# Measured Security Features Implementation In Cloud Environment

**CHANDHINI K**
M.Tech-Student Computer Science and Engineering,
R V College of Engineering, Bangalore, Karnataka, India

*Abstract:* **Cloud computing encompasses a set of IT based Services, delivered by a third party provider who owns the infrastructure and provided to customers over a network. It is now one of the fastest growing technologies of the IT trade for business. Thus the high flexibility and portability of cloud have raised numerous security concerns. Security issue in cloud computing has become the vital reason of impeding its development. This work shows a concern on the security element in cloud environment for small business addressing their shortcomings and finding solutions for it. Measured security features have been implemented by developing a secured data encryption, exchange and decryption infrastructure resulting in a data security model.**

*Key words :* **IT Based Services; Cloud Environment; Measured Security; Data Encryption;**

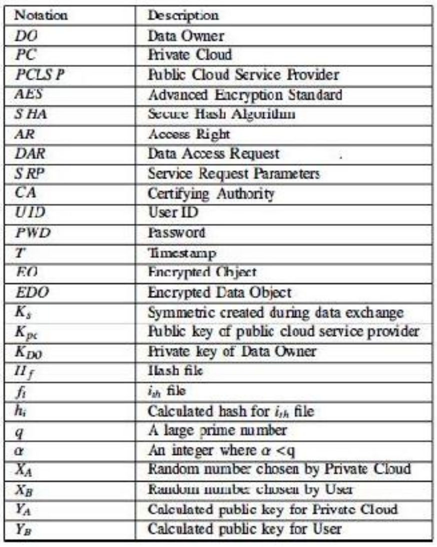
## I. INTRODUCTION

Cloud computing encompasses a set of IT based Services, delivered by a third party provider who owns the infrastructure and provided to customers over a network. It is now one of the fastest growing technologies of the IT trade for business. Thus the high flexibility and portability of cloud have raised numerous security concerns. Security issue in cloud computing has become the vital reason of impeding its development. Concern on the security element in cloud environment for small business addressing their shortcomings and finding solutions for it are dealt here. Measured security features have been implemented by developing a secured data encryption, exchange and decryption infrastructure resulting in a data security model**.** A distributed architecture, that centralizes server resources on a scalable platform in order to provide on demand computing resources and services, is termed as cloud computing [1]. Thus it can be presented as a model for convenient and easier network access to a shared pool of configurable services that is rapidly provisioned through as needed facilities and released with minimal management efforts. Cloud computing enables cloud services. Companies get to consume several services and computing as utility rather than building and maintaining their own computing infrastructures through cloud.

## II. PROPOSED MODEL

The following notations are used in the proposed model

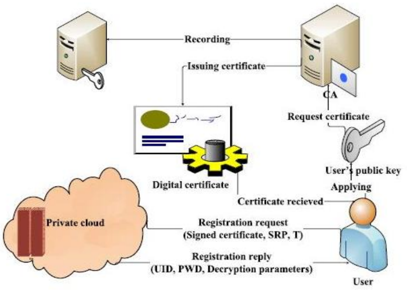
TABLE I
NOTATION USED IN PROPOSED MODEL AND WORKSCHEME



| Notation | Description |
|---|---|
| *DO* | Data Owner |
| *PC* | Private Cloud |
| *PCLS P* | Public Cloud Service Provider |
| *AES* | Advanced Encryption Standard |
| *S HA* | Secure Hash Algorithm |
| *AR* | Access Right |
| *DAR* | Data Access Request |
| *S RP* | Service Request Parameters |
| *CA* | Certifying Authority |
| *UID* | User ID |
| *PWD* | Password |
| *T* | Timestamp |
| *EO* | Encrypted Object |
| *EDO* | Encrypted Data Object |
| $K_s$ | Symmetric created during data exchange |
| $K_{pc}$ | Public key of public cloud service provider |
| $K_{DO}$ | Private key of Data Owner |
| $H_f$ | Hash file |
| $f_i$ | $i_{th}$ file |
| $h_i$ | Calculated hash for $i_{th}$ file |
| $q$ | A large prime number |
| $\alpha$ | An integer where $\alpha$ <q |
| $X_A$ | Random number chosen by Private Cloud |
| $X_B$ | Random number chosen by User |
| $Y_A$ | Calculated public key for Private Cloud |
| $Y_B$ | Calculated public key for User |

## III. GENERAL SCENARIO OF PROPOSED SCHEME

Hybrid cloud usage facilitates maintaining in-house storage for sensitive operations, and also allows cost efficiency which is a prime factor for small business. Work flow in the proposed system thus encompasses as DO places data on the cloud applying AES - 128 bit key techniques as the PCLSP is un-trusted. User need to register first to access data and registration scheme is handled by the PC. After successful registration user sends data access request to PC, and after required verification PC forwards the request to the PCLSP which in turn checks to verify the request and finally sends the requested data to the user in an encrypted form. In proposed system only authentic users get the access to the data in public cloud. One of the prime targets of the proposal is to remove workload from DO. DO does not need to stay online to handle several cloud based tasks (as user registration, data request etc.) in proposed system. AR has also been incorporated in the system. And secure data exchange has been implemented with modified symmetric station to station key agreement incorporating digital signature for authentication.

