# EncryScation: An Secure Approach for Data Security Using Encryption and Obfuscation Techniques for IaaS and DaaS Services in Cloud Environment

**Krunal Suthar and Jayesh Patel**

**Abstract** Now a day's a user of internet wants a freedom to access their valuable data from anywhere any time. Here, Cloud computing comes with its numerous services where user can have get anything like system power, Storage, applications and many more with just less charges. Users of Cloud mainly use it for various purpose and currently storing the data on Cloud is the very important scenario to be consider. With lots of advantage to store data on cloud and free self from burden of maintain record other side, it is very important for user that the data must be secure even it is on rest or in transition. The researcher of Cloud working on their own to deal with this issue but in most of the research proposal consider client side security related issues i.e. Integrity checking, Authentication, Versioning etc. At other side some Research model gives more importance to security data related issue of Cloud service provider i.e. Database encryption, Security based on Metadata, Data Obfuscation etc. But both of above fundamental not make strong impact for Cloud users and Service providers. To have achieve best of them here in this paper we presented a model with two techniques that's Data Obfuscation for server side to secure database details from outsiders and Encryption, authentication at client side. In this paper we have discussed implemented and testing of model towards performance and security. The proposed model ensures both users and service providers to bind trust on each other.

**Keywords** Cloud storage · Data protection · Integrity · Confidentiality · Encryption · Obfuscation

K. Suthar (✉)
Computer Engineering Department, Rai University, Ahmedabad, India
e-mail: krunal_bece@yahoo.co.in

J. Patel
Department of MCA, AMPICS, Kherva, India
e-mail: jayeshpatel_mca@yahoo.com

N. Modi et al. (eds.), *Proceedings of International Conference on Communication and Networks*, Advances in Intelligent Systems and Computing 508,
DOI 10.1007/978-981-10-2750-5_34

# 1 Introduction

The cloud computing is a virtual environment provides various services i.e. IaaS, SaaS, PaaS, DaaS to the users now days. In which users can use its virtual machine allocated to him with nominal charges and for some other reasons like to use licensed software, Store valuable information, High availability without binding of Geographical area etc. In contrast to various features provided by Cloud computing viz. elasticity, anytime access, availability, reliability, faster processing, etc.; security of user details available on cloud are still a burning issue and need to solve for wide adaption of Cloud. As a user may to reduce local burden and increase availability any where it put important data like Financial information, credential information, medical information, files etc. on cloud storage, It is very important to provide security to this data while the data is in trantion (sending from client to Cloud machine) and also when data available on cloud storage. So, using techniques like Encryption, Obfuscation we achieve a complete secure model from both the end Client and Cloud service providers.

The primary purpose of encryption is to guard the of information stored on local machine or transmitted via the network. Encryption algorithms play a especially important part in the security as well it's a key elements for data security like Authentication, Integrity and Non-repudiation. Even the data is in transmission coz of data is in unreadable format the intruder can't get anything out of that.

Changing the format or structure of data to hide actual meaning, Data obfuscation technique is used which makes reverse engineering very difficult. The good about obfuscation over encryption is that encrypted data cannot be processed until it is decrypted, but obfuscated data can be processed without de obfuscation.

If we consider encryption of data on client machine based on sensitivity of its data and then storing the information to cloud storage server, gives surety to client about secure transmission of their file on network. For Providers once it available on his premises database which contains information about lots of client in public domain using Obfuscation technique it's ensure that no any users data are misuse or tempered by unauthorized access.

This paper use encryption and obfuscation technique to provide efficient cloud storage confidentiality. Normally, Integrity or confidentiality is ensured by encryption mechanism, but for security issues in cloud encryption alone is not sufficient for information security [1]. Encryption required integrating with obfuscation technique. While Obfuscation alone is also not good for providing complete security of data in cloud storage because the unauthorized users are able to get information through attack like brute force or sometimes by reverse engineering, which break security of Cloud environment.

The paper is arranged as follows: in Sect. 2 we discuss about various security proposals, in Sect. 3 we discuss brief of proposed methodology. Section 4 we provides detailed discussion on results with security analysis followed by Sect. 5 Conclusion. Finally in last Section, we provides list of References.

