Prevention of Attacks on Big Data Records by Multiple Security Strategies

Aiswarya S, Hindu Priyadharshini M
(Computer Science And Engineering, St. Joseph's Institute Of Technology, Chennai, India)
(Computer Science And Engineering, St. Joseph's Institute Of Technology, Chennai, India)
Corresponding auther: Aiswarya S

Abstract : *This Project Formulates The Several Types Of Big Data Relational Database Securities As A Constrained Efficient Techniques To Solve The Security Problems. While Transferring Data From One Server To Another There Are Many Possibilities Of Attacking The Data By Intruders. This Proposed System Will Provide Efficient Data To The Receiver Without Any Intruders Stealing The Data. This System Address The Novel Problems Of Securely Sending Provenance For Data Security Using Range Partitioning, J-Bit Encoding, Des Algorithm And Secure Data Hiding Algorithm (Sdha).In Range Partitioning, It Divides The Table Records And Assigns Partition Number To It. In J-Bit Encoding Each Bit Was Encoded. That Made An Original Dataset To Encoded Data. It Works By Manipulate Bits Of Data To Reduce The Size And Optimize Input For Other Algorithm. Then Des Encryption Was Implemented. It Is A Symmetric-Key Algorithm For The Encryption Of Electronic Data. Finally The Sdha Was Implemented To Secure The Original Data. The Text Can Be Known As Cover Text Which Embedded With Original Data To Prevent Alterations To Original Data. These Security Features Can Provide An Efficient Way Of Providing Security For Of Big Data Dataset.*

Keywords *-Big Data, Encryption, J-Bit Encoding, Intruders, Partition.*

Date of Submission: 05-03-2018 Date of acceptance: 20-04-2018

I. INTRODUCTION

This Project Formulates The Several Types Of Big Data Relational Database Securities As Constrained Efficient Techniques To Solve The Security Problems. While Transferring Data From One Server To Another There Are Many Possibilities Of Attacking The Data By Intruders. The Main Contributions Of The Paper Are Securely Sending Provenance For Data Security Using J-Bit Encoding, Des Algorithm And Secure Data Hiding Algorithm (Sdha).The Purpose Of This Project Is To Transfer The Important Database Records To Server To Server With Multiple Security Strategies For Streaming Data On Big Data. This Has Been Implemented Useful For Security Implementations On The Streaming Data In Distributed Networks With Security Strategies.

II. PROPOSED AND ITS ADVANTAGES

The Purpose Of This Project Is To Transfer The Important Database Records To Server To Server (One Server To Another) With Multiple Security Strategies For Streaming Data On Big Data. This Has Been Implemented Useful For Security Implementations On The Streaming Data In Distributed Networks With Security Strategies.

2.1 Proposed System

The Proposed System Addresses The Novel Problem Of Securely Transmitting Provenance For Data's Using J-Bit Encoding, Des Algorithm And Sdha. Ms Sql Framework Was Used. J-Bit Encoding Was Used For Encoding Process. Data Set Will Make Partition And Grouping For Encoding. We Propose A Data Hiding-Based Solution To Overcome The Inter Packet Delays. Des Was Used For Encryption For Encryption And Decryption. Here The Embedding Is Hidden That The Presence Of Data Hiding Is Invisible To The User. The Alterations To Original Data Can Be Prevented By Using Sdha.

2.2 ADVANTAGES

J-Bit Encoding And Decoding Process Are More Confidential.Des Algorithm Is Used For Encryption And Decryption Of Data. Secure Data Hiding Algorithm (Sdha) Is Used To Cover The Data Into Another Data So That The Intruder Cannot Identify The Hidden Data. Time Invariant. Process Large Dataset.

III. System Architecture

A System Architecture Or Systems Architecture Is The Conceptual Model That Defines The Structure, Behavior, And More Views Of A System. An Architecture Description Is A Formal Description And Representation Of A System, Organized In A Way That Supports Reasoning About The Structures And Behaviors Of The System. A System Architecture Can Comprise System Components, The Expand Systems Developed, That Will Work Together To Implement The Overall System. There Have Been Efforts To Formalize Languages To Describe System Architecture, Collectively These Are Called Architecture Description Languages. System Architecture Is Depicted In The Following Fig.1

