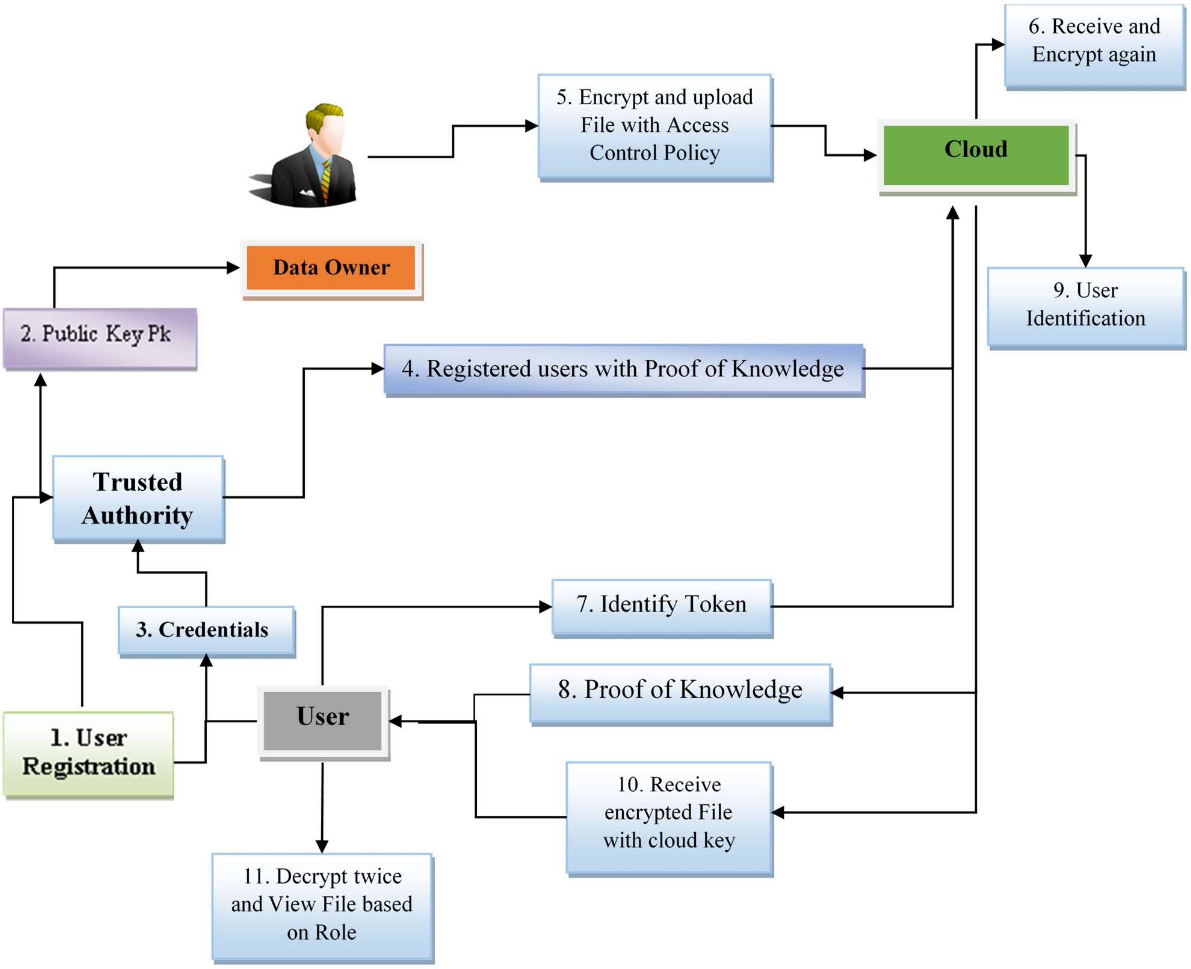