## 2 Literature Review

Authors at [1] proposed a cryptographic technique for data security Issues in Cloud computing. In model data are Encrypted before stored on storage servers and key of file are available to data owner only; user is only approved by issuing the corresponding decryption keys by owner. Along with encryption they also used obfuscation methods to increase the confidentiality of data. Authors also proposed Algorithms are for encryption and obfuscation technique. Before storing data on Cloud premises it's encrypted or obfuscated at client side. The Proposed technique is safe to store the cloud users' data on cloud premises. Authors also argue that Encryption only or obfuscation only is not sufficient for cloud data storage.

Author at [2] presented a model for DaaS Which work to secure data which available on Cloud Machines. Proposed methodology provides two important features First Features indicate about how store data on DaaS. Second feature says that how get data from DaaS so that data confidentiality preserve. They also proposed sensitive columns mechanism for character encryption before sending it on Cloud premises, it also obfuscate Database columns at client side which contains numeric values using mathematical function before sending to Cloud storage. Main focus of proposed model to work with query over encrypted and obfuscated data. Many of the researcher are only gives idea about only obfuscation or encryption methodology for security purpose [3–7]. Some of the researcher not put focus on important criteria like efficient sharing [8] or they not shown implemented results of their proposed scheme [9, 10]. Some researcher are only provides abstract of security [11–14] or the literature about the various security issues in Cloud [15].

## 3 Proposed Methodology

The proposed model [16] with all the algorithms steps are presented in International conference NUiCONE 2015 organized at Nirma University and will be published in IEEE soon. So here we just provide overview of the model proposed and mainly focuses on results and analysis of proposal.

### *3.1 Overview*

See Fig. 1.

### *3.2 Experimental Setup and Techniques*

Here for experimental result we use ARO Encryption techniques and MONCrypt Obfuscation Technique [17]. The Client has the following Configuration Microsoft

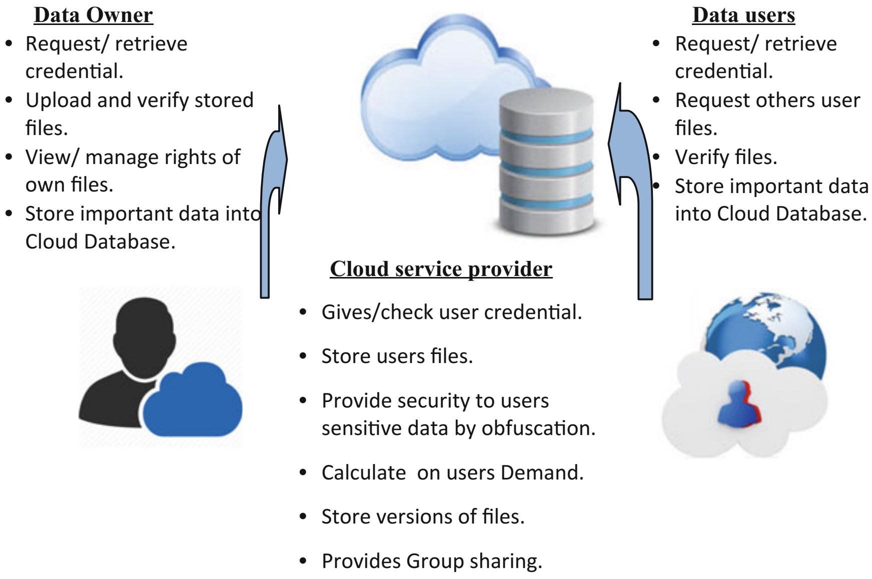
Data Owner
• Request/ retrieve credential.
• Upload and verify stored files.
• View/ manage rights of own files.
• Store important data into Cloud Database.
Data users
• Request/ retrieve credential.
• Request others user files.
• Verify files.
• Store important data into Cloud Database.
Cloud service provider
• Gives/check user credential.
• Store users files.
• Provide security to users sensitive data by obfuscation.
• Calculate on users Demand.
• Store versions of files.
• Provides Group sharing.

**Fig. 1** Basic proposed model

windows 8 operating system 64 bit, 2.5 GHz Intel pentium processor, 4 GB RAM, 500 GB of Storage. The server having VMWare ESXi module run on 3 GHz processor with GB or Ram and 250 GB of HDD. The users upload the data via user interface form VMware Client.

