The International Journal Of Engineering And Science (IJES)
|| Volume || 5 || Issue || 3 || Pages || PP -32-36 || 2016 ||
ISSN (e): 2319 – 1813 ISSN (p): 2319 – 1805

Optimizing Secured Data Using Proxy Re-Signature In The Cloud

Harshal Mahajan ,Hemant Verma
Department Of Computer Science And Engineering And Information Technology , VITS, Indore
Department Of Computer Science And Engineering And Information Technology , VITS, Indore

----------**ABSTRACT**----------
Data Storage In The Cloud And Sharing The Data With The Group Is Data Integrity Process Now Days, Data Owner Can Easily Share Data With Other Users, In The Cloud, Users Can Easily Modify And Share Data. With Data Storage & Sharing Applications (Eg. Drop Box And Google Drive) Given By The Cloud, So To Avoid Data Integrity & To Provide Data Security, Is Needed And Challenging Process. In This Paper We Propose A System Which Will Help In Integrating Data And Will Provide Security. Proposed System Uses The Shamir Secret Sharing Algorithm For Security And For Analysis HAPS .This Paper Will Focus On Construction Of PANDA, Modification Of PANDA Along With Brief Description Of Architecture Of System.

Keywords *– Data Data-Integrity, Proxy Re-Sign, Un-Authorized User Revocation.*

Date Of Submission: 01 March 2016 Date Of Publication: 16 March 2016

I. INTRODUCTION

Data Storage And Sharing With The Group Is Data Integrity Process, Data Owner Can Easily Share Data With Other Users, In The Cloud, And Users Can Easily Modify And Share Data. With Data Storage & Sharing Devices Such As (Drop Box And Google Drive) Provided By The Cloud, , Every User (User Of Sharing Devices) Is Able Not Only To Access And Change Shared Data With Addition Of New Data With Re-Signing Original Data, But Also Share The Latest Version Of The Shared Data With The Rest Of The Group. Even The Cloud Provider Assure For The Data Security There Is The Problem Of Data Integrity And Data Security It Is Due To Extensibility And Scalability Of The Software And Hardware And Failure Of Human Error. The Protect The Integrity Of Data In The Cloud, To Ensure Shared Data With Modification. Integrity Can Verify With The Third User , Data Owners As Well As Data Users In The Group Need To Compute & Re-Signatures On The Blocks In The Cloud Shared Data. Different Chunks In Shared Data Are Always Signed By Different Shareholders Of The Data Due To Data Modifications Performed By Different Shareholders Of The Data In The Cloud. For Security Reasons, Once A User Is Withdrawn From The Group, And The Chunks Which Were Previously Signed By The Member Is Resigned With The Sharing And Modifying The Data Without Using New Signature .The Mechanism Which We Are Presenting In The Paper Is To Allow A Public Verifier For The Data Integrity And Security A Number Of Mechanisms Have Been Proposed Which Were Discussed In Paper[1] [2]. In This Paper We Have Used Shamir Secret Sharing Algorithm For Security And For Analysis HAPS & Focused On System Architecture

In This System That Will Provide Verification For The Data Integrity We Can Call It As A Third Party Auditor Previous Work Which Is Focused On The Data Integrity & Security Of The System Which We Have Discussed Here With Extension Of ANDA To Increase The Integrity As Well As The Security Level. The Previous Work Which Referred Here Is In [4] & [7]. With Shared Data, If The User Modifies A Block, He/She Needs To Compute A New Signature For The Modified Block. Due To The Modifications By Any User, Different Chunks Are Signed By Different Users. For Security Reasons, When A User Leaves The Group Or Do Suspicious Activity, The User Must Be Withdrawn From The Group. As A Result, This Withdrawn User Should No Longer Be Able To Entrance Into It And Neither Modify It, And The Signatures Generated By This Withdrawn Users Validity Is Limited To The Group [5]. Therefore, Although The Content Of Shared Data Is Not Changed During User Revocation, The Chunks, Which Were Previously Signed By The Withdrawn User, Still Need To Be Re-Signed By An Existing User In The Group. As A Result, The Integrity Of The Data Can Still Be Verified With The Public Keys Of Existing Users Only.