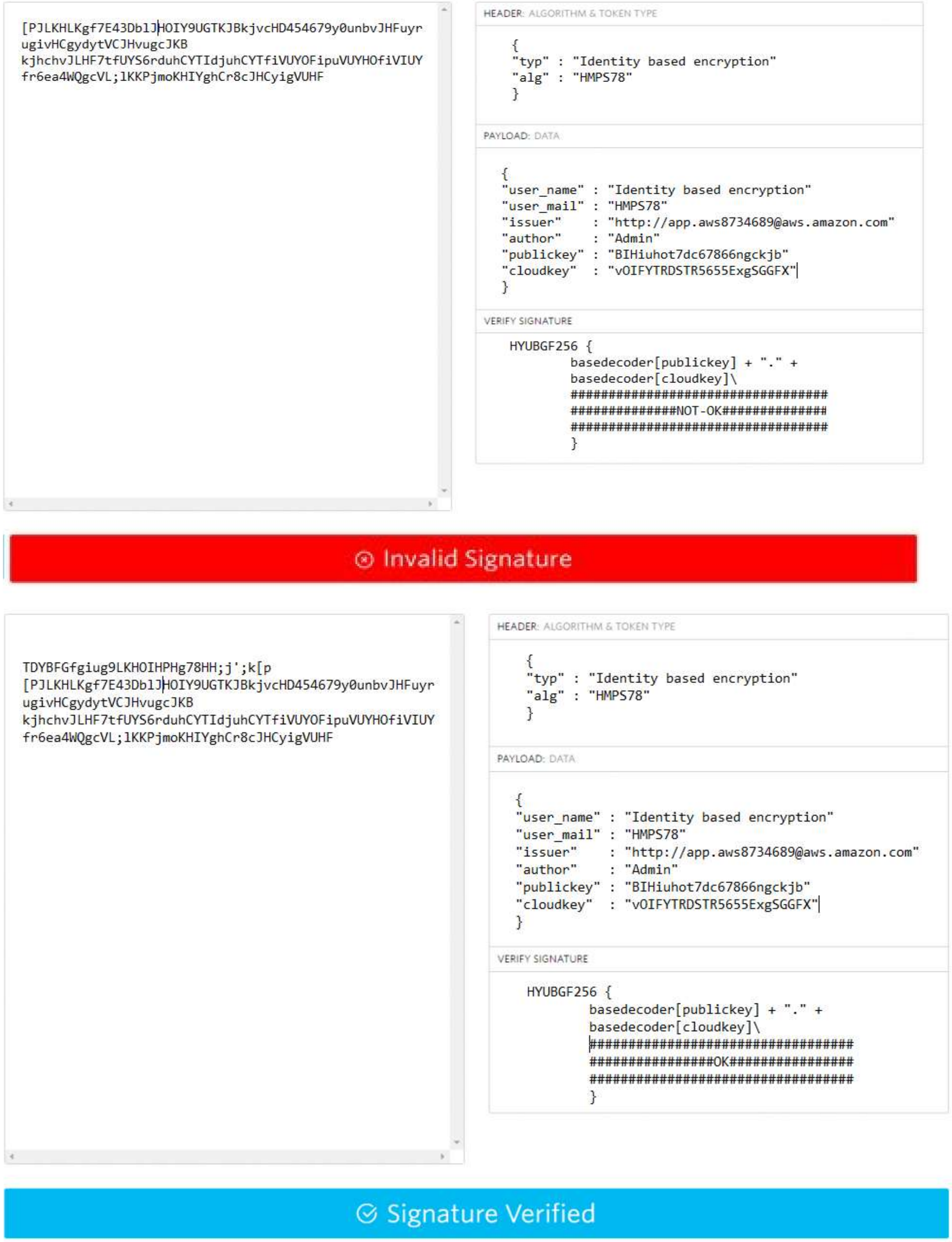