# 4 Result Discussion

## 4.1 Basic Analysis

Figure 2 below shows phase wise cryptographic/obfuscation operations required. All the hash functions are performed offline and they are quite faster.

By using SHA hash function which executes in few milliseconds to compute a hash of even 1 MB file. So, overall, the overhead occurred by the cryptographic operations involved in EncryScation is very low.

In order to understand the proposed algorithms in, we consider a sample data table which stored in the cloud storage as shown in the Table 1. The data are encrypted and obfuscated by the proposed algorithms [16]. It can be noted in Table 2 that data are obfuscated. Obfuscated data in Table 2 consumes less memory in comparison with the Table 1.

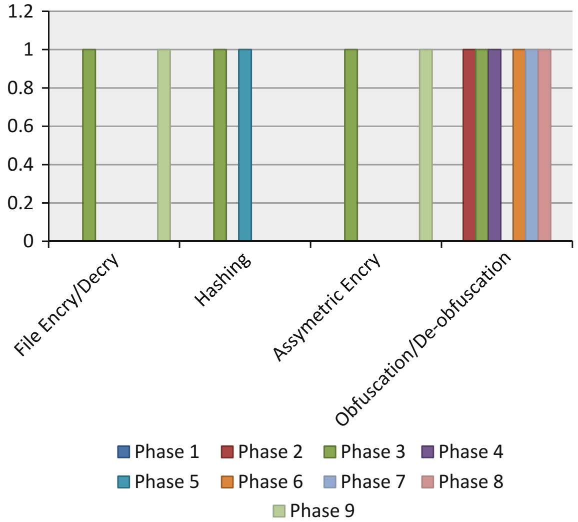

**Fig. 2** Cryptographic operations/obfuscation (Phase wise)

**Table 1** Transactional table with plain text

| Trans_Id | Cust_Id | Item_Name | Quantity | Total_P |
|---|---|---|---|---|
| TId_1003 | A230kum | Printer | 5 | 10,000 |
| TId_923 | B301sus | Harddisk | 13 | 30,000 |
| TId_2304 | C100mon | Monitor | 13 | 22,000 |
| TId_9087 | B002lav | Mouse | 9 | 1250 |
| TId_0012 | G123aro | Keyword | 12 | 2400 |

## 4.2 *Security Analysis*

A. **Storage Correctness**: DO (or DU) can anytime request CSP for data correctness. DO issues a Dynamic random bit request to CSP, and CSP gives in form of hash of those bits having size is almost in KB. After receiving hash value from CSP, DO (or DU) compares it with new calculated hash code. If both found same, it is concluded that the integrity of data is verified.

B. **Lightweight**: Confidentiality and integrity are to be achieved through encryption and hash algorithms. Because of consume heavy computational we advise these two operations to be performed offline on the premise of DO or DU. To check integrity of data, the whole file is not transferred, but only a small sized data is exchanged between CSP and DO/DU, which is independent of the file size.

C. **Dynamism**: Granting/revoking access rights to/from DU or with the group of users is done through executing SQL query and make updation in the required Database entry.

D. **Versioning**: DO/DU is able to store multiple version of their file on CSP and can able to get it as required.

**Table 2** Transactional table with cipher text using encryption and obfuscation

<table>
<tr><th>]zUdbju|p</th><th>L!pvL|xh</th><th>RymhQnwhy</th><th>Zz!dljx}&</th><th>]m\wb}ru{</th></tr>
<tr><td>]k<g3mL:?</td><td>J<y6x<5t></td><td>U,{{kx\|</td><td>2</td><td>@</td></tr>
<tr><td>]k?g5mLBU</td><td>K=3x96|?</td><td>Qm&pdvlum</td><td>)</td><td>0</td></tr>
<tr><td>]k<g6mL;@</td><td>L<z3r94v =</td><td>K{{yw rw{</td><td>)</td><td>!</td></tr>
<tr><td>]kDg3mLBC</td><td>K>#3d93u<</td><td>Uy%{drdry</td><td>Q</td><td>0</td></tr>
<tr><td>]k=g3mL9></td><td>P?{5u;4j=</td><td>Vuzglmhlq</td><td>2</td><td>0</td></tr>
</table>

E. **Data Obfuscation**: The sensitive details like Credential information, Account information etc. are obfuscated and stored on CSP Database which ensure CSP that DO/DU data are safely available on premises and no chance to tempered or misuse.

