IJARES/May 2014/Volume-2/Issue-5/1071-1076 **ISSN 2347- 9337**

**INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN ENGINEERING AND SCIENCE**

# IMPLEMENTATION OF SECURE QUERIES BY DATABASE PARADIGM

**Dr.M.V.Siva Prasad[1], P.Sandeep Reddy[2], S.Gangadhar[3]**

[1]Professor, Dept of CSE, Anurag Engineering College, Kodad, A.P, India

[2]Assistant Professor, Dept of CSE, Anurag Engineering College, Kodad, A.P, India

[3]M.Tech Student, Dept of CSE, Anurag Engineering College, Kodad, A.P, India

**ABSTRACT:**

Conventional additive homomorphisms have been utilized in existing work, to permit servers to run aggregation queries above encrypted information which permits the working out of encryption of totting up encrypted values devoid of necessitate their decryption within the course. Query processing engines are operated on the server and in secure coprocessors. Each and every optimization probable in a conventional database system with no confidential attributes are still appropriate to unrestricted sub-queries carried out on the server. The query is clearly encrypted at user position by means of public key of secure coprocessors.

***Keywords: Secure coprocessors, Attribute, Query processing engines, Decryption, Public key.***

## 1. INTRODUCTION:

Encryption of data is simply one of the links in a succession of conviction that make certain the protection of Trusted DB. The additional feature of encryption granularity and custom cipher designing are considered. Designs of Tamper resistant are considerably constrained in computational aptitude and memory capability which makes executing completely featured database explanation using secure coprocessors extremely demanding [4]. Trusted DB accomplish by making use of general unsecured server possessions to greatest extent feasible. Regardless of outgoings and performance limits of confidential hardware, the expenses of

running confidential DB are orders of extent inferior to any possible upcoming cryptography-only method. Additionally it does not edge query perspicuity [13]. A full-fledged, confidentiality enabling protected database leveraging server-side confidential hardware can be put up and run at a portion of the outlay of any cryptography-enabled confidential data processing on general server hardware [8]. When privacy becomes an apprehension, information needs to be encrypted previous to outsourcing. Once encrypted, explanation can be envisioned that: uncomplicatedly transport data back towards the user where it can be decrypted and queried, organize cryptographic build server side to procedure encrypted information, and procedure encrypted information server-side within tamper-proof area of confidential hardware [1]. Conventional additive homeomorphisms have been utilized in existing work, to permit servers to run aggregation queries above encrypted information. These permits the working out of encryption of totting up encrypted values devoid of necessitate their decryption within the course. Existing homomorphism does necessitate the corresponding effort of no less than a modular increase in performing their matching procedure [11]. For safety, this modular increase desires to be performing in field by a great modulus. For effectiveness goes one step additional and proposes to carry out aggregation in parallel by concurrently adding together multiple2-bit integer value. The expansion of confidential data base to make use of numerous secure coprocessors is uncomplicated by means of Physical installation of extra secure coprocessors all along with confidential data base codebase [3]. A probable utilize of a secure coprocessors is to carry out aggregation completely within it. The consequence can subsequently be re-encrypted and broadcast reverse to user.

## 2. METHODOLOGY:

Query processing engines are operated on the server and in secure coprocessors. Aspect within the database is classified as being moreover public or else private. Concealed attributes are encrypted and can be decrypted by user or else by secure coprocessors [14]. In outsourced surroundings it is frequently needed that numerous clients access the database concurrently. We make a note of a solitary Secure coprocessors is not enough to hold the workload in such a situation. The