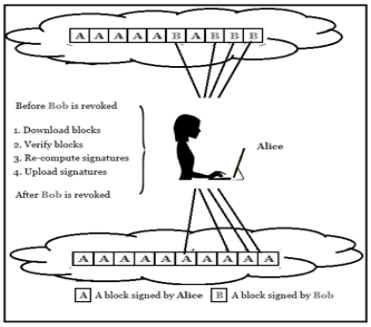

Figure 1.1: Straight Forward Approach

Since Shared Data Is Stored To The Cloud And Users Need Not Longer Store It On Local Devices, A Straightforward Method To Re-Compute All The Signatures During User Withdrawing (As Shown In Fig. 1) Is To Ask An Existing User (I.E., Alice) To First Download The Chunks Previously Signed By The Withdrawn User (I.E., Bob), Verify The Correctness Of These Blocks, Then Re-Sign These Chunks, And Upload The New Signatures To The Cloud. However, This Straightforward Method May Cost The Existing User A Massive Amount Of Communicational And Computational Re- Sources By Downloading And Verifying Blocks And By There Are So Many Facilities For Storing Data And Sharing Services Which Shares Chunks Of Data Like Google Drive. These Mechanisms Provide Several Facilities Of Modifying Data And Allow Sharing Latest Version Of Modified Data With Enduring Group. The Cloud Service Provider Issues A Good Quality Service With Sufficient Security But Data Integrity Can Be Condensed Due To Human Errors And Software Or Hardware Failure. For Maintaining Integrity In Shared Data Many Methods Have Been Proposed. Every Data Block In Group Data Is Attached With Signature By User Responsible For Updating Of Data. Data Integrity Is Depending Upon The Correctness Of Signature. Here, A Data In Each Block Is Having Signature, And Also The Knowledge Integrity Is Depend On The Accuracy Of All The Signatures. An Efficient Approach To Check Integrity Of Data Without Downloading Complete Data Within A Group. This Has To Be Done By Means Of Public Verifier Which Is Using Cloud Data And A Third Party Auditor (TPA) Have An Capability Of Confirmation On Integrity Of Data. Many Existing Works Illustrates Auditing On The Integrity Of Personal Knowledge. The Latest Work In Cloud Focuses On Conserving Identity Of User From Worldwide Cloud Verifiers During Maintaining Integrity Of Group Data. But None Of Existing Method Provides Methodology.

1. Problem Statement

In This Paper, We Discussed The Data Integrity And Security Model, For The Cloud Computing & Illustrate The Objectives Of Our Proposed Mechanism.

1.1 Proposed System Architecture

2.1.1. Shared Data In Cloud
2.1.2. Revocation Of Users
2.1.3. Proxy Resignatures
2.1.4. HAPS Construction
2.1.5. PANDA Construction
2.1.6. PANDA Extension
2.1.7. Evaluation Of Performance

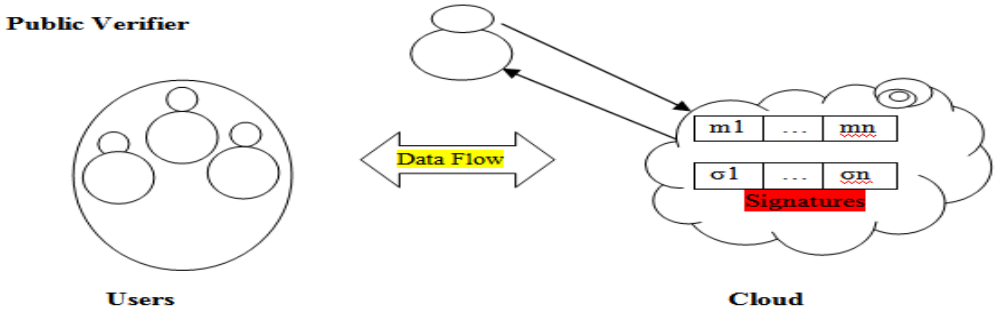

Figure 2.1: System Architecture

2.1.1. Shared Data In Cloud

Data Which Is Shared In The Cloud Module Has Secured And Provide Reliable Environment To The Users, The Integrity Of Data In The Proposed System Compromise The Integrity, Due To The Existence Of Peripheral Failures And Individual Errors. To Protect The Integrity Of Data In The Cloud Numbers Of Mechanisms Have Been Proposed. In The Proposed System, A Signature Is Attached To Each Block In Data. Once A User Alters Chunk Of Data Shared Data, User Needs To Compute A New Signature For The Modified Block. This Module Is Used For Checking Data Integrity In The Cloud.