6. Receive and Encrypt again
5. Encrypt and upload File with Access Control Policy
Cloud
Data Owner
9. User Identification
2. Public Key Pk
4. Registered users with Proof of Knowledge
Trusted Authority
7. Identify Token
3. Credentials
8. Proof of Knowledge
User
1. User Registration
10. Receive encrypted File with cloud key
11. Decrypt twice and View File based on Role

Figure 2. Framework workflow for Encryption-Based Secured Data Sharing in Sharing technique

IV. RESULTS & DISCUSSION

For the implementation of the new key system, Amazon Web Service cryptographic services is used. The advanced encryption standard's symmetric algorithm is used as AES-GCM using the Galois/Counter mode. This is focused on mathematically solving the issues using the parameters of the function.



```
[PJLKHLKgf7E43DblJHOIY9UGTKJBkjvcHD454679y0unbvJHFuyr
ugivHCgydytVCJHvugcJKB
kjhchvJLHF7tfUYS6rduhCYTIdjuhCYTfiVUYOFipuVUYHOfiVIUY
fr6ea4WQgcVL;lKKPjmoKHIYghCr8cJHCyigVUHF
```

```
{
"typ" : "Identity based encryption"
"alg" : "HMPS78"
}
```

```
{
"user_name" : "Identity based encryption"
"user_mail" : "HMPS78"
"issuer"    : "http://app.aws8734689@aws.amazon.com"
"author"    : "Admin"
"publickey" : "BIHiuhot7dc67866ngckjb"
"cloudkey"  : "vOIFYTRDSTR5655ExgSGGFX"
}
```

```
HYUBGF256 {
        basedecoder[publickey] + "." +
        basedecoder[cloudkey]\
        ###################################
        ###############NOT-OK##############
        ###################################
        }
```

```
TDYBFGfgiug9LKHOIHPHg78HH;j';k[p
[PJLKHLKgf7E43DblJHOIY9UGTKJBkjvcHD454679y0unbvJHFuyr
ugivHCgydytVCJHvugcJKB
kjhchvJLHF7tfUYS6rduhCYTIdjuhCYTfiVUYOFipuVUYHOfiVIUY
fr6ea4WQgcVL;lKKPjmoKHIYghCr8cJHCyigVUHF
```

```
{
"typ" : "Identity based encryption"
"alg" : "HMPS78"
}
```

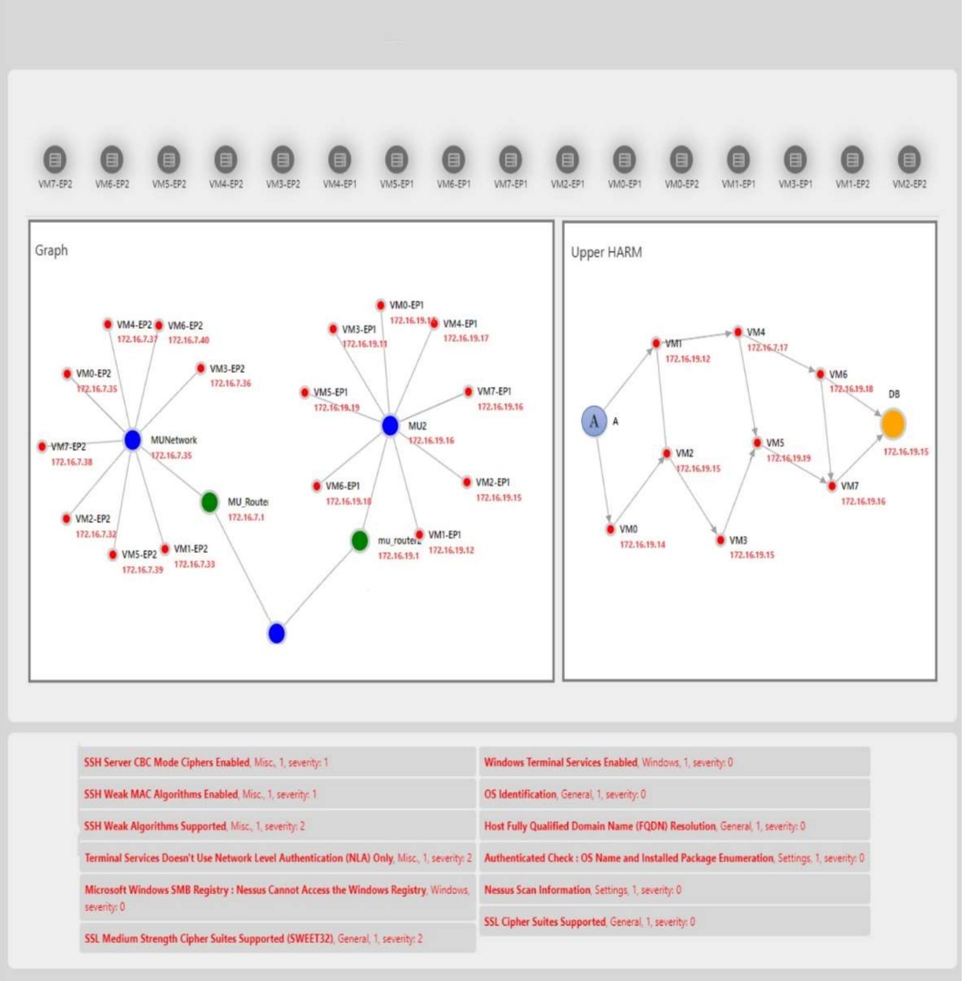
```
{
"user_name" : "Identity based encryption"
"user_mail" : "HMPS78"
"issuer"    : "http://app.aws8734689@aws.amazon.com"
"author"    : "Admin"
"publickey" : "BIHiuhot7dc67866ngckjb"
"cloudkey"  : "vOIFYTRDSTR5655ExgSGGFX"
}
```

```
HYUBGF256 {
        basedecoder[publickey] + "." +
        basedecoder[cloudkey]\
        ###################################
        #################OK################
        ###################################
        }
```

