International Journal of Engineering Science Invention (IJESI)
ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726
www.ijesi.org ||Volume 7 Issue 3 Ver. VI || March 2018 || PP23-27

A Review On Data Integrity Models And Schemes

Pramod Kumar, Dr. Vikram Kapoor, Dr. Manmohan Singh Rauthan
Dept. Of Computer Science& It Uttarakhand Technical UniversityUa, India
Dept. Of Computer Science & ItUttarakhand Technical University Ua, India
Dept. Of Computer Science & Eng.Hnb Garhwal University, SrinagarUa, India
Corresponding Auther: Pramod Kumar

Abstract—*The Applications Stored On Remote Servers And Executing On The Internet Might Compromise To Data Integrity. Data And Information Sharing Among Multiple Organizations Is Crucial In Public Channel To Effectively Make Cooperative And Mission-Critical Decisions And Assurance Of Data Integrity Is Challenging In The Presence Of Collaborative Parties That Make Frequent Data Modifications. Data Integrity Refers To Prevention Of Unauthorized And Improper Data Modification.The Present Study Gives Recent Developments In The Area Of Data Integrity Models And Schemes With Their Comparative Analysis. It Also Presents Drawback Of Data Integrity Models And Provides Guidelines To The Design And Development Of Best Data Integrity Models And Scheme.We Have Taken Various Data Integrity Models And Schemes As Sample For Efficiency Comparisons And Discuss The Results Based On Various Operation Used In Respective Schemes.This Paper Identified Various Data Integrity Requirements Which Are Must Require In Strong And Efficient Data Integrity Models And Schemes.*

Keywords—*Remote User, Data Integrity, Message Digest, Hash.*

Date of Submission: 19-03-2018 Date of acceptance 02-04-2018

I. INTRODUCTION

In 1975, Kenneth J. Biba Have Developed A Formal State Transition System Of Computer Security Policy That Describes A Set Of Access Control Rules Designed To Ensure Data Integrity [1].In 1987, Clark–Wilson Integrity Model [2] Specify And Analyzes An Integrity Policy For A Computing System Which Is Foundation Of Data Integrity Models. They Have Commented On The Issue Of Improper Data Modification Using Well-Formed Transactions Between Users And Servers. The Model Is Primarily Concerned With Formalizing The Notion Of Information Integrity. Data Integrity Is Maintained By Preventing Modification Of Information In A System Due To Either Malicious Intent Or Network Error. Clark–Wilson Integrity Model [2] Describes How The Information In The System Should Be Kept Secure From One State Of The System To The Next State. They Claimed That This Model Defines Data Integrity Enforcement Rules And Certification Rules While Biba's Integrity Model Prevents Possible Data Corruption By Limiting Information Flow Among Data Objects3. Clark And Wilson Find Out That The Existing Data Integrity Models Such As Biba’s Model Is Better Suited To Imposing Data Integrity Rather Than Enforcing Information Confidentiality

Md-5 Stands For Message-Digest Algorithm[5]. Md-5 Algorithm Is Co-Invented By Rivest In Mit Computer Science Laboratory And Rsa Data Security Company [5] In 1992. Md-5 Is A Non-Reversible Encryption Algorithm. It Calculates A 128-Bit Digest For An Arbitrary L-Bit Message. It Is An Enhanced Version Of Its Predecessor Md-4. Md-5 Has Been Applied In Many Applications, Including Digital Signature (Ds), Encryption Of Stored Information In A Dbms And Encryption Of Communication Information On Networks. Md-5 Makes Large Amounts Of Data To Be Compacted Into A Secure And Confidential Format Before Signing The Private Key By Digital Signature. A Brief Description Of Md-5 Algorithm As Follows: Md-5 Algorithm Divides Plaintext Input Into Blocks Of 512-Bit, And Each Block Is Again Divided Into Sixteen(16) Words Of 32-Bit, After A Series Of Processing, The Outputs Of The Algorithm Consist Of Four 32-Bit Message Words. After These Four 32-Bit Message Words Are Cascaded, The Algorithm Generates A 128-Bit Hash Value Which Is The Required Cipher-Text. The Algorithm Could Be Described In Two Stages: Pre-Processing And Hash Computation. Preprocessing Involves Padding A Message, Parsing The Padded Message Into M-Bit Blocks, And Setting Initialization Values To Be Used In Hash Computation. The Final Hash Value Generated By The Hash Computation Is Used To Determine The Message Digest.

