ijournals International Journal of Software & Hardware Research in Engineering
ISSN No: 2347-4890 Volume 2 Issue 4, April 2014

Procuring Data Storage Security In Cloud Environment By Using Two Step Secure Protocol

Gokulan.V1, Dr. Kalaikumaran.T2, Dr. Karthik .S 3

PG Scholar, Department of CSE, SNS College of Technology, Coimbatore-351.
Professor and Head, Department of CSE, SNS College of Technology, Coimbatore-352.
Professor and Dean, Department of CSE,SNS College of Technology,Coimbatore-353.

ABSTRACT

Cloud computing has quickly become one of the most prominent buzzwords in the IT world due to its revolutionary model of computing as a utility. It promises increased flexibility, scalability, reliability and security while promising decreased operational and support costs. However, many potential cloud users are reluctant to move to cloud computing on a large scale due to the unaddressed security issues present in cloud computing. Two major challenges to the cloud service providers are providing better data security and keeping the user data highly confidential from the intruders. Designed two-step protocol is based on ECDSA algorithm and sobol sequence method. Using ECDSA method, data loss can be minimized with less computation time for generating the public key and user becomes confident about the data security. Protocol is highly applicable for users who have less resources and limited computing capability. For the cloud service providers, protocol allows third party auditor or verifier to periodically verify the data integrity without receiving the original data again and again from the database. Also, protocol concerns the data security, confidentiality and integrity in terms of not revealing the data contents to the attackers and it consumes less time to detect the data loss verify the integrity of data by using sobol sequence method

Index Terms- Cloud storage security, ECDSA, fibonacci sequening, third party auditor.

1 INTRODUCTION

Cloud computing is a technical jargon which allows thin client (PC, any mobile device) to access the resources provided by the server over a link made by a network (Internet). Moreover, cloud computing is not an innovation terminology, but a means to, constructing IT services that use advanced computational power and improved storage capabilities. A big question arises, how secure the data is in cloud? So the proposed scheme gives utmost safety of data from the intruders with the use of cryptographic method. In security issue we have emphasized on the significance of ensuring remote data integrity. Security is always a major concern and in cloud computing this security level is fulfilled by exploring it in various security challenges. Thus the verification process becomes more challenging. The data stored in cloud is open to the attackers or brokers no matter how much the data is secured and protected. So for highly secured data we have projected the isolation of the encryption and decryption processes from the cloud to a broker service that is trusted by both the cloud provider and the cloud consumer. To attain maximum security we have divided and encrypted the data with the help of extremely secured processors so that the data is protected from unfair means. Since the owner of data loses his control over his own data when he stores his data in cloud so it's a common thing that the query of security arises regarding the data. Here, a secure protocol using random sampling sobol sequence and ECDSA algorithm for the integrity and the security of the data available in the cloud which are far better than those of RSA and other public key cryptographic methods. The Elliptic Curve Cryptography Digital Signature method provides nearly equal security with small keys comparable to RSA and other public key cryptographic methods. In addition of these are capable of detecting the data modification if occurred in the absence of the authenticated dealer. And, proposed a scheme of change or modify or insert or delete or reorder the data, stored in the cloud. In this design of protocol, the encryption of the data is done to ensure the confidentiality and then, the computation of metadata is done over the encrypted data. This is accomplished only when the consumer demands it.

2 EXISTING SYSTEM

Presently, to provide confidentiality in cloud environment, Elliptical Curve Cryptography method uses 80 bits key. Use of pseudorandom sequencing was overcome by sobol sequencing in the protocol. But, sobol needs gray code for its code generation. Also, it can be implemented in procedure oriented programming languages like FORTRAN, C. In the aspect of key size, ECC method was effective than RSA method. But, ECC was not effective in providing confidentiality.

IJSHRE

© 2014, IJOURNALS All Rights Reserved

Data security is an important aspect of quality of service, as a result, security must be imposed on data by using encryption strategies to achieve secured data storage and access. Because of opaqueness nature of cloud, it is still having security issues. The cloud infrastructure even more reliable and powerful then personal computing, but wide range of internal, external threats for data stored on the cloud. Since the data are not stored in client area, implementing security measures cannot be applied directly. In this work, we implement RSA algorithm before storing the sensitive data in cloud. When the authorized user request the data for usage then data decrypted and provided to the user.

