Cloud Data Storage Security Techniques and Security Issues on Mobile device

Seema Banduji Bhalekar [1]
Dept of Computer Science,
Amravati University
Amravati, MS. India

V. M. Thakare[2], Ph. D
SGB Amravati
University, Amravati,
MS. India

U.S. Junghare[3]
Brijlal Biyani Science SGB
College, Amravati,
MS. India,

ABSTRACT

Cloud computing is a revolution which has made world of internet more like a place of dynamic storage. It has made a lot of changes in infrastructure side. It has deeply impacted the software industry. Many companies and institution are used cloud computing technology but major security issues are how the data keep secured and safe.

This paper discussed the different cloud data storage security techniques and analyzes the issue of the data security.

Keyword

Mobile cloud computing, data security techniques, issues.

1. INTRODUCTION

Cloud computing is the new technology of the networking. User's data is stored on the cloud storage servers maintained by service provider. It contains pay as you go pricing model. It can be dynamically delivers the services over the internet on user demand.

Mobile cloud computing is today's most inviting technology due to its cost efficiency and flexibility. This technology holds the potential to reduce the requirements of expensive computing infrastructure for the IT-based solution and services that the industry uses. It promises to provide a flexible IT architecture and it accessible through internet for hand held devices [1].

Mobile devices are becoming the most essential part of life. The market of mobile phones has expanded rapidly. Due to rapid progress, mobile computing becomes a powerful part in development of IT [2].

In mobile cloud computing data processing and storage happens away from the mobile device, it does not have large storage capacity. Due to storing data on cloud there is an issue of data security. As the internet enabled mobile devices including smart phone and tablet continue to grow, web based malicious threats will continue to increases in number to make more complex. So the data security is more critical in mobile cloud environment.

2. DIFFERENT DATA SECURITY TECHNIQUES

As the data is stored on the cloud server outside of the mobile, so the security has the major concern. User does not have any assurance that their data is properly stored on the server. This paper discussed the different security technique as given below.

2.1. Homomorphic token pre-computation technique

R. Vasu et al [3] investigated the problem of the data security in cloud data storage. Author proposed an effective and flexible distributed scheme to ensure correctness of user's data in cloud data storage which can able to update, delete, insert and append the data and also proposed an erasure correcting code to provide redundancy on data vectors and guarantee of the data dependability. To achieve the integration of storage correctness insurance, the homomorphic token Pre-computation technique is utilized.

Following steps are involved to achieve security on user's data.

2.1.1. File distribution preparation

In this scheme F-data file is split into fixed size of blocks which are stored on server. Data block is represented as element in Galois field GF (2p) for p=8 to 16. This techniques disperse the data file F redundancy across a set of n= m + k distributed server.

2.1.2. Token pre-computation

This technique is used to detect correctness of the data storage. It is used to achieve assurance of the data storage as well as data error localization. When user wants to check the correctness of the data, user can send the challenge token to the cloud server. Each cloud server computes the token on the data vector and sends them to user. If the data is not matched, modification has been done by unauthorized user.

2.1.3. Challenge token function and error localization

In this technique user can verify the correctness of the data stored on the cloud server. For the detection of the error, users send the challenge token and select the filename. Cloud service providers select the server and send the data to the client, upon receiving challenge request. Then client generated the token. If the token are not matched, data is not store to the server. In this condition service provider ask to correct the data on the server.

2.2Mobicloud

A. S. Shimpi et al. [4] proposed a new mobile cloud framework known as Mobicloud. ESSI plays an important role in mobicloud. It is a virtual machine that is designed for an end user having full control of the information stored in its virtual hard drive. Author presented new mobile framework through trust management and private data isolation.

2.2.1. Mobile cloud trust management

The trust management model of mobile cloud includes identity management, key management and security policy enforcement. It used user centric identity management that allows an individual full control for identities. It also implies that user has control over the data sharing over the internet and also can transfer and delete the data when required. Author introduced an integrated solution involving identity based cryptography and attribute based data access control to construct the trust management system for mobile cloud. It proposed fully functional identity based encryption scheme which has chosen cipher text security in random oracle model

2.2.2. Multitenancy

Multitenancy is one of the key feature of cloud services. User's data is stored in one big database and unique encryption key is used to secure data for each users .The proposed multitenant data management system partition on the data into two security level

1) Critical data
2) Normal data.