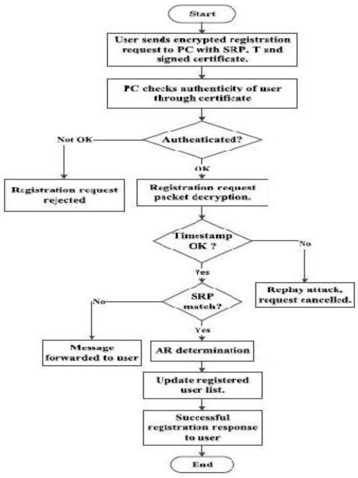


***User registration view***

## IV. PROPOSED WORK SCHEME

### *USER REGISTRATION*

User registration is a very important aspect of the system because proper measures need to be taken to identify harmless users. At first user must collect a certificate which confirms user's claim to be legal and also proves his identity. There are well known and trustworthy certifying authorities where from the user can receive that digitally signed certificate, which also contains the user's public key. After collecting the certificate the user sends registration request. Fig. 4.2 shows this aspect. With registration request user sends the signed certificate, DO here predetermines the services that they can allow toward its users and users need to select from those which constitute the SRP also a T. This T is used so that any third party can't do a replay attack with it later. Then the registration request, SRP and also the T is encrypted using user's private key for user's authentication towards the PC. PC first checks to see the authenticity of the user through the certificate. And then checks validity of the requestthrough T. Finally checks the S RP. If the preferences match with that of the categories predetermined by the DO, AR is determined for that user otherwise a message is forwarded to the user to choose from the allowed services. After this the PC updates the registered user list with corresponding UID, PWD and AR. Then finally registration process is completed and the UID, PWD, data decryption parameters (data decryption key, hash function) and T encrypted with DO's private key which is again encrypted with user's public key. Along with it the digital certificate of the organization is also sent containing its public key which proves its authenticity. This entire work process of user registration is given through a flowchart.


Start
User sends encrypted registration request to PC with SRP, T and signed certificate.
PC checks authenticity of user through certificate
Authenticated?
Not OK
OK
Registration request rejected
Registration request packet decryption.
Timestamp OK ?
No
Yes
Replay attack, request cancelled.
SRP match?
No
Yes
Message forwarded to user
AR determination
Update registered user list.
Successful registration response to user
End

### *SECURE DATA EXCHANGE PROCESS*

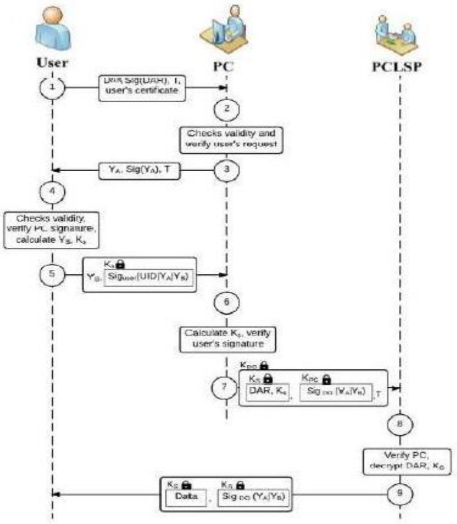
In the system user initiates the data exchange process. At first user needs to create his own digital signature for the DAR to ensure that even if the user account is sacrificed the malicious user can not conduct forgery with a different request. Then T is encrypted with user's private key to prevent replay attack. Finally digitally signed data access request together with encrypted T is sent to the PC. After receiving the request, PC checks the validity of the request through T. Then verify the Data request using the proper hash function and user's public key. Here station to station key agreement is initiated by the PC. Now PC selects a random number XA and calculates YA using equation (1). PC also signs this value to ensure its integrity even if it is stolen. T is also used here encrypted with DO's private key. Now user first checks the T and then verify users signature. Similarly now user selects another random number XB and calculates YB using equation (2) and also calculates Ks using using equation (3): Then user concatenates the corresponding user ID, YA , and YB. The result is signed with his private key. The signature is encrypted with Ks. Here T is also encrypted with user's private key. User then sends YB, the signature together with the T and his own public-key certificate to PC. Then calculates Ks using equation (4) .Then PC verifies user signature using the created Ks. This approach prevents man in the middle attack. PC then concatenates YA and YB and signs the result with its private key. The signature is also encrypted with the Ks. The Ksencrypted signature is again encrypted using user public key.