Figure 3. Authentication Mechanism for Key Management System with (a) Invalid Signature (b) Valid Signature

The interpretation of the data received as messages is performed using Watson's IBM

QRadar Advisor. The reason for using this is the capacity to demonstrate the accidents as needed. This tool has the potential to include different IPs-related results. The Figure 3. It reflects the Key Management System Authentication Process (a) Invalid Signature (b) Valid Signature. The Figure 4. demonstrated the implementation of an Amazon Web Services-based authentication mechanism (AWS).



SSH Server CBC Mode Ciphers Enabled, Misc., 1, severity: 1

SSH Weak MAC Algorithms Enabled, Misc., 1, severity: 1

SSH Weak Algorithms Supported, Misc., 1, severity: 2

Terminal Services Doesn't Use Network Level Authentication (NLA) Only, Misc., 1, severity: 2

Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry, Windows, severity: 0

SSL Medium Strength Cipher Suites Supported (SWEET32), General, 1, severity: 2

Windows Terminal Services Enabled, Windows, 1, severity: 0

OS Identification, General, 1, severity: 0

Host Fully Qualified Domain Name (FQDN) Resolution, General, 1, severity: 0

Authenticated Check : OS Name and Installed Package Enumeration, Settings, 1, severity: 0

Nessus Scan Information, Settings, 1, severity: 0

SSL Cipher Suites Supported, General, 1, severity: 0

Figure 4. Authentication Mechanism deployed by signature in AWS

Finally, by attribute-based encryption using keys such as hidden key and public key with Information Proof principles, the cryptographic complexity of our framework was evaluated and measured to safely exchange and navigate Public Health Related data (Pima Indians Diabetes Database) in the cloud to prevent the redundant data. Obtained the cost of server computation expended in revocation to evaluate client revocation output. We use the Attribute Based Encryption to access the Public Health Record information seen safely in Figure 5, reflecting this outcome.