2.1.2. Revocation Of User Module: The Revocation Of User In A Group Is Carried Out Based On Some Security Reasons Revoked User Won't Be Able To Access And Alter Shared Data. In This Module Once The User Withdrawn From A Group The Chunks Of Data Distributed By The Withdrawn User Must Be Resigned By Existing User Using The Public Key. Resigning Will Increase The Integrity Of The Whole Data Can Be Verified With The Public Keys Of Existing Users Only.

2.1.3. Proxy Re-Signatures Module: This Proxy Re-Signature Module Is A Translator Between Two Users Allows A Semi-Trusted Proxy To Act As A Translator Of Signatures Between Two Users. The Interchanging Of Signature Of Two Users. Meanwhile, The Proxy Is Not Able To Learn Any Involved Users Private Keys And The Cloud Act As The Proxy In The Module And Alter Signatures For Users During User Withdrawn Process. Efficiency Will Be Improved During User Revocation Progress.

2.1.4. HAPS Construction Module: Proxy Re-Signature Scheme Are Not Block Less Verifiable, If We Directly Apply These Proxy Re-Signature Schemes As Discussed Abovethen A Verifier Has To Download The Entire Data To Check The Integrity. In The Proposed System HAPS Is Used, Homomorphic Authenticable Proxy Re-Signature Is A Chunk Less Provable And Nonmalleable Scheme. HAPS Uses Different Algorithms (Keygen, Rekey, Sign, Resign And Verify) Increasing The Chunk Less Data Verification On Shared Data.

2.1.5. PANDA Construction Module: A Public Auditing Mechanism For Shared Data With Efficient User Revocation (PANDA) Allows The Data Owner Who Acts As The Group Administrator And Withdraws Users From The Group When It Is Necessary. This Module Of The Cloud Is Used To Perform As The Semi-Trusted Proxy And Translate Signatures For Users In The Group With Resigning Keys, So As To Avoid Data Integrity; The Re-Signing Has Been Performed By The Cloud In This Module Which Improves The User Withdrawing Efficiency And Also It Saves Communication And Computation Resources For Existing Users.

Panda Includes Six Algorithms: Keygen, Rekey, Sign, Resign, Proofgen, And Proofverify.

 In Keygen, Every User In The Group Produces Its Own Public Key And Private Key

In Rekey, The Cloud Computes A Re-Signing Key For Each Pair Of Users In The Group.

 In Sign, When User Shares Data He/She Can Compute Signature Along With The Data Block.

 In Resign, If Any User Is Withdrawn From The Group, Then The Cloud Then The Chunks Are Re-Signed The Which Were Previously Signed By This Withdrawn User With A Resigning Key.

 In Proofgen Under The Challenge Of A Public Verifier The Cloud Is Able To Produce A Proof Ownership Of Shared Data.

 In Proofverify, A Public Verifier Is Capable In Checking The Correctness Of A Proof Responded Cloud

2.1.6. PANDA Extension Module: In This Section, We Will Make Use Of Several Different Verification Methods To Extend Our PANDA In Terms Of Finding Reliability, Scalability, Probability And.

A. Detection Probability:

As Presented In Our Mechanism, A Verifier Selects A Number Of Random Blocks Instead Of Choosing All The Chunks In Shared Data, Which Will Improve The Efficiency Of Auditing.

B. Scalability: To Improve The Results Of Probability, Extensibility And Scalability Of Proposed Mechanism By Reducing The Total Number Of Resigning Keys In The Cloud And Enabling Chunk Verification For Verifying Multiple Verification Tasks Concurrently.

• Reduce The Data Integrity Due To Re-Signing Keys: As Described In Anda, The Cloud Needs To Establish And Maintain A Re-Signing Key For Each Group Of Two Users. Since The Number Of Users In The Group Is Denoted By D And The Total Number Of Re-Signing Keys For The Group Is D(D 1)/2. If The Cloud Data Is Shared By Many Users, E.G. D = 300, Then The Total Number Of The Data With Re-Signingned

Keys That The Cloud Must Store With Security And Adjust Is 19, 900, Which Significantly Increases The Complexity Of Key Management In Cloud.