## Protocol Verification Through Scyther

To verify our operational protocols, we have used Scyther [18], the tool that provides formal proofs for security protocol verification. Scyther has proven to be an effective tool for verification, falsification, and analysis of security protocols. With guaranteed termination it verify protocols with limitless number of sessions. The phases in each operation in our model are verified under various conditions in Scyther and found to be full proof against different attacks viz. man-in-the-middle attack, DoS and replay attack. Due to limitation of space, we only illustrate testing of phase Registration.

We show a claim of an attack for registration phase in Fig. 4 . In the attack, CDO#1 completes his role as CDO up to the claim. Claims are reachable and the protocols are found to be secure. We further check all our phases of Cloud storage security model in Scyther tool and displayed in Table 3 .

**Table 3** Analysis of Scyther Outcomes for Proposed Protocols

| Phases | Properties | | | | |
|---|---|---|---|---|---|
| | Confidentiality | Authenticity | Integrity | Access control | Freshness |
| Registration | Yes (Ni,Tj,Tk) | Yes (ID$_{CDO}$) | Yes (Ni) | Yes (K$_{PU\text{-}CSP}$, K$_{PU\text{-}CDO}$) | Yes (Ni) |
| Pre-storage | NA | NA | NA | NA | NA |
| Storage | Yes (H$_{CDO}$, N$_{i}$, T$_{j,}$ HT) | Yes (ID$_{CDO}$) | Yes (H$_{CDO}$, N$_{i}$) | Yes (K$_{PU\text{-}CSP}$, K$_{PU\text{-}CDO}$) | Yes (Ni) |
| Transmission errors | Yes(IDCDO,Ni, HT) | YES (IDCDO) | NA | NA | YES (Ni) |
| Manage access rights | Yes (FileID, AR, ET, HT, K$_{S\text{-}FILEID}$) | Yes (ID$_{CDO}$, ID$_{CDU}$) | Yes (FileID, AR, K$_{S\text{-}FILEID}$) | Yes (K$_{PU\text{-}CSP}$, K$_{PU\text{-}CDO}$) | NA |
| Dynamic integrity verification | Yes (FileID, Ni, Bt, Tj, C) | Yes (ID$_{USER}$) | Yes (FileID, Ni, H$_{CSP}$, H$_{CDO,}$ C) | Yes (K$_{PU\text{-}CSP}$, K$_{PU\text{-}USER}$) | Yes (Ni) |
| Data obfuscation | NA | NA | NA | NA | YES (Ni) |
| Versioning | Yes(ID$_{CDO}$,Ni, FileID, Tj) | YES (IDUSER) | NA | Yes (K$_{PU\text{-}CSP}$, K$_{PU\text{-}CDO}$) | YES (Ni, Tj) |
| Data download | Yes (FileID, Ni, Ti, Tj) | Yes (ID$_{USER}$) | Yes (FileID, Ni) | Yes (K$_{PU\text{-}CSP}$, K$_{PU\text{-}USER}$) | Yes (Ni) |