In 1993, A Secure Hash Algorithm Was Developed By National Institute Of Standards And Technology (Nist) And Published As A Federal Information Processing Standard In 1993 [6]. It Calculates A 160-Bit Digest For An Arbitrary L-Bit Message. Pre- Processing Is Done Same As In Md-5[5] Except That An Extra 32- Bit Register E Is Added With An Initial Value Of C3d2e1f0. Other Registers Are Assigned With

Higher Order Bytes First. For Each Block, It Requires 4 Rounds Of 20 Steps, Resulting In A Total Of 80 Steps, To Generate The Message Digest.

In 1996, Mihir Et Al.'S [7] Showed That The Use Of Cryptographic Hash Functions Like Md-5 [5] Or Sha [6] For Message Authentication Are Very Easy To Implement, These Mechanisms Are Usually Based On Ad Hoc Techniques That Lack A Sound Security Analysis. They Present New Constructions Of Message Authentication Schemes Based On A Cryptographic Hash Function. Schemes [7], Nmac And Hmac, Are Proven To Be Secure As Long As The Underlying Hash Function Has Some Reasonable Cryptographic Strengths. Moreover They Show, In A Quantitative Way, That The Schemes Retain Almost All The Security Of The Underlying Hash Function. In Addition Schemes [7] Are Efficient And Practical.

In 2007, Ben Moss [4] Showed That Integrity Is Not Only A Fundamental Aspect Of Virtue, It Is Also A Fundamental Problem In Computer Security. In Both Contexts It Has A Similar Meaning; The State Of Being True, Honest, Pure Or Whole. In The field Of Security, The Integrity Problem Concerns The Unauthorized Modification Of Data: In Other Words, Tampering. Ben Moss Proposes A Well-Defined Model For The Data Integrity Problem. This Model Considers The Problem As Four Distinct Sub-Problems, Allowing A Formal Definition To Be Constructed For Each One.

The Problem Encapsulates The Following Sub-Problems:

- Detection: Determining Any Modification In The Exposed Data;
- Location: Identifying Any Instances Of Modification In The Exposed Data;
- Correction: Restoring Any Instances Of Modification In The Exposed Data To Their Original State;
- Prevention: Precluding Any Instances Of Modification In The Exposed Data.

In Cloud Computing One Of The Major Threats Is Data Privacy And Data Integrity. There Is Lot Of Research Going On In This Field To Ensure And Provide Data Integrity In Cloud Storages. Many Solutions Have Been Provided To Focus On Resolving The Issues Of Integrity.

In 2007, Juels And Kaliski [8]Proposed A Model Proofs Of Retrievability (Por) Was One Of The First Most Important Attempts To Formulize The Notion "Guaranteed Remotely And Reliable Integrity Of The Data Without The Retrieving Of Data File." It Is Basically A Data Encryption Mechanism Which Detects Data Corruptions And Retrieve The Complete The Data Without Any Damage.

In 2008, Shacham And Waters [9] Gave A New Model For Por Enabling Verifiability Of Unlimited Number Of Queries By User With Reduced Overhead. Later Bowels And Juels11 Gave A Theoretical Model For The Implementation Of Por, But All These Mechanisms Proposed Were Weak From The Security Point Because They All Work For Single Server. Therefore Bowels11 In Their Further Work Gave A Hail Protocol Extending The Por Mechanism For Multiple Servers.

In 2007, Atienies And Burns [12] Gave Provable Data Possession (Pdp) Mechanism Which Verifies The Integrity Of Data Being Outsourced, Detecting All Kind Of Errors Occurring In Data But Doesn't Guarantee Complete Data Retrievable.

In 2008, Atienies And Pietro [13] Proposed A Scheme Which Overcome All Problems In Pdp, But The Main And Basic Problem On Both Proposed System Didn't Overcome Was They Work On Single Server. Therefore, Later Curtmola [14] Proposed A Scheme To Ensure Data Reliability And Retrievability Of Data For Multiple Servers. Many Mechanisms Has Been Proposed Till Now To Guarantee And Ensure Complete Data Integrity And Data Privacy Of Cloud Storages Based On Encryption And Cryptographic Mechanisms Using Hash Values And Data Encoding.