expansion of confidential DB to make use of numerous secure coprocessors is uncomplicated by means of Physical installation of extra Secure coprocessors all along with confidential DB codebase, as shown in fig1 introduce the database scheme and encryption keys steadily in to the novel Secure coprocessors from an existing or user [9]. In multi-client circumstances it could be needed to contain numerous distinct client-Secure coprocessors keys in support of moreover access control or augmented safety or additional clients are negotiated. The conservatory to hold such a situation is also straightforward. The information accumulated on host server disk is encrypted by means of a particular master encryption key recognized only to secure coprocessors because all update or insert process are carried out by secure coprocessors the master key is amass within secure coprocessors and is certainly not conversed to the exterior [7]. Because the complete database reside exterior the secure coprocessors, its dimension is not bound by secure coprocessors memory limits. Pages that require being access by secure coprocessors-side query handing out are bringing in on demand by paging component [2]. Query implementation necessitates a set of phase. In the initial phase a user defines a database scheme and incompletely inhabits it. Susceptible element is noticeable by means of SENSITIVE keyword which the client layer clearly practices by encrypting matching aspect [6]. User sends an uncertainty appeal towards host server all the way through a criterion SQL boundary. The uncertainty is clearly encrypted at user position by means of public key of secure coprocessors [16]. The host server consequently cannot decrypt uncertainty and forward the encrypted uncertainty to the request manager within the secure coprocessors. Each and every optimization probable in a conventional database system with no confidential attributes are still appropriate to unrestricted sub-queries carried out on the server [12]. Authentic expenses are orders of extent lower than any explanation on basis of software-only cryptography on hardware of legacy server. Request manager decrypts the uncertainty and forward it towards the uncertainty Parser produce a set of plans which are build by rewrite innovative client uncertainty into sub-queries, and, consistent with their objective information set categorization, every sub-query within plan is recognized as being moreover public or private [5]. The

implementation times of private query comprise the time necessary for process of encryption and decryption inside secure coprocessors. Uncertainty Optimizer subsequently assess the implementation expenses of every plan and choose the most excellent plan in support of implementation forward it towards the dispatcher forwards public uncertainty towards the host server and concealed queries towards secure coprocessors engine though managing dependency [15]. The net consequence is that the utmost probable exertion is operated on host server's inexpensive cycles. The concluding uncertainty consequence is accumulated, digitally signed through secure coprocessors Query correspondent, and dispatch to user. At a elevated level uncertainty optimization within a database scheme works as Query Plan maker construct probably manifold plans in support of user query; in support of every constructed plan the Query Cost assessor compute an estimation of implementation expenditure of plan; superlative plan specifically one with slightest outlay, is subsequently particular and approved on towards the Query Plan Interpretor in support of implementation [10]. The query optimization procedure within confidential DB efforts by key differentiation in estimating Query Cost appropriate to separation of information.

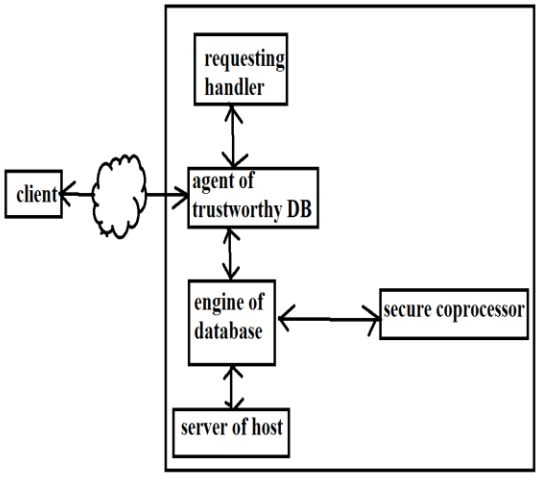


Fig1: An overview of confidential DB construction

## 3. RESULTS:

The implementation times of private query comprise the time necessary for process of encryption and decryption inside secure coprocessors. The public query implemented on host server moreover comprise the processing period to line the confidential DB stack with server database engine moreover output the concluding effect. Each and every optimization probable in a conventional database system with no confidential attributes are still appropriate to unrestricted sub-queries carried out on the server. When evaluated with totally unsecured baseline situation, safety does not appear inexpensive

with implementation times being superior and advantage from confidential DB's leveraging of unfaithful server's CPU in support of non-sensitive query segment. Authentic expenses are orders of extent lower than any explanation on basis of software-only cryptography on hardware of legacy server.

## 4. CONCLUSION:

Designs of Tamper resistant are considerably constrained in computational aptitude and memory capability which makes executing completely featured database explanation using secure coprocessors extremely demanding. A full-fledged, confidentiality enabling protected database leveraging server-side confidential hardware can be put up and run at a portion of the outlay of any cryptography-enabled confidential data processing on general server hardware. Existing homomorphism does necessitate the corresponding effort of no less than a modular increase in performing their matching procedure. The public query implemented on host server moreover comprise the processing period to line the confidential DB stack with server database engine moreover output the concluding effect. Uncertainty Optimizer subsequently assess the implementation expenses of every plan and choose the most excellent plan in support of implementation forward it towards the dispatcher. In multi-client circumstances it could be needed to contain numerous distinct client- Secure coprocessors keys in support of moreover access control or augmented safety or additional clients are negotiated.