John C. Mace et.al [8] have proposed an automated dynamic and policy-driven approach to choose where to run workflow instances and store data while providing audit data to verify policy compliance and avoid prosecution. They also suggest an automated tool to quantify information security policy implications to help policy-makers form more justifiable and financially beneficial security policy decisions. Service oriented architecture (SOA) is used for work flow deployment in an enterprise. For efficiency, productivity and to achieve public cloud, the cloud computing uses the approaches like retaining control, setting policy, monitoring and runtime security. The dynamic deployment approaches in public cloud computing are security assessment, work flow deployment, policy assignment, audit data and policy analysis.

Qiang Guo et.al [9] gives the unique definition for trust in cloud computing and various issues related to trust are discussed here. An extensible trust evaluation model named ETEC has been proposed which includes a time-variant comprehensive evaluation method for expressing direct trust and a space variant evaluation property for calculating recommendation trust. An algorithm based on ETEC model is also shown here. This model also calculates the trust degree very effectively and reasonably in cloud computing environments.

3 PROPOSED SYSTEM

Security, reliability, confidentiality, liability, privacy etc are the main concerns on the topic of cloud computing technique and the peak concern is security. It depends on the CSP that how they guarantee the client regarding these tribulations. The worry about security includes problem related to passive attacks, data location, privacy, data integrity, freedom, problem related to man in the middle attack and long-term viability. These asserted problems are endless, in the proposed system, made an attempt to resolve some of these problems with the help of ECDSA method where the data is safe and secure from external threats. To overcome intruder's attack and to inflate confidentiality, ECDSA method is used with 320 bits of key value. To perform data verification, existing system uses sobol sequencing. But, it can be coded only in C language. As a solution, Fibonacci sequencing has been framed to minimize the data loss in the cloud environment. ECDSA is a variant of the DSA which uses elliptic curve cryptography. As with elliptic curve cryptography in general, the bit size of the public key believed to be needed for ECDSA is about twice the size of the security level, in bits. By comparison, at a security level of 80 bits, meaning an attacker requires the equivalent of about 2^{80} operations to find the private key, the size of a DSA public key is at least 1024 bits, whereas the size of an ECDSA public key would be 160 bits. On the other hand, the signature size is the same for both DSA and ECDSA, 4 t bits, where 't' is the security level measured in bits, that is, about 320 bits for a security level of 80 bits.

Protocol concerns the data security, confidentiality and integrity in terms of not revealing the data contents to the attackers and it consumes less time to detect the data loss verify the integrity of data by using sobol sequencing method.

4 IMPLEMENTATION

4.1 Cloud storage model

With the help of following figure we can easily understand the cloud storage model and working of each type. In cloud computing the user is the one who stores his private data in cloud to prevent it from hazards and this is done with the help of CSP. Say, if the user require that information again then in order to access that particular data the user have to send an appeal to the CSP then the CSP will verify that whether the user is authenticated or not.

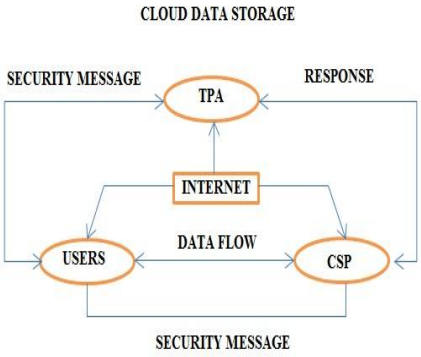

Fig 1: Cloud data storage model

Cloud user: Cloud User is the person who uses the services of cloud.

Cloud Service Provider (CSP): The data to be stored or taken back is done through CSP. CSP manage the cloud server and provide a paid service to the user.

Third Party Auditor (TPA): TPA is also called a Verifier; if the user is suffering from lack of timing then the data verification is done by TPA or verifier. TPA provides user request mode and auditing mode. User request mode gives the accessing permission from the cloud server. Auditing mode establishes the path to security auditing page. This is

© 2014, IJOURNALS All Rights Reserved

used to register the login to the web server. It contains name, password, address, and host name (online), security code. After registered authentication it will lead to the web server access into the cloud network. This will auto generate after login to the web server. The users to gives permission to upload, download, reports the data from the user end. It will get through to the data upload/data download/reports directly.

To upload the data into the web server, upload the data/files user have to encrypt the data and upload data command button. User can able to upload the data by both private and public segments. In this process user gives the data path, and then encrypted the data by private and then uploaded the data into the web server. In this download the user have to specify the file name which was already uploaded into the database list and then user have to decrypt the data by using the authentication which was provided, and then only user have to download the data. The auditing security gives data dynamics, data integrity, audit report results. In this case user selected the audit report option, and then it's waiting for audit request from server end to gather the information which was accessed.