Critical data secured by data encrypted key generated by the user and normal data is secured by data encrypted key generated by cloud service provider.

2.3. Cryptographic technique

L. Ma et al. [5] proposed advanced cryptographic technique for data privacy in cloud storage. It proposed a family of scheme for data privacy such as ID-PKC, CL-PKC, key escrow encryption, threshold decryption and IDA based scheme.

2.3.1. ID-PKC based scheme

When data sharing invitation sent to group member by email, it is difficult to enhance extra data security. For this it proposed ID base public key cryptography (ID-PKC). In this scheme ID (email address) is available that is widely use. Trusted email provider (TTP-CLD) perform as private key generating centre (KGC) It generate private key of users from users ID- email address. CLT is the data owner for the cloud storage. Cloud provider CLD returns account information to owner CLT via mail

The steps of this scheme is as follows

1) TTP-CLD provide private key when the owner CLT applied. The TTP-CLD generate private key from user ID-email address
2) Security parameter KCZ^{+} is given. Setup algorithm run BDH parameter generator IG by taking input k. It generates two groups G1, G2 of order q and an admissible bilinear map e: G1*G2→G2. Then P € G_i will be choose. S € Z_q pick randomly and set $P_{pub} = s^{p}$. Then cryptographic hash function H1 :{ 0, 1}*→G1* and H2:G2→ {0, 1} n chosen. c=$G1^{*}$ *{0, 1} is the cipher text. S € Zq* is the master key and system parameter param =<q, G1, G2, e, n, P, P_{pub}, H1, H2>.
3) Alice private key is generated eg.ID € {0, 1}*. Algorithm Extract computes $Q_{ID=}$H1 (ID) € G1*. S is master key so Alice private key d_{ID} is to be d_{ID} =SQ_{ID}.

Owner CLT generates a Random Group Key. If the public key of Alice is $I_{DA,}$ it computes Q_A=H1 (I_{DA}) €G1* and r€ Zq* is randomly choose to encrypt RGK like c=< rp, RGK

H2 ($g^{r}{}_{A)>}$ where g_A=e (Q_A, P_{pub}) €G2*

4) Group members request the TTP-CLD for private key
5) If the group members receives private key, it decrypt out the RGK

2.3.2. CL-PKC based scheme

Similar to the ID-PKC scheme, TTP-CLD is used in this scheme known as KGC. KGC has no access to the private key of the CLTs but it can access partial private key. It gives security parameter K. So the setup algorithm IG generates BDH parameter with input K. The private key is not generated in this scheme.

2.3.3. Key Escrow encryption based scheme

With the help of key Escrow agent, TTP-CLD can decrypt the encrypted data. Key Escrow agent (KEA) acted by public organization, government or administration agency. to store the data recovery key, it hold key Escrow component. For the data recovery component it takes DRK and DRF as inputs. Partial encrypted data perform as DRF when the data encryption is required

2.3.4. Threshold decryption scheme

ID based threshold decryption scheme is used to share secrete. It share private key. It induces a large number of keys share for each private key. CLT generate RGK to encrypt sharing data. TTP-CLD share the master key by using secrete sharing scheme. If the one party generate a random number SHR1, the other party holds the value SHR2 = master key ⊕ R. The master key can be recovered by SHR1 ⊕SHR2. By using public key, CLTs transport encrypted RGK and received private key to decrypt out RGK.

2.4. Data Integrity technique

Preeti Garg et al [6] worked on data confidentiality and access control. Author proposed a scheme for trusted authority. It provide key to data owner (DO) and generates incremental message authentication code (MAC) of the file provided by DO. DO request storage service provider (SSP) for a file. It access policy then encrypted file is send to Decryption Service provider (DSP). DSP send this file to DO as well as trusted authority.TP again generate MAC and check it for equality with previous MAC stored. If these two MAC are matched then integrity of file is verified and result is transferred to DO.

2.5. PP-CP-ABE scheme and ABDS system

Z. Zhou et al [7] present a compressive security data inquiry framework for mobile cloud computing. It consists of two schemes such as CP-ABE scheme and ABDS system.

2.5.1. A privacy preserving CP-ABE (PP-CP-ABE) scheme:-

CP-ABE used to facilitate key management and cryptographic access control in an expressive and efficient way. An attribute descriptive string assigned to a user and each user may be tagged with multiple attributes under the construction of CP-ABE. Multiple users may share common attribute which allow sensors to specify a data access policy by composing multiple attribute through logical operators such as "AND", "OR".