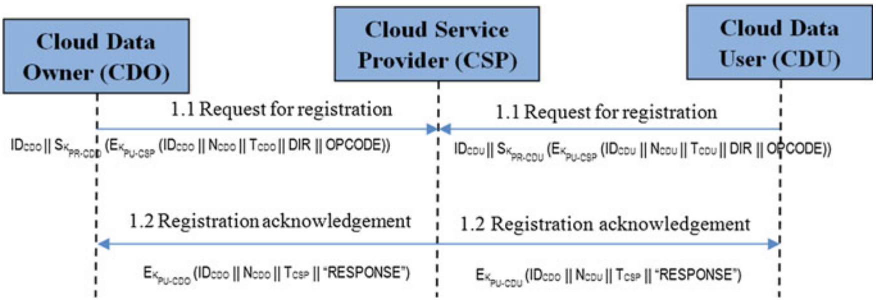
Cloud Data Owner (CDO)
Cloud Service Provider (CSP)
Cloud Data User (CDU)
1.1 Request for registration
$ID_{CDO} || S_{K_{PR-CDO}} (E_{K_{PU-CSP}} (ID_{CDO} || N_{CDO} || T_{CDO} || DIR || OPCODE))$
1.1 Request for registration
$ID_{CDU} || S_{K_{PR-CDU}} (E_{K_{PU-CSP}} (ID_{CDU} || N_{CDU} || T_{CDU} || DIR || OPCODE))$
1.2 Registration acknowledgement
$E_{K_{PU-CDO}} (ID_{CDO} || N_{CDO} || T_{CSP} ||$ "RESPONSE")
1.2 Registration acknowledgement
$E_{K_{PU-CDU}} (ID_{CDO} || N_{CDU} || T_{CSP} ||$ "RESPONSE")

**Fig. 3** Role CSP—Registration phase (Scyther outcome)

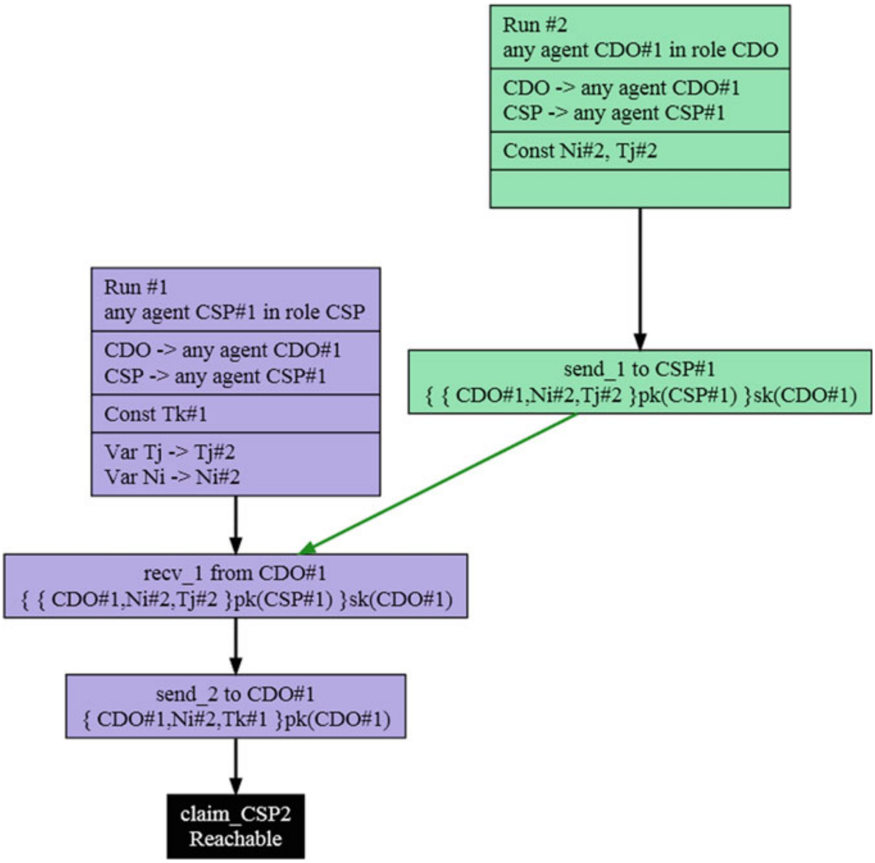

**Fig. 4** Sequence diagram: Registration phase

# 5 Conclusion

Cloud computing provides good services to but due to lack of security many of the users are beware to adopt it. To address the problem of providing data security services to both Cloud user as well service provider, we proposed a new scheme by putting encryption and obfuscation technique works together. Data will be encrypted before sending on Cloud server based on sensitivity of data and user kept key secret gives security to data in transition coz data available in encrypted format on cloud machine makes user ensure about confidentiality.

We used obfuscation technique for security purpose at Cloud server side by which there is very less chance of tempering the data at server. We proposed an algorithm which supports all this operations and providing results with security and basic analysis. From the Model analysis using scyther security tool, it is observed that proposed scheme provides better protection to stored information on a cloud and even the data is in transition than the another available approaches which are based on encryption, obfuscation technique alone from Cloud users as well Service providers view.