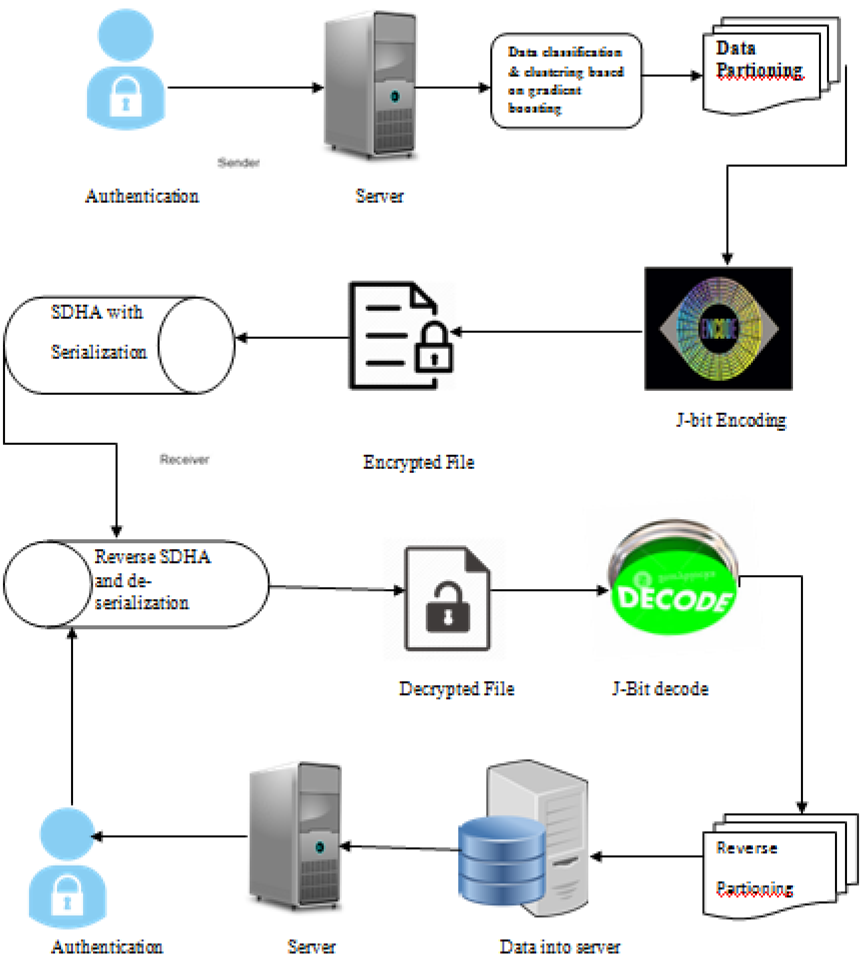

Figure.1 System Architecture

The System Architecture Explains About The Working Of Data Transfer From Sender To Receiver. This Transfer Process Involves Four Techniques Such As Data Partitioning-Bit Encoding, Data Encryption Standard And Secure Data Hiding Algorithm.

These Partitions Are Assigned Index By Hash Function. Then The Data Is Encoded Using J-Bit Encoding And Encrypted. It Is Then Serialized And Converted To Object File .After That The Data Is De-Serialized And Decrypted. The Decrypted Data Is Then Decoded And The Reverse Partitioning Is Done. The Resulted Data Is Directly Attached To The Receiver's Server. Finally The Receiver Authenticates The Server And Gets The Data. The Decrypted Data Is Then Decoded And The Reverse Partitioning Is Done. The Resulted Data Is Directly Attached To The Receiver's Server. Finally The Receiver Authenticates The Server And Gets The Data. The Sender Authenticates To The Server Using User Validation. Then He Or She Retrieves Data From The Server. Then They Are Sent To The Receiver. To The Data To Safe And Secure Following Process Taken Place. The Data Is Partitioned Using Data Partition. Data Partition Is Process Of: A Partition Is A Division Of A Logical Database Or Its Constituent Elements Into Distinct Independent Parts. Database

Partitioning Is Normally Done For Manageability, Performance Or Availability Reasons, Or For Load Balancing.

After The Data Is Been Partitioned It Is Sent To The Next Module Which Is J-Bit Encoding. In J-Bit Encoding Each Bit Is Being Encoded And Then Sent For Encryption Of Data. Then The Encrypted File Is Generated. This File Is Used For Serialization By Secure Data Hiding Algorithm. Here The Data Is Hidden Inside File Called Cover Text. The Original Text Is Encapsulated Inside The Cover Text So That For The Intruder Who Has Seen From Outside Thinks That It's A Different File Such As Audio And Video File Etc. But Actually The Original Text Is Embedded Inside The Cover Text. This Prevents Attacks From Attackers So That The File Safely Reaches The Receiver. At Last The Process Gets Reversed By Deroute Of Sdha, Des, J-Bit Decoding And Reverse Partitioning. Then The File Directly Gets Attached To The Server Of The Receiver. This Kind Of Data Transferring From One System To Another Make The Data Even Safer.

IV. System Implementation

In System Implementation, Defining How The Information System Should Be Built (I.E., Physical System Design), Ensuring That The Information System Is Operational And Used, Ensuring That The Information System Meets Quality Standard And Their Process Is Discussed Below.