2.5.2. ABDS System scheme:-

ABDS system achieves scalable and fine-grained data access control, using public cloud services. Based on ABDS, user's attributes are organized in carefully constructed hierarchy. So the cost of membership revocation can be minimized. ABDS is suitable for mobile computing to balance communication and storage overhead. Thus reduces the costs of data management operations for both the mobile cloud nodes and storage service providers. The proposed solution is computation efficient for lightweight mobile devices and it is storage efficient of ABDS scheme where both data inquires and sensors only need to store log2(N) private key while N key are require when using CP-ABE scheme.

2.6. Asymmetric key approach

Mr. Y. Graham et al. [8] proposed a Asymmetric key approach. It contains two asymmetric algorithm key which is encryption key and decryption key. Decryption key is called private or secrete key because it typically kept secrete and encryption key is called public key because it spread to all. Everybody has own unique public key. Public key is able to send encrypted message to the owner of the secrete key. The secrete key can not be reconstructed from the public key.

2.7. Pre-computed Token scheme

D. Purushothaman et al [9] proposed pre-computed token scheme. In this technique some shortest verification token are generated. It will help to ensure security in cloud storage. If the

user wants to check the correctness of the data in the cloud then user send challenge to the cloud server. Upon receiving challenge, it asks user whether it is authorized user or not. When assurance is received to the cloud server it computes the short signature over the specified block and returns them to the user. If it matched, user data is correct and then it store to the cloud server

2.8. RC4 Cipher Algorithm

Vijay G.R. et al. [10] proposed RC4 stream cipher algorithm. It is used to provide the confidentiality over the different network. RC4 cipher algorithm is also used to improve the performance of processing cryptographic computation system.

This algorithm consist of two stages which process during encryption as well as decryption. It is divided into two parts. First part is the key scheduling algorithm (KSA) and a second part is Pseudo Random Generator Algorithm (PRGA). RC4 stream cipher algorithm generates a state table of fixed length 256 bytes. Key stream that XOR with plaintext and cipher text is generated during encryption and decryption

2.8.1. KSA

KSA is known as the first stage of the algorithm. KSA initialize state vectors S. This algorithm is used to initialize the permutation in the array "S". Key Length is defined as the number of bytes. It is in the range of $1 \leq$ key length ≤ 256. The array S is initialized the first to identity permutation. S is then processed for 256 iteration.

2.8.2. PRGA

It is the second stage of the algorithm. It is used to generate the output key stream that used to encrypt and decrypt the data by XORing operation

2.9. Elliptic Curve Cryptographic Technique

V. Gampala et al. [11] proposed elliptic curve cryptography to provide confidentiality and authentication of the data between clouds. It is a public key cryptosystem. In this technique public key is used for encryption signature verification and private key is used for decryption signature verification.

An elliptic curve over a field K is a nonsingular cubic curve in two variables $f(x, y) = 0$. Elliptic Curve groups for cryptography are examined with field of F_p and F_{2m}.

2.10. Public Key Cryptographic Technique

As the data storing process is done outside, security is the major concern. K. Singh et al. [12] provide Public Key Cryptographic technique to provide security of the user's data on the cloud server. This technique contained three primary services

2.10.1. Authentication

To achieve authentication over data, cloud providers enable users authentication via assigning blocking window through which user must pass by giving username and password. If the passing information is valid, user can access the data.

2.10.2. Data Integrity Security

It detects change in information during transmission of the data. It use digital signature over data to check whether change in information occur or not when user send data over cloud and extract data from cloud. To achieve data integrity during transmission of data, user first calculate hash value of message then user will retrieve own private key and encrypt hash value which was calculate from message and after that encrypted hash value will append the message and send to the cloud. Cloud providers calculate hash over data or message. If calculated hash and appended hash is not matched, cloud will not accept the data and send query for retransmission of previous data. The same procedure will be held on when user extract data from cloud. By this method both user and cloud provider will be able to detect whether data integrity is loss or not.

2.10.3. Confidentiality

In this technique, firewall and intrusion detection system is used to detect unconscious activity from the side of unauthorized servers and attackers. It stored data separated over the server according to use. The user private data is stored on one server and user's stored data which is accessible by another user is stored on another server. In that way confidential data which user use for their own use is not accessible for another user because these two servers are not have any connection. Proxy firewall avoids direction connection with internal servers of cloud on which private data of users is stored. It hides IP addresses of internal server by which servers can be protected by hackers. So user's private data is protected and confidentiality is maintained for the private data.