$$Y_A = \alpha^{X_A} \mod q \qquad (1)$$

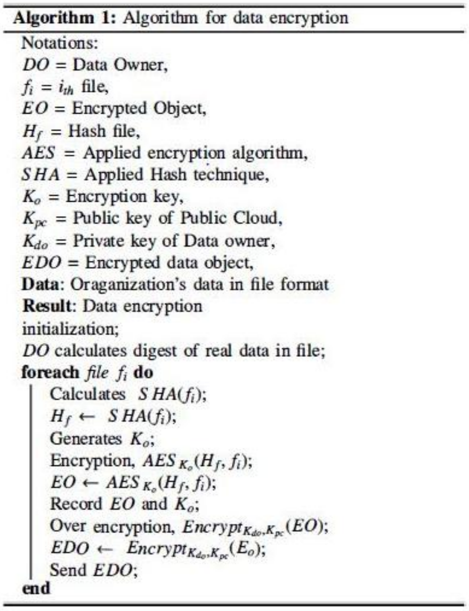
$$Y_B = \alpha^{X_B} \mod q \qquad (2)$$

$$K_s = {Y_A}^{X_B} \mod q \qquad (3)$$

$$K_s = {Y_B}^{X_A} \mod q \qquad (4)$$


User
PC
PCLSP
1
DAR, Sig(DAR), T, user's certificate
2
Checks validity and verify user's request
3
$Y_A$, Sig($Y_A$), T
4
Checks validity, verify PC signature, calculate $Y_B$, $K_s$
5
$K_s$
$Y_B$, $Sig_{user}(UID|Y_A|Y_B)$
6
Calculate $K_s$, verify user's signature
7
$K_{DO}$
$K_S$
DAR, $K_s$
$K_{PC}$
$Sig_{DO}(Y_A|Y_B)$
T
8
Verify PC, decrypt DAR, $K_S$
9
$K_S$
Data
$K_S$
$Sig_{DO}(Y_A|Y_B)$

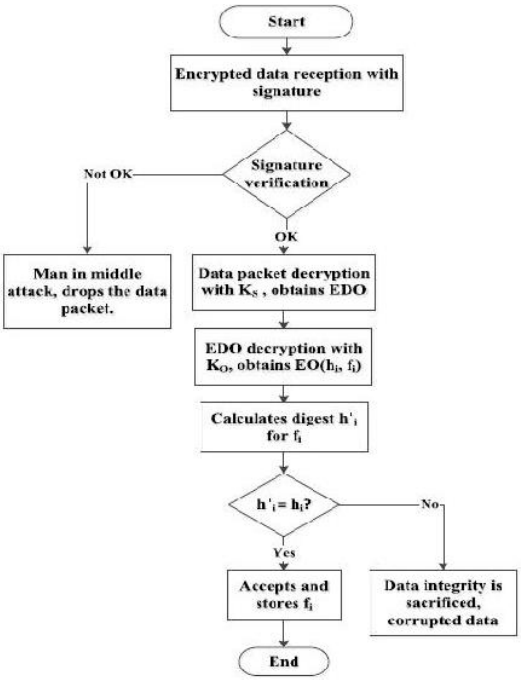
Now it's time to forward the data request to PCLS P. At this point several encryptions are done. Starting with, at first DAR, symmetric key are encrypted using Kpccomprising the DAR information packet. Then encrypted information packet together with encrypted concatenated signature is again encrypted using KDO. And T is also added at this stage to stop replay attack. With all these encrypted information and signed certificate of DO, are sent to the PC. PC first checks the validity of message through T. Then it decrypts the entire information packet using the public key of data owner found from that certificate proving DO's authenticity. Similarly decrypts the DAR information packet using PCLS P's private key. Extracts the Ks from there and encrypts the requested data using that key. Finally the encrypted data together with encrypted concatenated signature, sent from PC to the user. User at first verifies signature and then decrypts the data using the Ks.



```
Algorithm 1: Algorithm for data encryption
Notations:
$DO$ = Data Owner,
$f_i$ = $i_{th}$ file,
$EO$ = Encrypted Object,
$H_f$ = Hash file,
$AES$ = Applied encryption algorithm,
$SHA$ = Applied Hash technique,
$K_o$ = Encryption key,
$K_{pc}$ = Public key of Public Cloud,
$K_{do}$ = Private key of Data owner,
$EDO$ = Encrypted data object,
Data: Oraganization's data in file format
Result: Data encryption
initialization;
$DO$ calculates digest of real data in file;
foreach file $f_i$ do
    Calculates $SHA(f_i)$;
    $H_f \leftarrow SHA(f_i)$;
    Generates $K_o$;
    Encryption, $AES_{K_o}(H_f, f_i)$;
    $EO \leftarrow AES_{K_o}(H_f, f_i)$;
    Record $EO$ and $K_o$;
    Over encryption, $Encrypt_{K_{do},K_{pc}}(EO)$;
    $EDO \leftarrow Encrypt_{K_{do},K_{pc}}(E_o)$;
    Send $EDO$;
end
```