Range Partitioning, J-Bit Encoding, Data Encryption Standard, Secure Data Hiding Algorithm (Serialization)

4.1 Partitioning

Partitioning Addresses Key Issues In Supporting Very Large Tables And Indexes By Decomposing Them Into Smaller And More Manageable Pieces Called Partitions. Sql Queries And Dml Statements Do Not Need To Be Modified In Order To Access The Partitioned Tables. However, After The Partitioned Are Defined Ddl Statements Can Access And Manipulate Individual Partitions Rather Than Entire Table Or Index.

Partitioning Improves Query Performance. In Many Cases The Results Of A Query Can Be Achieved By Accessing A Subset Of Partitions, Rather The Than The Entire Table. Tables Can Be Partitioned Into Up To 1024k-1 Separate Partition. In The Proposed System, Data Gets Partitioned By Range Partitioning By Assigning A Range Of Desired Rows To The Table. By Partitioning The Data Performance Gets Increased. Each Row In A Partitioned Table Is Unambiguously Assigned To A Single Partition. The Partitioned Key Is A Set Of One Or More Columns That Determines The Partition For Each Row As Shown In The Fig 2.

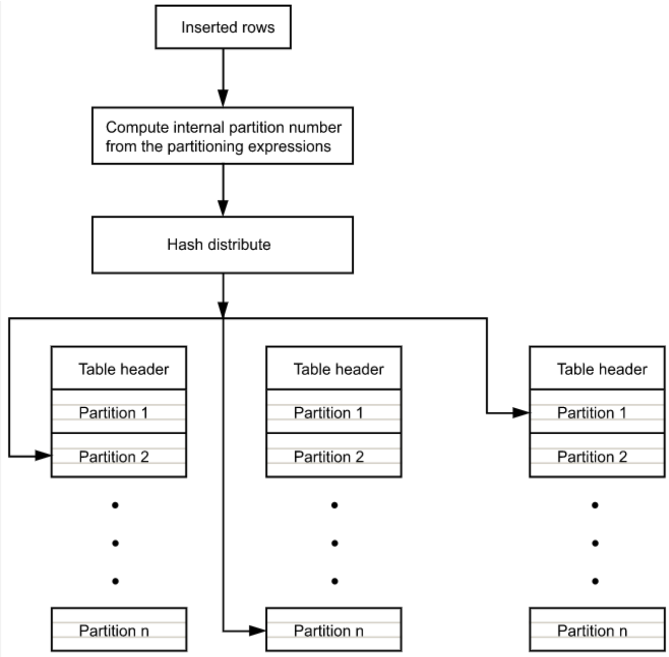

Figure.2 Partitioning

This Class Eventually Divides The Table Records And Assigns Partition Number To It. Range Partitioning Is Being Used Here To Partition The Datasets.

4.2 J-Bit Encoding

J-Bit Encoding Is An Encoding Process Where Each Single Bit Gets Manipulated And Encoded. This Algorithm Will Manipulates Each Bit Of Data Inside File To Minimize The Size Without Losing Any Data After Decoding Which Is Classified To Lossless Compression.

4.3 Data Encryption Standard

The Data Encryption Standard Is A Symmetric-Key Algorithm For The Encryption Of Electronic Data. Although Now Considered Insecure, It Was Highly Influential In The Advancement Of Modern Cryptography.Totally 16 Rounds Takes Place In 64-Bit Block Length Of 56-Bit Key Length Which Makes The Data Highly Secure As Shown In The Fig.3.

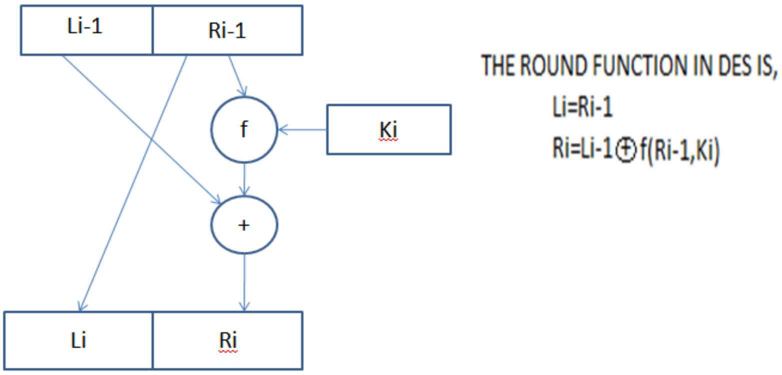

Figure.3 Encryption

This Class Gets All The Encoded Records And Encrypts Them As A Whole File Along The Secret Key. Des Encryption Is Being Used To Securely Encrypt The Data Sets.

4.3 Secure Data Hiding Algorithm

Secure Data Hiding Algorithm Can Hide Any Secret Message In Any Standard Cover Media Such As Text, Image, Audio, Video Files. Here We Used This Algorithm For Hiding The Encrypted Text. Encrypted Text Would Be Covered With A Secret Key. Serialization Is A Process Of Saving An Object's State To A Sequence Of Bytes As Shown In The Fig 4.