If authenticated, it will allow the user to access the data else not. The data accessed by the user if in encrypted form that it can be decrypted using his secrete key. And the last the TPA will keep a periodic check on the data and verify it periodically only when the user himself allows to verify the TPA. Since, in cloud computing the user loses his control over the data as soon as the data is transferred, data is more prone to the errors or damage from anonymous users and attacks. The data may be lost or modified by unfair means. Thus to prevent it from these many problems an efficient and secure method is needed.

4.2 Threats to violate security

Cloud computing offers many benefits, but is vulnerable to threats. As cloud computing uses increase, it is likely that more criminals find new ways to exploit system vulnerabilities. Many challenges and risks in cloud computing which increase the threat of data compromise. To mitigate the threat, cloud computing stakeholders should invest heavily in risk assessment to ensure that the system encrypts to protect data, establishes trusted foundation to secure the platform and infrastructure, and builds higher assurance into auditing to strengthen compliance. Security concerns must be addressed to maintain trust in cloud computing technology.

Internal Threats: Caused internally in the cloud where the Cloud Service Provider can leak the information of the user or may modify it for its own purpose.

External Threats: These kinds of threats are induced by intruders to the cloud data storage. To resolve this affair, the data is dispersed into many fractions of data say 64KB's fractional part (fragmentation) regardless of the repository of the original data and this is accomplished through ECDSA method and sobol sequence method. These methods compose integrity, and confidentiality, and are also efficient. These methods are far better than those of RSA, ECC.

4.3 Design of two step secure protocol

ECDSA method is based on a finite field in cyclic form, it stands on the field and group speculations and using these, public key is employed for high level security. The RSA and other systems also provide this key but with lesser range. Thus the ECDSA method require less time and less key generation as compared to RSA. Though in ECDSA, the signature generation and verification require same time as in RSA. Signature generation algorithm and key pair generation algorithm of ECDSA needs a random number to be generated. This key should be small and should be unique and should be unpredictable so that it is free from the attackers.

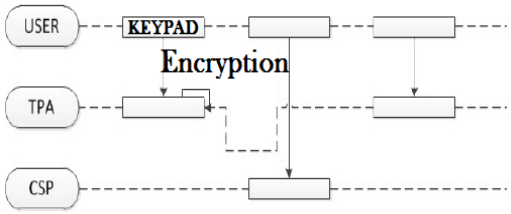

Fig 2: Setup phase

Algorithm 1:

Step1. Procedure: KeyPrd(k) ←{ PK,PR}
Step2. Take security parameter k (k>512)
Step3. Choose two random primes p an q
of size k: p≡q≡ 2
Step4. Compute n=pq
Step5. Compute Nn = lcm(p+1, q+1)
Step6. Generate random integer b<n, gcd(b, n)=1
Step7. Compute P, is a generator of En(0,b)
Step8. Private key PR={ Nn }
Step9. Public key PK={n, b, P}
Step10. Encryption(mi , S)←m'I
Step11. MetadataPrd(m'i ,n, b, P) ←Ti
Step12. Compute mi ' =mi + fk (S)
Step13. end for
Step14. end procedure

4.3.1 Verification

Now, arises the verification stage where the data verification is done by examining our system through various challenges and we have done it through following algorithms such as challenge, proof generation and check proof.

Algorithm 2:

Step 1. Procedure: Challenge(j,Q, kf) ←challenge
Step 2. Produce a random key kF
Step 3. Compute Q=rPε En(0,b)
Step 4. Create Challenge ={ kF, j, Q}

© 2014, IJOURNALS All Rights Reserved

Step 5. End Procedure

As soon as the server receives a challenge, it will generate an integrity proof with mi, encrypted form of data and chal as inputs and compute R as output by generating random numbers using Fibonacci function.

After creating challenge and proof, now it's the turn to check proof i.e.to check the integrity using public key pk, challenge query chal, and proof production R, as inputs and output 0 or 1 depending on the integrity of the file verification. If the integrity of file is verified as successfully then it will generate output as 1 else 0.