• Batch Auditing For Multiple Auditing Tasks: To Improve The Scalability Of Our Public Verification Process In Such Cases, We Can Further Extend The Aanda Algorithm To Support Batch Auditing By Make Use Of The Properties Of Bilinear Maps. With Batch Auditing, A Public Verifier Perform Multiple Auditing Tasks Simultaneously. Compared To The Batch Auditing In, Where The Verification Of Data In Each Auditing Task Are Generated By A Single User, Our Chunk Checking Process Needs To Perform On Multiple Tasks Where The Verification Metadata In Each Verification.

C. Reliability Of Panda: In Our Mechanism, It Is Hard For The Cloud To Store Secured Data And Administer The Re- Signing Keys, So That The Cloud Can Of Correctly And Successfully Convert Signatures From The Withdrawn From Group, User To An Existing User When It Is Necessary. However, Due To The Existence Of By The Internal Attacks, Only Storing These Re-Signing Keys In The Cloud With Re-Signing Of The Data Holder Proxy May Sometimes Allow Attackers To Disclose. These Data With Re-Signed Keys And Randomly Convert Signatures On The Data Provided By The Shareholder Of The Data, Even No User Is Withdrawn. Obviously, The Arbitrary Mistreat Of Re-Signing Keys Will Change The Ownership Of Corresponding Blocks In Shared Data Without Users' Permission Using Data, Affect The Integrity Of The Data By The Data Owner In The Cloud. To Prevent The Use Of Re-Signing Keys And Enhance The Reliability Of Our Mechanism, We Propose A System With An Extensive Version Of Our Mechanism, Denoted As Panda, In The Multi-Proxy Model.

2.1.7. Evaluation Of Performance Module: The Vital Purpose Of Panda Is To Enhance The Effectiveness Of User Revocation. In Resigning Of Chunk Of Data Tasks Are Involved Which Are Easier With The Accomplishment Of Cloud Resigning Mechanism Dramatically Increases The Performance. Our Mechanism Is Quite Efficient For Supporting Large Groups And It Allows Involved Verifier To Perform Batch Auditing Tasks.

3. Description Of System With Security Model

We Will Work In The System On The Using Three Parameters, 1) Cloud 2) The Public Verifier, And 3) Users (Who Share Data As A Group) .The Cloud Offers Data Storage And Sharing Services. And The Proposed System In The Cloud Provides Security In Data Integrity. The Public Verifier, Such As A Client Who Would Like To Utilize Cloud Data For Searching(Using Search Engine) Or A Third-Party Auditor (TPA) Can Provide Verification On Data Integrity Intend To Check The Integrity Of Shared Data Via A Request-And-Response Protocol With The Cloud. In The Group, Single User And The Group Users. The Original User Is The Holder Of Data. This Holder User Creates And Distribute Data Within The Group Through The Cloud. Data Holder And Other Users Can Access, Download And Modify Shared Data. Shared Data Is Separated Into A Number Of Chunks. A User In The Group Can Modify A Block In Shared Data By Performing Modification Operation On The Block.

The Cloud Itself Is Semi-Trusted Assumed In The System Which Used In The Paper, Which Means It Follows Rules And Does Not Contaminate Data Integrity As A Nasty Adversary, But It Verifying Multiple Auditing Tasks Simultaneously.

IV. Preliminaries

4.1. Bilinear Maps:

Let G1, G2 And G*T* Be Three Multiplicative Cyclic Groups Of Prime Order *P*, *G*1 And *G*2 Be The Generators Of G1 And G2. ψ Is A Computable Isomorphism From *G*2 To *G*1, With $\psi(G2) = G1$. The Map *E*: G1 $\times$ G2 $\rightarrow$ G*T* Is Said To Be An Admissible Bilinear Pairing If The Following Conditions Hold True.

(1) *E* Is Bilinear, I.E. For All $A, B \in Zp$.

(2) *E* Is Non-Degenerate,

(3) *E* Is Efficiently Computable.