In 2010, L. Thulasimani Et Al.'S [15] Proposed Vlsi Architecture For Implementation Of Integrity Unit In Sdr. The Proposed Architecture Is Reconfigurable In The Sense It Operates In Two Different Modes: Sha-192[6] And Md-5 [5].Due To Applied Design Technique The Proposed Architecture Achieves Multi-Mode Operation, Which Keeps The Allocated Area Resource At Minimized Level. The Proposed Architecture Also Achieves High Speed Performance With Pipelined Designed Structure. Comparison With Related Hash Function Implementation Has Been Done In Terms Of Operating Frequency, Allocated-Area And Area-Delay Product. The Proposed Integrity Unity Can Be Integrated In Security Systems For Implementation Of Network For Wireless Protocol, With Special Needs Of Integrity In Data Transmission.

In 2010, Danyang Cao Et Al's[16] Showed That The Message Digest To Be Generated By Md-5 Algorithm Has The Irreversible And Non-Counterfeit Features, So Md5 Algorithm Is Superior In Anti-Tamper Capability. This Paper Implements A Data Integrity Checking System Based On Md-5 Algorithm. The System Aids System Administrators To Monitor Their File Systems For Unauthorized Modifications. The Main Goal Of The System Is To Detect And Prevent Malicious Replacement Of Key Files In The System By Trojans Or Other Malicious Programs. It Plays A Protective Role Which Prevents The Hacker And The Virus From Invading. Practice Has Shown That The It Departments Of The Enterprise Achieve The System Management And Security Auditing With The Data Integrity Checking System, It Brings Visible Benefits To The Enterprise.

II. Literature Review

The Cloud Computing Is A Latest Technology Which Provides Various Services Through Internet. The Cloud Server Allows User To Store Their Data On A Cloud Without Worrying About Correctness & Integrity Of Data. Cloud Data Storage Has Many Advantages Over Local Data Storage. User Can Upload Their Data On Cloud And Can Access Those Data Anytime Anywhere Without Any Additional Burden. The User Doesn't Have To Worry About Storage And Maintenance Of Cloud Data. But As Data Is Stored At The Remote Place How Users Will Get The Confirmation About Stored Data. Hence Cloud Data Storage Should Have Some Mechanism Which Will Specify Storage Correctness And Integrity Of Data Stored On A Cloud. The Major Problem Of Cloud Data Storage Is Security. Many Researchers Have Proposed Their Work Or New Algorithms To Achieve Security Or To Resolve This Security Problem. In This Paper, We Propose A New Innovative Idea For Privacy Preserving Public Auditing With Watermarking For Data Storage Security In Cloud Computing. It Supports Data Dynamics Where The User Can Perform Various Operations On Data Like Insert, Update And Delete As Well As Batch Auditing Where Multiple User Requests For Storage Correctness Will Be Handled Simultaneously Which Reduce Communication And Computing Cost.

To Achieve Security, We Can Handover Our Data To A Third Outsource Party Who Will Specify The Correctness And Integrity Of The Cloud Data. Hence, New Concept Arrives As Third Party Auditor (Tpa) Who Will Audit The User Data Stored On The Cloud, Based On The User's Request. In This Case, The Cloud Service Provider Doesn't Have To Worry About The Correctness And Integrity Of The Data. In This Technique, Tpa Will Audit The Cloud Data To Check The Integrity Or Correctness In Two Ways As: 1) Download All Files And Data From The Cloud For Auditing. This May Include I/O And Network Transmission Cost. 2) Apply Auditing Process Only For Accessing The Data But Again In This Case, Data Loss Or Data Damage Cannot Be Defined For Un-Accessed Data. Public Audit Ability Allows User To Check Integrity Of Outsource Data Under Different System & Security Models. We Cannot Achieve Privacy As Tpa Can See The Actual Content Stored On A Cloud During The Auditing Phase. Tpa Itself May Leak The Information Stored In The Cloud Which Violate Data Security. To Avoid This, Encryption Technique Is Used Where Data Is Encrypted Before Storing It On The Cloud. Through This, We Achieved Privacy Up To Certain Extent But Which Increases Complex Key Management On User Side. This Technique Cannot Be Long Lasting As Unauthorized User Can Easily Access Original Content By Using The Decryption Key Which Is Easily Available. Hence To Achieve Privacy Preserving Public Auditing Using Tpa For Cloud Data Storage Security, Researchers Have Proposed Various Techniques.