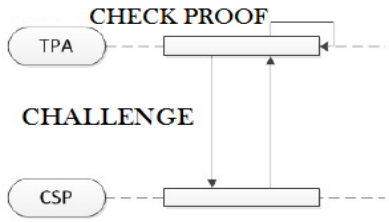

Fig 3: Verification phase

Algorithm 3:

Step 1. Procedure: CheckProof (T'I, r, kF, n) ←R'
Step 2. Produce n random numbers using key kF
Step 3. For 1 to n
Step 4. Produce j = ƒkF =(j)
Step 5. Compute R'=rS mod n
Step 6. Verify if(T'=R)
Step 7. return true
Step 8. else
Step 9. return false
Step 10. End if
Step 11. End Procedure

4.3.2 Dynamic data operations

The dynamic data operation is discussed at block level where Block Modification (BM), Block Insertion (BI) and Block Deletion (BD) can be done at any time by the server. These amendments are performed in general form ($Block_{op}$, U_b, N_b), where $Block_{op}$ indicates the block operation such as BM, BI and BD.

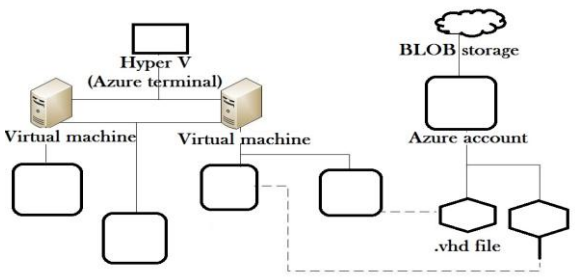

Fig 4: Data operations in windows azure

Using above algorithm we can even delete a block. The procedure will go reverse of above by creating a delete request (BD, r) and sending it to server for further delete operation which results in the construction of update version of the file F''.

Block Modification is the operation which is performed repeatedly and is accomplished using following

Algorithm 4:

Step 1. Create a new block mj
Step 2. Encrypt the new block using equation
M'Ub ← mUb+ ƒk (S)
Step 3. Compute new metadata using equation
TUb ← m'Ub P mod Nn
Step 4. Create request (BM, Ub, Nb) and sends to server.

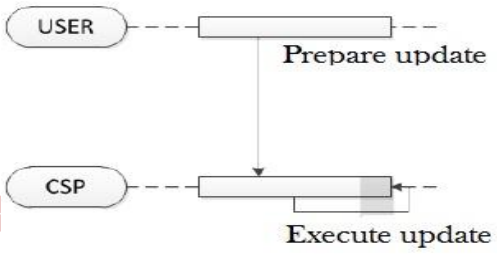

Fig 5: Data operations phase

Upon receiving an update request, the server replace the block Nb with m'Ub and construct update version of the file F'' by running algorithm 4.

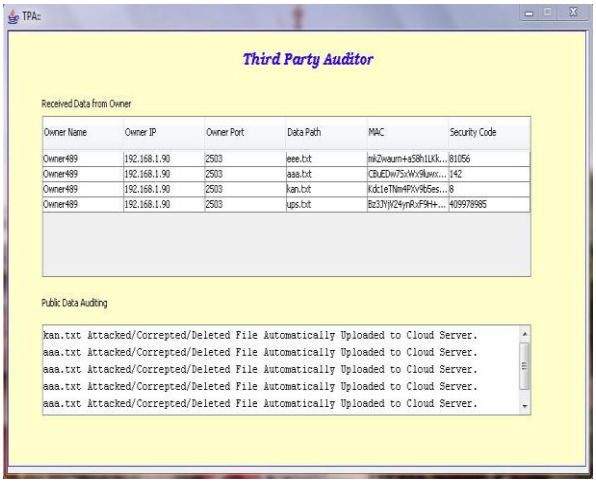

Fig 6: Third Party Auditor window

4.4 Analysis of the design

The data cannot be revealed to others stored in cloud as

IJSHR

© 2014, IJOURNALS All Rights Reserved

the secret parameter is not known eavesdropper because of Elliptic Curve Diffie-Hellman (ECDH) problem. According to the ECDLP, Suppose the equation Q=rp where Q, Pε En(a, b) and r<n. it is comparatively tough to find out r given Q and P.

Using ECDH and ECDL problems,protocol is confidential against data leakage even from TPA too which has *Ti* ← Nb *P (mod Nn)* because the secret key to be chosen by the user is purely confidential and purely unique and different every time thus the TPA also cannot tell or disclose the data to foes.

5 CONCLUSION

The provider's and the clients must make sure that the cloud is safe from all the external threats and there must be a mutual understanding between the client and the provider when it comes to the security on Cloud. Client-plus-cloud computing offers enhanced choice, flexibility, operational efficiency and cost savings for businesses and consumers. A number of regulatory, jurisdictional, and public policy issues remain to be solved in order for online computing to thrive. By using this protocol we can make our cloud highly secure and efficient. We prove that the ECDSA method generates small key size as compared to RSS method, so it can work effectively. Those users who have less resources and limited computing capability, they can use ECDSA method. It also supports public verifiability that enables TPA to verify the integrity of data without retrieving original data from the server and detects corruptions in the data as well.