### DATA ENCRYPTION BY DO

This data encryption phase is accomplished by the DO himself. In proposed system, AES-128 bit key encryption has been used [13]. Before encryption digest of the data is calculated using SHA-l. Because this digest is encapsulated with the data file to ensure integrity. After the digest calculation, data with the digest is encrypted using the generated Ko for AES . This resultant EO then over encrypted using PC's public key and DO's private key to authenticate DO to public cloud and sent. On reception, PCLSP uses its own private key and the public key of DO to decrypt the message and store the encrypted data files. One of our prime objectives is achieved here, where the data files only should be visible to the user and DO, not to the PCLSP as it is available over un-trusted domain. Algorithm of data encryption by DO is given in algorithm 1.


Start
Encrypted data reception with signature
Signature verification
Not OK
OK
Man in middle attack, drops the data packet.
Data packet decryption with $K_S$ , obtains EDO
EDO decryption with $K_O$, obtains EO($h_i$, $f_i$)
Calculates digest $h'_i$ for $f_i$
$h'_i = h_i$?
No
Yes
Accepts and stores $f_i$
Data integrity is sacrificed, corrupted data
End

*`Flowchart of data decryption by user*

### DATA DECRYPTION BY USER

Data decryption phase is accomplished by the user only. After the user receives encrypted data and PC signature, first verifies it using the Ks. After verification data is decrypted and EDO is obtained, which is again decrypted using Ko for AES based decryption key. From there a signature of PC and data file is found. Then digest of that data file is calculated and matched with the received one. Finally data is stored by the user.

## V. EXPERIMENTAL ANALYSIS AND INFERENCE

As the analysis conducted here is based only on the strength of cryptographic primitives. It encompasses description of phases that describes the outcome of following the proposed system based on the security standards used in the system. A better security infrastructure is a must to the affiliate this task. However, let's start with privacy concerns of both the user and DO. In the proposed system DO places its data on PCLSP. Here data is placed in an encrypted manner using strongly secured AES encryption system. And the encryption key of those data is only known to the DO and user. This aspect results in data confidentiality. Then in proposed system, T has been used repeatedly. This might seem unnecessary and repetitive to some. But for their concern, it needs to be made clear that this is a strong proven method to stop replay attack. In the proposed system digital signature has been used as well. As it is known that the purpose of a digital signature is to guarantee that the entity sending the message really is who it claims to be. It is linked to the data in such a manner that if the data is changed, the digital signature is invalidated. Using it during data encryption by DO, signatures created by the entities while in data exchange, served to retain data integrity and to prevent non-repudiation attack. Now in the proposed system another security aspect that has been used repeatedly is digital certificate. Authenticity is such a criteria, which needs to be proved every time even if the communicating entity is verified. There has been used the hybrid approach of using a combination of symmetric and asymmetric key encryption while in data encryption and also during data exchange. Hence a secured approach for data encryption and fast operation for key transfer is utilized here. Then modified version of station to station key agreement has been used in the proposed system to create the session key during data exchange. It prevents man in the middle attack effectively and also eradicated the chances of data spoofing and snooping. Access control is also provided in proposed system. Because while registration, based on SRP users are granted their allowed AR. Thus it ensures access to protected information must be restricted to people who are authorized to access the information. Security measures taken in the system have been applied one after another resulting in encryption and over encryption, really made data theft a futile act enhancing data security to the strongest.