## REFERENCES:

[1] Shahram Ghandeharizadeh and David J. DeWitt. Hybrid-RangePartitioning Strategy: A New Declustering Strategy for MultiprocessorDatabase Machines. In Proceedings of VLDB, pages 481 –492. Morgan Kaufmann Publishers Inc., 1990.

[2] Valentina Ciriani, Sabrina De Capitani Di Vimercati, Sara Foresti,Sushil Jajodia, Stefano Paraboschi, and Pierangela Samarati. Combining fragmentation and encryption to protect privacy in datastorage. ACM Trans. Inf. Syst. Secur., 13(3):22:1–22:33, July 2010.

[3] Murat Kantarcioglu and Chris Clifton. Security issues in queryingencrypted data. In Sushil Jajodia and Duminda Wijesekera,editors, DBSec, volume 3654 of Lecture Notes in Computer Science,pages 325–337. Springer, 2005.

[4] Gagan Aggarwal, Mayank Bawa, Prasanna Ganesan, HectorGarcia-Molina, Krishnaram Kenthapadi, Rajeev Motwani,Utkarsh Srivastava, Dilys Thomas, and Ying Xu 0002. Twocan keep a

secret: A distributed architecture for secure databaseservices. In CIDR, pages 186–199, 2005

[5] Rakesh Agrawal, Dmitri Asonov, Murat Kantarcioglu, Yaping Li.Sovereign Joins. In Proceedings of the 22nd International Conference on Data Engineering, page 26. IEEE Computer Society, 2006.

[6] Shiyuan Wang, Divyakant Agrawal, and Amr El Abbadi. A comprehensiveframework for secure query processing on relationaldata in the cloud. In Secure Data Management, pages 52–69, 2011

[7] Einar Mykletun and Gene Tsudik. Incorporating a secure coprocessorin the database-as-a-service model. In Proceedings of IWIA,pages 38–44, Washington, DC, USA, 2005. IEEE Computer Society

[8] Bishwaranjan Bhattacharjee, Naoki Abe, Kenneth Goldman,Bianca Zadrozny, Chid Apte, Vamsavardhana R. Chillakuru andMarysabel del Carpio. Using secure coprocessors for privacy preserving collaborative data mining and analysis. In Proceedingsof DaMoN, 2006

[9] Sai Wu and Feng Li and Sharad Mehrotra and Beng Chin Ooi.Query optimization for massively parallel data processing. InProceedings of CCS , page Article 12. ACM, 2011.

[10] Rosario Gennaro, Craig Gentry, and Bryan Parno. Non-interactiveverifiable computing: Outsourcing computation to untrustedworkers. In Tal Rabin, editor, CRYPTO, volume 6223 of LectureNotes in Computer Science, pages 465–482. Springer, 2010.

[11] Marten van Dijk, Craig Gentry, Shai Halevi, and Vinod Vaikuntanathan.Fully homomorphic encryption over the integers. InHenri Gilbert, editor, EUROCRYPT, volume 6110 of Lecture Notesin Computer Science, pages 24–43. Springer, 2010.

[12] Mustafa Canim, Murat Kantarcioglu, Bijit Hore, and SharadMehrotra. Building disclosure risk aware query optimizers forrelational databases. Proc. VLDB Endow., 3(1-2):13–24, September 2010

[13] Hakan Hacigumus, Bala Iyer, Chen Li and Sharad Mehrotra.Executing SQL over Encrypted Data in the Database-Service-Provider Model. In Proceedings of SIGMOD, pages 216–227, 2002

[14] Sanjay Agrawal and Vivek Narasayya and Beverly Yang. Integratingvertical and horizontal partitioning into automated physicaldatabase design. In Proceedings of SIGMOD, pages 359 – 370.ACM, 2004.

[15] Bala Iyer Hakan Hacigumus and Sharad Mehrotra. Efficient executionof aggregation queries over encrypted relational databases.In Database Systems for Advanced Applications, volume 2973, pages633–650, 2004.

[16] "TrustedDB: A Trusted Hardware basedDatabase with Privacy and Data Confidentiality", Sumeet Bajaj, Radu Sion, 2013.