2.11. Hybrid textual authentication technique and CPDP

K. Murugesan et al. [13] presented a framework for multicloud. It is used hybrid textual authentication technique for user security in multicloud. Authentication scheme protected user from shoulder-surfing, dictionary attack. CPDP scheme is used to provide security and integrity to data stored on cloud. CPDP include two techniques that is hash index hierarchy and homomorphic variable response.

2.11.1. Hybrid Textual Authentication

This authentication technique consists of three phases such as registration phase, login phase and verification phase. Registration phase is the first phase of this technique in which user rates the color. In log in phase, user has to enter the password. It is based on the interface displayed on the screen. In the verification phase, the user entered password is verified with the content of the password generated during registration. User should rate RBYOLGEP color when users enter username at the time of login. An interface is displayed based on the colors selected by the user. Login interface consist of an 8×8 grid. This grid contain digit 1-8 placed randomly in the grid cells. The interface also contains a color grid which consists of 4 pairs of colors. Each pair of color represents the row and the column of grid. User get session password depending on rating given to colors.

2.11.2. CPDP scheme

This scheme provided security and integrity to data stored on cloud. The PDP is used to verify the integrity and availability of stored data in CSPs. The client uses the secrete key to pre-process the file. It generates a set of public verification information that is stored in TTP. The file as well as verification tags are transmitted to CSPs. The client can issue a challenge token for one CSP to check integrity and availability of outsourced data by using verification protocol. The CPDP include following two techniques

2.11.2.1. Hash Index Hierarchy

This architecture consists of hierarchical structure H on three layers. It represents relationship among all block for stored resources. It has three layers

1) Express Layer- It express abstract representation of the stored resources.

2) Service Layer-It immediately offers and manages cloud storage service

3) Storage Layer- It practically realizes data storage on many physical devices

In this architecture, the resources in express layer are split and stored into three CSPs in service layer. In storage layer, each CSP fragments and stores the assigned data into the storage servers. It allows logical order of the data block to organize the storage layer.

2.11.2.2 Homomorphic Verifiable Response

A homomorphism is a map f: P→Q between two groups such that f (g1+g2) = f (g1) × f (g2).

In this group, + denotes the operation in P and × denotes the operation in Q. This notation is used to define Homomorphic verifiable tags (HVTs).

This tag is given two values σ_i and σ_j for two messages mi and mj. The sum of these messages is $m_i + m_j = \sigma'$.

2.12. IDS and CIDSS technique

A. C. Donald et al [14] discussed some possible solution of the data security such as Intrusion detection technique (IDS) and cloud Intrusion detection system service (CIDSS). This solution gives following result

-Better detection of malicious code

-Reduced consumption of resources on mobile devices

-Reduced software complexity of mobile devices

It also discussed about homomorphic encryption mechanism with the combination of level 6 encryption. To secure text encode and decode level6 encryption is used. This solution provides best security and scalability during data staring.

3. ISSUE ON MOBILE DEVICE SECURITY

In the recent days securing data in mobile cloud computing has become more important. Maximum users used internet on the mobile devices. As compare to ordinary phone, smart phone is more capable for advanced computing and faster connectivity. As the use of internet on mobile device is increase, at the same time web based malicious threats is continue increases. In mobile cloud environment securing data is become more critical.

A. C. Donald et al [9] investigate the concept of mobile cloud computing, challenging security issue and branches. Some of the security issue discussed by author is as follow

1) Data loss from lost / stolen devices

2) Information Stealing by mobile malware

3) Data leakage through poorly written third party application

4) Limited computing power, limited battery and low quality display

5) Security issue such as Device security , privacy of mobile user and securing data on cloud

6) Network related issues such as bandwidth, latency, availability and heterogeneity

4. ANALYSIS

4.1. Benefits of Data security Techniques

Following table shows the common technique used to data store correctly and securely on the cloud server and its use in security on the data

Table1. Security technique and their solution

Technique	solution
CPDP scheme	provide security and integrity to data stored on cloud
IDS and CIDSS scheme	better detection of malicious code, reduced consumption , reduced software complexity of mobile devices
advanced cryptographic technique	provide data privacy protection or secure cloud storage
Asymmetric key approach	confidentiality and integrity of the data
RC-4	confidentiality over the different network
MD5,UTF8	enhance the security
Pre-computed token scheme	Data storage correctness and error localization