## VI. CONCLUSION AND FUTURE WORK

The ultimate concern of proposed model has been, to establish security infrastructure for those having small business and want to utilize the beneficiary phases of cloud. It encompasses a hybrid cloud deployment which eradicates the security limitations of a public cloud, while still being able to support many of the economic advantages of public cloud computing. Proposed system provides some operational security features through algorithm and flowcharts to offer an effective flexible cloud security solution. Providing security for users has been ultimate aim of the proposed system. Using a private cloud where all key management and registration process takes place, releases workload from DO and also personal information of users are not exposed to public cloud. The model empowers to provide security of user's data with secure data exchange and also facilitating a low computation cost on client. Thus symmetric key sharing is managed here with public key cryptography, to achieve faster performance with low computational overhead. Authentication, confidentiality, integrity, access control on original data and non-repudiation on Cloud etc. are the basic security measures of the proposal. Enhancing this security solution by introducing more trusted features and providing aspects of the effectiveness through time based simulations of this cloud security infrastructure would accumulate our future work.

## VII. ACKNOWLEDGEMENTS

The author thanks Dr.S.Sridhar, Professor and Director, Cognitive & Central Computing, R.V.College of Engineering, Bangalore, India for communicating this article to this Journal for publication after modifications to present my work in the form of a paper. The author would like to thank Dr.G.Shobha, HoD of CSE Department for the constant encouragement.

## VIII. REFERENCES

[1] R. Velumadhava Rao, K. Selvamani, “Data Security Challenges and Its Solutions in Cloud Computing" International Conference on Computer, Communication and Convergence (ICCC 2015), International Conference, Procedia Computer Science 48( 2015 ) 204 – 209.

[2] PreetiSirohi and Amit Agarwal, "Cloud Computing Data Storage Security framework relating to Data Integrity, Privacy and Trust" 2015 1st International Conference on Next Generation Computing Technologies (NGCT-2015) Dehradun, India, 4-5 September 2015

[3] M. Sugumaran, BalaMurugan. B, D. Kamalraj, " An Architecture for Data Security in Cloud Computing" 2014 World Congress on Computing and Communication Technologies 2014 IEEE DOI 10.1109/WCCCT.2015.53.

[4] Aws NaserJaber, MazlinaBinti Abdul Majid , " A Study in Data Security in Cloud Computing," 2014 IEEE 2014 International Conference on Computer, Communication, and Control Technology (I4CT 2014),

September 2 - 4, 2014 - Langkawi, Kedah, Malaysia

[5] Chaoqun Yu1,Lin Yang2,Yuan Liu1,Xiangyang Luo1,2, "RESEARCH ON DATA SECURITY ISSUES OF CLOUD COMPUTING", International Journal of Computer Applications Volume 113 - No. 1, March 2014.

[6] Hu Shuijing, "Data Security : the challenges of cloud computing" 2014 Sixth International Conference on Measuring Technology and Mechatronics Automation 2014.

[7] K Hashizume et al., "An analysis of security issues for cloud computing", Journal of Internet Services and Applications, a Springer open journal, pp 1-13, 2013.

[8] Kamara, S., Lauter, K., "Cryptographic cloud storage", Proceedings of the 14th international conference on Financial cryptography and data security, FC' 10, pp. 136- 149, Springer-Verlag, Berlin, Heidelberg (2012)

[9] EmanM.Mohamed, Hatem S. Abdelkader, " Enhanced Data Security Model for Cloud Computing." The 8th International Conference on INFOrmatics and Systems (INFOS2012) - 14-16 May Cloud and Mobile Computing Track 2015.

[10] Vinay kumar pant, Jyoti Prakash., " Three Step Data Security Model for Cloud Computing based on RSA and Steganography Techniques"978-1-4673-7910-6/15/$31.00 ©2014 IEEE.

[11] SiddharthDuttChoubey, Mohit Kumar Namdeo, "Study of Data Security and Privacy Preserving Solutions in Cloud Computing."978-1-4673-7910-6/15/$31.00©2014 IEEE

[12] AbdulazizAljabre,"Cloud Computing for Increased Business Value", International Journal of Business and Social Science, Vol. 3, No. 1, January 2013.

[13] M. Sudha, Dr.Bandaru Rama Krishna Rao, M. Monica, "A Comprehensive Approach to Ensure Secure Data Communication in Cloud Environment", International Journal of Computer Applications (09758887) Volume 12 No.8, December 2013.

[14] J. Heiser, and M. Nicolett, "Accessing the Security Risks of Cloud Computing", G00157782, Gartner,Inc., Stamford, CT, 2010.

[15] MohitMarwaha, Rajeev Bedi, "Applying Encryption Algorithm for Data Security and Privacy in Cloud Computing", IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 1, No 1, pp 367-370, 2008.