A. Mac Based Solution

It Is Used To Authenticate The Data. In This, User Upload Data Blocks And Mac To Cs Provide Its Secret Key Sk To Tpa. The Tpa Will Randomly Retrieve Data Blocks & Mac Uses Secret Key To Check Correctness Of Stored Data On The Cloud. Problems With This System Are Listed Below As • It Introduces Additional Online Burden To Users Due To Limited Use (I.E. Bounded Usage) And Stateful Verification. • Communication & Computation Complexity • Tpa Requires Knowledge Of Data Blocks For Verification • Limitation On Data Files To Be Audited As Secret Keys Are Fixed • After Usages Of All Possible Secret Keys, The User Has To Download All The Data To Recomputed Mac & Republish It On Cs. • Tpa Should Maintain & Update States For Tpa Which Is Very Difficult • It Supports Only For Static Data Not For Dynamic Data.

B. Hla Based Solution

It Supports Efficient Public Auditing Without Retrieving Data Block. It Is Aggregated And Required Constant Bandwidth. It Is Possible To Compute An Aggregate Hla Which Authenticates A Linear Combination Of The Individual Data Blocks.

C. Privacy Preserving Public Auditing Proposed By Cong Wang

Public Auditing Allows Tpa Along With User To Check The Integrity Of The Outsourced Data Stored On A Cloud & Privacy Preserving Allows Tpa To Do Auditing Without Requesting For Local Copy Of The Data. Through This Scheme [1], Tpa Can Audit The Data And Cloud Data Privacy Is Maintained. It Contains 4 Algorithms As

1) Keygen: It Is A Key Generation Algorithm Used By The User To Setup The Scheme.
2) Singen: It Is Used By The User To Generate Verification Metadata Which May Include Digital Signature.
3) Genproof: It Is Used By Cs To Generate A Proof Of Data Storage Correctness.
4) Verifyproof: Used By Tpa To Audit The Proofs It Is Divided Into Two Parts As Setup Phase And Audit Phase.

A) Setup Phase: Public And Secret Parameters Are Initialized By Using Keygen And Data Files F Are Preprocesses By Using Singen To Generate Verification Metadata At Cs & Delete Its Local Copy. In Preprocessing User Can Alter Data Files F.

B) Audit Phase: Tpa Issues An Audit Message To Cs. The Cs Will Derive A Response Message By Executing Genproof. Tpa Verifies The Response Using F And Its Verification Metadata. Tpa Is Stateless I.E. No Need To

Maintain Or Update The State Information Of Audit Phase. Public Key Based Homomorphic Linear Authentication With Random Masking Technique Is Used To Achieve Privacy Preserving Public Auditing. Tpa Checks The Integrity Of The Outsourced Data Stored On A Cloud Without Accessing Actual Contents. Existing Research Work Of Proof Of Retrievability (Por) [20] Or Proofs Of Data Possession (Pdp) Technique Doesn't Consider Data Privacy Problem. Pdp Scheme First Proposed By Ateniese Et Al. Used To Detect Large Amount Corruption In Outsourced Data. It Uses Rsa Based Homomorphic Authentication For Auditing The Cloud Data And Randomly Sampling A Few Blocks Of Files. A Second Technique Proposed By Juels As Proofs Of Retrievability (Por) Allows User To Retrieve Files Without Any Data Loss Or Corruptions. It Uses Spot Checking & Error Correcting Codes Are Used To Ensure Both "Possession" And "Retrievability". To Achieve Zero Knowledge Privacy, Researcher [3] Proposed Aggregatable Signature Based Broadcast (Asbb). It Provides Completeness, Privacy And Soundness. It Uses 3 Algorithms As Keygen, Gentag And Audit.

*D. **Using Virtual Machine***

Abhishek Mohta Proposed Virtual Machines Which Uses Rsa Algorithm, For Client Data/File Encryption And Decryptions [5]. It Also Uses Sha 512 Algorithm Which Makes Message Digest And Check The Data Integrity. The Digital Signature Is Used As An Identity Measure For Client Or Data Owner. It Solves The Problem Of Integrity, Unauthorized Access, Privacy And Consistency.