4.2. Blind Signatures:

Blind Signatures Had Been First Proposed By Chaum, Form A Special Type Of Signatures Where The Message Owner And The Signer Are Different Parties. More Specifically, The Message Owners Choose A Blinding Factor To Blind The Content Of Her Message And Send The Blinded Message To The Signer. After Received The Blinded Message, The Signer Generates A Signature On The Blinded Message And Returns It To The Message Owner. The Message Owner Is Able To Recover And Output A Regular Signature On The

Original Message Based On The Result Returned By The Signer And The Blinding Factor. The *Blindness* Properties Require That The Signer Cannot Learn The Content Of The Original Message During The Generation Of A Signature. For *Unlink Ability*, It Requires That The Signer Cannot Link A Blinded Message/Signature To Its Corresponding Unblended Form.

4.3. Shamir Secret Sharing:

A (W, T)-Shamir Secret Sharing Scheme, Where W = (2t − 1), Is Able To Divide A Secret S Into W Pieces In Such A Way That This Secret S Can Be Easily Recovered From Any T Pieces, While The Knowledge Of Any (T − 1)Pieces Expose No Information About This Secret S. The Essential Idea Of A (W, T)-Shamir Secret Sharing Scheme Is That, A Number Of T Points Define A Polynomial Of Degree (T−1). Suppose We Want To Share The Secret S To Zp.

We Set A0 = S And Define The Following Polynomial

F(X) = At−1xt−1 + ・ ・ ・ + A1x + A0, (1) By Picking At−1, ・ ・ ・, A1 Uniformly At Random From Zp. Each Piece Of The Share Is Actually A Point Of Polynomial F(X), For Example, (Xi, F (Xi)). The Secret S Can Be Recovered By At Least A Number Of T Points Of Polynomial F(X) With Lagrange Polynomial Interpolation. Shamir Secret Sharing Is Generally Used In Key Management Schemes And Secures Multi Computation.

V. Conclusion

In This Paper, We Introduce A Modified System For The Data Integrity And Security. For The Security We Have Used Security Model Shamir Secret Sharing Algorithm & For The Security Analysis We Used Haps Is The Right Approach To The Achieve Anonymity In Stored Data In The Cloud Which Is With Publicly-Verifiable Data- Integrity In Mind. Our Approach Decouples The Anonymous Protection Method From The Data Tenure Mechanism Via The Use Of Security Mediator. Our Solution Not Only Reduces The Calculation Of Data Tenure Mechanism And Bandwidth Requirement Of This Mediator, But Also Minimizes The Trust Placed On It In Terms Of Data With Confidentiality And Identity. The Efficiency Of Our System Is Also Empirically Demonstrated. When A User Withdrawn From The Group And Allowing The Semi-Trusted Cloud To Re-Sign Blocks That Were Signed By The Revoked User With Proxy Re-Signatures. Results Are Improved In Terms Of Efficiency Of User Revocation, And Available Users In The Group Can Save A Improved Result And Communication Resources During Process Of Revocation Of User

REFERENCES

[1] B Wang, B. Li, And H. Li, "Public Auditing For Shared Data With Efficient User Revoation In The Cloud," IEEE Transaction On Service Computing 2014.

[2] B.Wang, B. Li, And H. Li, "Public Auditing For Shared Data With Efficient User Revoation In The Cloud," In The Proceedings Of IEEE INFOCOM 2013, 2013, Pp. 2904- 2912.

[3] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, And M. Zaharia, "A View Of Cloud Computing," Communications Of The ACM, Vol. 53, No. 4, Pp. 50-58, April 2010.

[4] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, And D. Song, "Provable Data Possession At Untrusted Stores,"In The Proceedings Of ACM CCS 2007, 2007, Pp. 598-610.

[5] H. Shacham And B. Waters, "Compact ProofsOf etrievability," In The Proceedings Of ASIACRYPT 2008. Springer-Verlag,2008,Pp. 90-107.

[6] C. Wang, Q. Wang, K. Ren, And W. Lou, "Ensuring Data Storage Security In Cloud Computing," In The Proceedings Of ACM/IEEE Iwqos 2009, 2009, Pp. 1-9.

[7] Q. Wang, C. Wang, J. Li, K. Ren, And W. Lou, "Enabling Public Verifiability And Data Dynamic For Storage Security In Cloud Computing," In The Proceedings Of ESORICS 2009. Springer-Verlag, 2009, Pp. 355-370.

[8] C. Wang, Q. Wang, K. Ren, And W. Lou, "Privacy-Preserving Public Auditing For Data Storage Security In Cloud Computing," In The Proceedings Of IEEE INFOCOM 2010, 2010, Pp. 525-533.