# References

1. Arockiam, L.; Monikandan, S., "Efficient cloud storage confidentiality to ensure data security," Computer Communication and Informatics (ICCCI), 2014 International Conference vol., no., pp. 1, 5, 3–5 Jan. (2014).
2. Atiq, R.; Hussain, M..: Efficient Cloud Data Confidentiality for DaaS. International Journal of Advanced Science and Technology Vol. 35, October (2011).
3. Halder, R.; Cortesi, A., "Obfuscation-based analysis of SQL injection attacks," Computers and Communications (ISCC), IEEE Symposium on, vol., pp. 931,938, 22–25 June (2010).
4. Hataba, M.; El-Mahdy, A.; "Cloud Protection by Obfuscation: Techniques and Metrics," P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), 2012 Seventh International Conference on, vol., no., pp. 369,372, 12–14 Nov. (2012).
5. Patel H. B.,; Patel D. R.; Borasaniya B.; Patel A.; Data Storage Security Model for Cloud Computing, Advances in Communication, Network, and Computing Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering Volume 108, 2012, pp 37–45. (2012).
6. Hyun-Suk, Yu.; Yvette, E.; Kyung K,; Securing Data Storage in Cloud Computing, Security Engineering Research Institute (Journal of Security Engineering), No. 9, No. 3, June, pp 251–260(2012).
7. Kamara S,; Lauter K,; Cryptographic Cloud Storage, IFCA/ LNCS 6054, Springer-verlag, Berlin Heidelberg, pp 136–149. (2010).
8. el-Khameesy, N.; Hossam R., A Proposed Model for Enhancing Data Storage Security in Cloud Computing Systems, Journal of Emerging Trends in Computing and Information Sciences, VOL. 3, NO. 6, June, pp 970–974(2012).
9. Wang, C.; Wang, Q.; Ren, K.; Lou, W.; Ensuring data storage security in Cloud Computing, Quality of Service, 2009. IWQoS. 17th International Workshop on, vol., no., pp. 1, 9, 13–15 July. (2009).

10. Yvette E. Gelogo, Sunguk L.,; Database Management System as a Cloud Service, International Journal of Future Generation Communication and Networking Vol. 5, No. 2, pp 71–76 June (2012).
11. Ikechukwu, U.; Omenka. U;, Building Trust and Confidentiality in Cloud computing Distributed Data Storage, West African Journal of Industrial & Academic Research, Vol. 6 No. 1 March, pp 78–83. (2013).
12. Xiaojun Yu, Qiaoyan W.; A View about Cloud Data Security from Data Life Cycle, International Conference on Computational Intelligence and Software Engineering (CiSE), pp 1–4, IEEE, Dec. (2010).
13. Mathew, A.; Survey Paper on Security & Privacy Issues in Cloud Storage Systems, EECE, Term Survey Paper, April, pp 1–13(2012).
14. Mahajan, P.; Setty, S.; Lee, S.; Depot: Cloud storage with minimal trust, 9th USENIX Symposium on Operating System Design and Implementation, pp 1–26. (2010).
15. Suthar, K., Patel, J..: Security of Cloud IAAS, DAAS Services using Encryption, Obfuscation Techniques: A Review. Technix International Journal for Engineering Research Volume 1 Issue 6, Jan (2015).
16. Suthar K., Patel J "EncryScation: A Novel Framework for Cloud IaaS, DaaS security using Encryption and Obfuscation Techniques" In 5th Nirma University International conference on Engineering(NUiCONE) Dec 2015.
17. L. ArockiamÅ and S. Monikandan " Security Framework to Ensure the Confidentiality of Outsourced Data in Public Cloud Storage" In International Journal of Current Engineering and Technology E-ISSN 2277–4106, P-ISSN 2347–5161.
18. Cremers, C., "The Scyther Tool: Verification, falsification, and analysis of security protocols". In Proc. of the 20th Int. Conf. Computer Aided Verification (CAV'08). Lecture Notes in Computer Science, vol. 5123. Springer Verlag, 414–418, 2008.