*E. **Non Linear Authentication***

D. Shrinivas Suggested Homomorphic Non Linear Authenticator With Random Masking Techniques To Achieve Cloud Security [7]. K. Gonvinda Proposed Digital Signature Method To Protect The Privacy And Integrity Of Data [8]. It Uses Rsa Algorithm For Encryption And Decryption Which Follows The Process Of Digital Signatures For Message Authentication.

*F. **Using Eap***

S. Marium Proposed Use Of Extensible Authentication Protocol (Eap) Through Three Ways Hand Shake With Rsa. They Proposed Identity Based Signature For Hierarchical Architecture. They Provide An Authentication Protocol For Cloud Computing (Apcc) [9]. Apcc Is More Lightweight And Efficient As Compared To Ssl Authentication Protocol. In This, Challenge –Handshake Authentication Protocol (Chap) Is Used For Authentication. When Make Request For Any Data Or Any Service On The Cloud. The Service Provider Authenticator (Spa) Sends The First Request For Client Identity. The Steps Are As Follows

A) When Client Request For Any Service To Cloud Service Provider, Spa Send A Chap Request / Challenge To The Client.

B) The Client Sends Chap Response/ Challenges Which Is Calculated By Using A Hash Function To Spa

C) Spa Checks The Challenge Value With Its Own Calculated Value. If They Are Matched Then Spa Sends Chap Success Message To The Client.

Implementation Of This Eap-Chap In Cloud Computing Provides Authentication Of The Client. It Provides Security Against Spoofing Identity Theft, Data Tempering Threat And Dos Attack. The Data Is Being Transferred Between Client And Cloud Providers. To Provide Security, Asymmetric Key Encryption (Rsa) Algorithm Is Used. Dhiyanesh Proposed Mac Based And Signature Based Schemes For Realizing Data Audit Ability And During Auditing Phase Data Owner Provides A Secret Key To Cloud Server And Ask For A Mac Key For Verification [11]. Wang Proposed An Effective And Flexible Distributed Schemes As Homomorphic Token With Distributed Verification Of Erasure Coded Data Proposed Scheme Achieves An Integration Of Storage Correctness Insurance And Data Error Localization I.E. Identification Of Misbehaving Server [12].

*G. **Using Automatic Protocol Blocker***

Balkrishna Proposed Efficient Reed Solomon Technique For Error Correction Which Check Data Storage Correctness [13]. Kiran Kumarproposed Automatic Protocol Blocker To Avoid Unauthorized Access [14]. When An Unauthorized User Access User Data, A Small Application Runs Which Monitors User Inputs, It Matches The User Inpu T, If It Is Matched Then It Allow User To Access The Data Otherwise It Will Block Protocol Automatically. It Contains Five Algorithms As Keygen, Singen, Genproof, Verifyproof, Protocol Verifier. Protocol Verifier Is Used By Cs. It Contains Three Phases As Setup, Audit And Pblock.

*H. **Random Masking Technique***

Jachak K. B. Proposed Privacy Preserving Third Party Auditing Without Data Encryption. It Uses A Linear Combination Of Sampled Block In The Server's Response Is Masked With Randomly Generated By A Pseudo Random Function (Prf) [16]. Researchers Of [17] Use The Concept Of Virtual Machines, The Rsa Algorithm Is Used To Encode And Decode The Data And Sha 512 Algorithm Is Used For Message Digest Which Check The Integrity Of Information.

Dr. P.K. Deshmukh Uses The New Password At Each Instance Which Will Be Transferred To The Mail Server For Each Request To Obtain Data Security And Data Integrity Of Cloud Computing [17]. This Protocol Is Secure Against An Untrusted Server As Well As Third Party Auditor. Client As Well As Trusted Third Party Verifier Should Be Able To Detect The Changes Done By The Third Party Auditor. The Client Data Should Be Kept Private Against Third Party Verifier. It Supports Public Verifiability Without Help Of A Third Party Auditor. This Protocol Does Not Leak Any Information To The Third Party Verifier To Obtain Data Security. This Proposed Protocol Is Secure Against The Untrusted Server And Private Against Third Party Verifier And Support Data Dynamics. In This System, The Password Is Generated And That Will Be Transferred To Email Address Of The Client. Every Time A Key Is Used To Perform Various Operations Such As Insert, Update Delete On Cloud Data. It Uses Time Based Uuid Algorithm For Key Generation Based On Pseudo Random Numbers. If An Intruder Tries To Access The Users' Data On A Cloud, That Ip Address Will Be Caught And Transferred To The User So That User Will Be Aware Of.