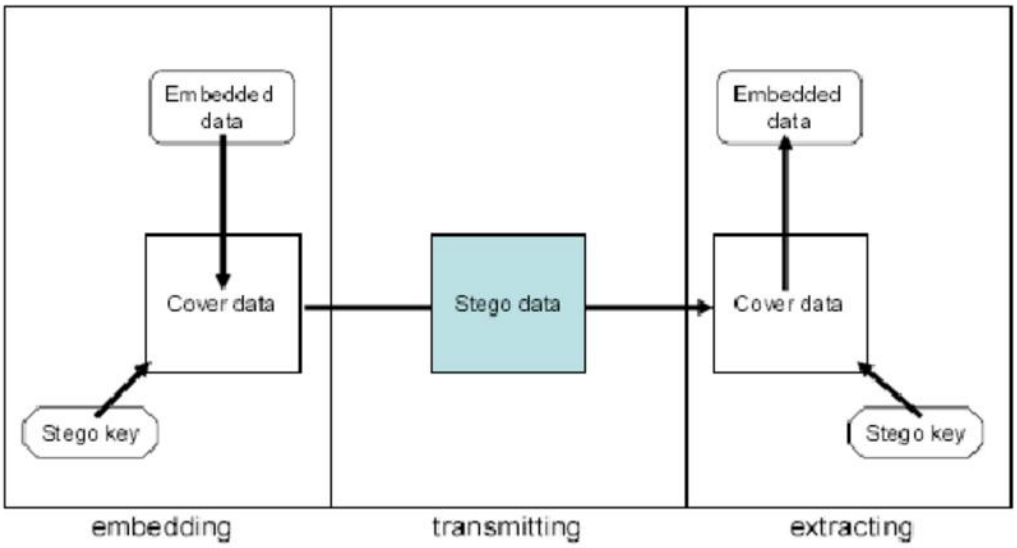

Figure.4 Sdha

V. Conclusion

The Proof Of Concept Implementation Of Our Sdha Technique Was Used To Conduct Experiments Using Both Synthetic And Real-World Data. A Comparison Our Sdha Technique With Previously Posed Techniques Shows The Superiority.

- The Final Result Is To Transmit The Large Data From Server (Source) To Server (Destination) Successfully.
- Secure Data Streaming Transmission Is Done.
- Loss Of Data Can Be Reduced.
- Speed Of Transmission Of Big Data Stream Records Is Increased.
- The Multiple Securities Provided For Security And Prevent The Attacks From The Attackers

One Server Can Act As A Multiple Clients. Transformation Time For Frames Can Be Reduced. Even If Power Fails, There Is No Data Loss And Stored In Data Base. The Arms System Architecture With A Focus On The Extensions To The Isma Security Standard To Enable Adaptive Streaming Of Encrypted Mpeg-4 Content. Although We Have Addressed Many Challenges In Building This System, There Are Many More Problems Yet To Be Solved. We Are Investigating Various Optimizations In The Coding And Streaming To Improve The Bandwidth Utilization While Minimizing The Distortion Experienced By The Clients In Wired And Wireless Networks

REFERENCES

[1] D. Han, C. G. Giraud-Carrier, And S. Li, "Efficient Mining Of High-Speed Uncertain Data Streams," Appl. Intell., Vol. 43, No. 4, Pp. 773–785, 2015.

[2] H. Karau, A. Konwinski, P. Wendell, And M. Zaharia, Learning Spark:Lightning-Fast Big Data Analytics. Sebastopol, Ca, Usa: O'reilly Media, 2015.

[3] W.-P. Ding, C.-T.Lin, M. Prasad, S.-B.Chen, And Z.-J. Guan, "Attribute Equilibrium Dominance Reduction Accelerator (Dccaedr) Based On Dis-Tributedcoevolutionary Cloud And Its Application In Medical Records," Ieee Trans. Syst., Man, Cybern., Syst., Vol. 46, No. 3, Pp. 384–400,Mar. 2016.

[4] Y. Xun, J. Zhang, And X. Qin, "Fidoop: Parallel Mining Of Frequent Itemsets Using Mapreduce," Ieee Trans. Syst., Man, Cybern., Syst., Vol. 46, No. 3, Pp. 313–325, Mar. 2016.

[5] X. Meng Et Al., "Mllib: Machine Learning In Apache Spark," J. Mach.Learn. Res., Vol. 17, No. 1, Pp. 1235–1241, 2016.

Aiswarya S"Prevention of Attacks on Big Data Records by Multiple Security Strategies""International Journal of Engineering Science Invention (IJESI), vol. 07, no. 04, 2018, pp 12-16