6 REFERENCES

[1] Ashalatha. R, "A survey on security as a challenge in cloud computing" *International Journal of Advanced Technology & Engineering Research*, vol. 2, no. 4, July 2012.

[2] Buyya, Chee Shin, Venugopal. R "Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility," *Future Generation Computer Systems*, vol. 25, no. 6, Jun. 2009, pp. 599-616.

[3] Wang. L, Gregor Laszewski, Marcel Kunze, Jie Tao, "Cloud Computing: A Perspective Study", *New Generation Computing- Advances of Distributed Information Processing*, pp. 137-146, vol. 28, no. 2, 2008.

[4] Oprea. A, Reiter, and Yang. K, "Space-Efficient Block Storagentegrity," *Proc. 12th Ann. Network and Distributed System Security Symp. (NDSS '05)*, 2005.

[5] Brian Hay, Kara Nance, Matt Bishop, "Storm Clouds Rising: Security Challenges for IaaS Cloud Computing" *Proceedings of the 44th Hawaii International Conference on System Sciences* 2011.

[6] John C.Mace, Aad van Moorsel, Paul Watson, "The Case for Dynamic Security Solutions in Public Cloud Workflow Deployments" *School of Computing Science & Centre for Cybercrime and Computer Security (CCCS) Newcastle University, U.K.*

[7] Qiang Guo, Dawei Sun, Guiran Chang, Lina Sun, Xingwei Wang, "Modeling and Evaluation of Trust in Cloud Computing Environments" *3rd International Conference on Advanced Computer Control,* 2011.

[8] Caronni and M. Waldvogel, "Establishing Trust in Distributed Storage Providers", *In Third IEEE P2P Conference, Linkoping 03,* 2003.

[9] Wang, D. Agrawal, A.E. Abbadi: *A Comprehensive Framework for Secure Query Processing on Relational Data in the Cloud. Secure Data Management* 2011.

[10] Li, M. Krohn, D. Mazieres, D. Shasha. *Secure untrusted data repository (SUNDR). OSDI* 2004.

[11] Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z.Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," *Proc. Of CCS '07*, pp. 598–609, 2007.

[12] Shacham. H and B.Waters, "Compact Proofs of Retrievability", *Proc.14th Int'l Conference Theory and Application of Cryptology and Information Security: Advances in Cryptology (ASIACRYPT)*, pp.90-107, 2008.

[13] Yan Zhu, Huaixi Wang, Zexing Hu, Gail-J. Ahn, Hongxin Hu, Stephen S. Yau, "Dynamic Audit Services for Integrity Verification of Out-sourced Storages in Clouds," *Proc. of the 26th ACM Symposium on Applied Computing (SAC)*, 2011.

Gokulan.V B.E degree in Computer Science and Engineering from Jawaharlal Institute of Technology, Anna University, Chennai, Tamil Nadu India in 2012. Currently, pursuing M.E degree in Software Engineering from SNS College of Technology, Anna University, Chennai. His area of interest are cloud computing, processing of applications energy effectively in android- cloud environment.

Professor Dr. T. Kalaikumaran, is presently Professor & Head in the Department of Computer Science & Engineering, SNS college of Technology (An Autonomous Institution), Coimbatore. He received M.E degree from the Anna University, Chennai and Ph.D degree from Anna University, Chennai. His area of interest includes data mining and specifically, he is into detecting hotspots in crime.

Professor Dr.S.Karthik is presently Professor & Dean in the Department of Computer Science & Engineering, SNS College of Technology, affiliated to Anna University Coimbatore, Tamilnadu, India. He received the M.E degree from the Anna University Chennai and Ph.D

© 2014, IJOURNALS All Rights Reserved

degree from Anna University of Technology, Coimbatore. His research interests include network security, web services and wireless systems. In particular, he is currently working in a research group developing new Internet security architectures and active defense systems against DDoS attacks. Dr.S.Karthik published more than 35 papers in refereed international journals and 25 papers in conferences and has been involved many international conferences as Technical Chair and tutorial presenter. He is an active member of IEEE, ISTE, IAENG, IACSIT and Indian Computer Society.

IJSHRE

© 2014, IJOURNALS All Rights Reserved