4.2. Limitations of the Data Security Technique

Following table shows the drawback of the some data security techniques which discussed by different authors

Table2. Security techniques and their limitation

Author name	Techniques	Limitation
D. Huang et al.	Multitenant secure data management system	• It is not scalable when database is huge.
		• Data encryption keys for users are maintained in centralized location which is vulnerable to the single point failure problem
		• Computation overhead is distributed to multiple processors in cloud system.
		• Compromising one ESSI will not impact other ESSIs.
K. Murugesan et al.	textual password technique	• vulnerable to eves dropping, dictionary attack shoulder surfing etc.

5. CONCLUSION

This paper discussed about different security technique which are helpful for data storage security such as Homomorphic token which achieve the integration of data storage correctness and data error localization. IDS and CIDSS homomorphic encryption technique which is used for better detection of malicious code, it reduced consumption of resources on mobile device. RC4, MD5, UTF8, CPDP which provide security and data integrity.

This paper also investigates the security issues on mobile device. This paper will helpful for the researcher who works on cloud data storage security.

6. REFERENCES

[1] V. Guha and Dr M. Shrivastav," Review of Information Authentication in Mobile Cloud over SaaS and PaaS Layer", International Journal of Advanced Computer Research ISSN (print):2249-7277 ISSN (online):2277-7970, Volume-3, Number-1, Issue -9, March -2013.

[2] S. Patel, "A Survey of Mobile Cloud Computing: Architecture, Existing work and Challenges", International Journal of Advanced Research in Computer Science and Software Engineering, Volume-3, Issue -6, June -2013.

[3] R. Vasu,"Techniques for Efficiently Ensuring Data Storage Security in Cloud Computing", IJCTA, Sept-Oct 2011.

[4] A. S. Shimpi and R.P. Chander," Secure Framework in Data processing for Mobile Cloud Computing", International Journal of Computer Science and Informatics ISSN (print):2231-5292, Volume-2, Issue-3, 2012

[5] L. Ma and J. Sum and Y. Li,"Comparing General paradigm on Data Secrecy Protection for Outsourced file in Mobile Cloud Computing", Journal of Networks, Volume -7, No -9, Sept -2012

[6] P. Garg and Dr V. Sharma, "Secure Data Storage in Mobile Cloud Computing", International Journal of Scientific and Engineering Research, Volume-4, Issue-4, April 2013

[7] Z. Zhou and D. Huang," Efficient and Secure Data Storage operation for Mobile Cloud Computing", 2012 8th International Conference on Network and Service Management (CNSM 2012)

[8] Mr. Y. Graham and Mr. P. Shende,"Mobile Data Security on Cloud Computing Using SAAS",International Journal of Advanced Research in Computer Engineering and Technology , Volume -2, Issue-11, November 2013

[9] 9)D. Purushothaman and Dr. S. Abburu,"An Approach for Data Storage Security in Cloud Computing", copyright(c)2012 International Journal of Computer Science Issue . All right reserved

[10] V. G. R. and R. M. Reddy,"Data Security in Cloud based on Trusted Computing Environment", International Journal of Soft Computing and Engineering, ISSN: 2231-2301, Volume-3, Isssue-1, March -2013.

[11] V. Gampala, S. Inuganti and S. Muppidi," Data Security in Cloud Computing with Elliptic Curve Cryptography", International Journal of Soft Computing and Engineering, ISSN: 2231-2307, Volume-2, Issue-3, July -2012.

[12] K. Singh, I. Kharbanda and N. Kaur," Security Issue occurs in Cloud Computing and their solution", Karmjit singh et al. / International Journal on Computer Science and Engineering, ISSN: 0975-3397, Volume-4 No. 05, May 2012

[13] K. Murugesan and S. Sudheendran, "Ensuring User Security and data integrity in multicloud", International Journal of Soft Computing and Engineering, ISSN: 2231-2307, Volume-3, Issue-2, May -2013.

[14] A. C. Donald, S. A. Oli and L. Arockiam,"Mobile Cloud Security Issue and Challenge: A Perspective", International Journal of Engineering and Innovative Technology, Volume-3, Issue -1, July -2013