III. Conclusions

A Handful Of Data Integrity Schemes Have Been Studied In This Article. It Has Been Analyzed That The Data Integrity Schemes Have Been Enhanced With More And More Research. The Designers Of Data Integrity And Information Security Were Devoted To Take Many Measures To Protect Private Data And Systems In Early Days. The Traditional Security Model Tends To Strength The Protection Layer Of The Protected Resource. Designers Believe That Strengthening The Protection Layer Is Enough Without Caring About The Integrity Of The Protected Data. However, With The Development Of Network Technology, Network Security Tasks Extend From Protection Of Confidential Data To Protection Of Information Systems Which Provide Network Services To Institution Employees, Customers And Partners. In This Study, It Has Been Observed That Many Optimizations Are Possible On The Data Integrity Methods To Reduce The Computation Cost And Communication Cost. It Also Has Been Find Out That Large Message Digest Code Are More Secure.

References

[1] E. Bertino And R. S. Sandhu. Database Security-Concepts, Approaches, And Challenges. Ieee Trans. Dependable Sec. Comput., 2(1):2-19, 2005.

[2] D. D. Clark And D. R. Wilson. A Comparison Of Commercial And Military Computer Security Policies. In Ieee Symposium On Security And Privacy, Pages 184-195, 1987.

[3] K. Biba. Integrity Considerations For Secure Computer Systems. Technical Report Tr-3153, Mitre, 1977.

[4] "The Data Integrity Problem And Multi-Layered Document Integrity": By Ben Moss, Ph.D., University Of Nottigham, 2007, 141 Pages.

[5] Rivest, R., The Md5 Message Digest Algorithm, Rfc 1321, Mit Lcs And Rsa Data Security, Inc., April 1992

[6] Sha-1 Standard, National Institute Of Standards And Technology (Nist),"Secure Hash Standards, " Fipspub180-1www.Itl.Nist.Gov/Fipspub/Fips180-1.Html 2003s.

[7] Mihir Bellare, Ran Canettiy, Hugo Krawczykz: "Keying Hash Functions For Message Authentication", Advances In Cryptology - Crypto 96 Proceedings, Lecture Notes In Computer Science Vol. 1109, N. Koblitz Ed., Springer-Verlag, 1996.

[8] A. Juels And B.S. Kaliski, Jr., "Pors: Proofs Of Retrievability For Large Files," In Ccs‟07: Proceedings Of The 14th Acm Conference On Computer And Communications Security.

[9] H. Shacham And B. Waters, "Compact Proofs Of Retrievability," In Proceedings Of Asiacrypt ‟08, Dec. 2008.

[10] K. D. Bowers, A. Juels, And A. Oprea, "Proofs Of Retrievability: Theory And Implementation," Cryptology Eprint Archive, Report 2008/175, 2008.

[11] K. D. Bowers, A. Juels, And A. Oprea, "Hail: A High-Availability And Integrity Layer For Cloud Storage," Cryptology Eprintarchive, Report 2008/489, 2008.

[12] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson,And D. Song, "Provable Data Possession At Untrusted Stores,"In Proceedings.Of Ccs ‟07, Pp. 598–609, 2007

[13] G. Ateniese, R. D. Pietro, L. V. Mancini, And G. Tsudik, "Scalable And Efficient Provable Data Possession," In Proceedings Of Securecomm '08, Pp. 1–10, 2008.

[14] R. Curtmola, O. Khan, R. Burns, And G. Ateniese, "Mr-Pdp: Multiple-Replica Provable Data Possession," In Proceedings Of Icdcs '08, Pp.411–420, 2008.

[15] L.Thulasimani, M.Madheswaran: "Design And Performance Analysis Of Unified Reconfigurable Data Integrity Unit For Mobile Terminals", International Journal Of Computer Science And Information Security, Vol. 7, No. 2, 2010.

[16] Danyang Cao, Bingru Yang: "Design And Implementation For Md5-Based Data Integrity Checking System", Ieee 2010.

Pramod Kumar"A Review On Data Integrity Models And Schemes"International Journal of Engineering Science Invention (IJESI), vol. 07, no. 03, 2018, pp23-27