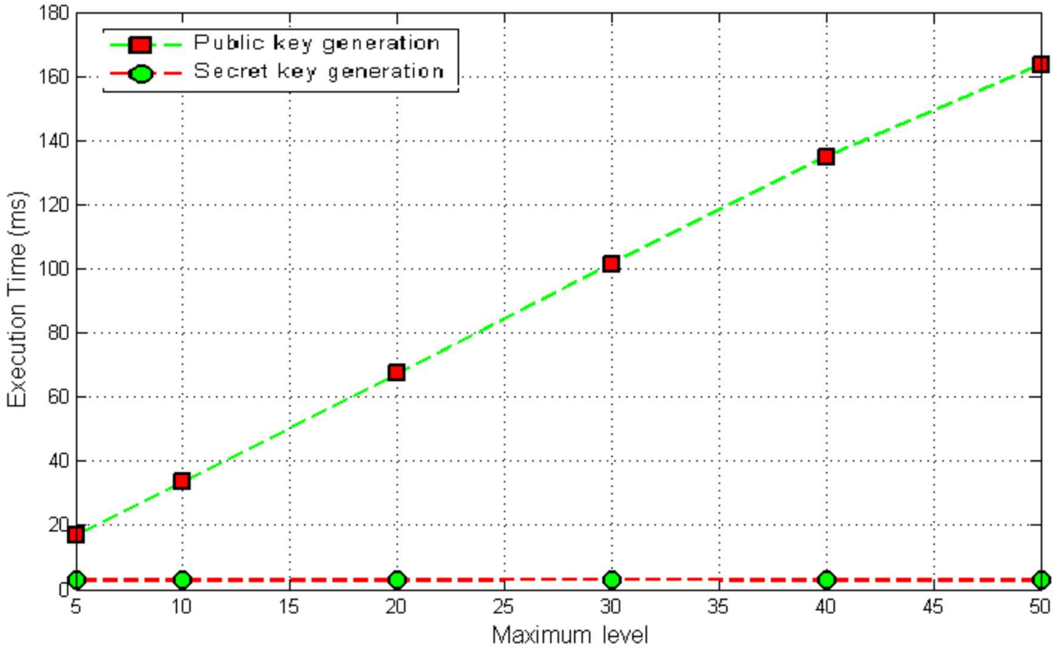


Figure 5. Using Hidden Key and Encryption Key Generation Execution Time required for Attribute Based Encryption in Public Health Record

V. CONCLUSION

This results indicate that the proposed method is promising and is capable to be a vital solution for Public Health Record in cloud to avoid Sharing data. A stable community key management algorithm for enhancing Attribute-based Encryption protection is included in this portion. Furthermore, to ensure that this research work provides an appropriate key protection, encryption & decryption and authentication mechanism for this research work. Finally, from the outcome of the experiment, the authentication mechanism and computation time is analysed. Our algorithm is therefore able to achieve better trade-offs between security and efficiency to avoid the Sharing data.

Reference

1. Shashi Mehrotra Seth & Rajan Mishra 2019, ‘Comparative analysis of encryption algorithms for data communication’, International Journal Computer Science and Technology, vol. 2, no. 2, pp. 292-294.
2. Vishalakshi N S and S.Sridevi, “Survey on Secure De-duplication with Encrypted Data for Cloud Storage,” international journal of advanced science and research, Vol. 4, Issue 1, January 2017.
3. Bellare, Mihir, Sriram Keelveedhi, and Thomas Ristenpart. "Message-locked encryption and secure deduplication." Advances in Cryptology–EUROCRYPT 2013. Springer Berlin Heidelberg, 2013. 296-312.
4. Chen, Rongmao, Yi Mu, Guomin Yang, and Fuchun Guo. "BL-MLE: Block-Level Message-Locked Encryption for Secure Large File Deduplication." (2015). Information Forensics and Security, IEEE Transactions on 26 (2015), no. 12: 2643-2652.

5. Miguel, Rodel, and Khin Mi Mi Aung. "HEDup: Secure Deduplication with Homomorphic Encryption." In Networking, Architecture and Storage (NAS), 2015 IEEE International Conference on, pp. 215-223. IEEE, 2015.
6. Bellare, Mihir, Sriram Keelveedhi, and Thomas Ristenpart. "Dupless: Server-aided encryption for deduplicated storage." Proceedings of the 22nd USENIX conference on security. USENIX Association, 2013.
7. Puzio, Pasquale, Refik Molva, Melek Önen, and Sergio Loureiro."ClouDedup:Secure Deduplication with Encrypted Data for Cloud Storage." Cloud Computing Technology and Science (CloudCom),2013 IEEE 5th International Conference on (Volume:1)p.363 – 370.
8. Li, Jie, Xia Chen, Xumin Huang, Song Tang, Yingmeng Xiang, Mehdi Hassan, and Abdul Hameed Alelaiwi. "Secure Distributed Deduplication Systems with Improved Reliability." Computers, IEEE Transactions on 64, no. 12(2015): 3569 – 3579