International Journal of Advanced Information Science and Technology (IJAIST) *ISSN: 2319:2682*
Vol.5, No.9, September 2016 DOI:10.15693/ijaist/2016.v5i9.50-56

TRUSTED AND OPTIMIZED DATABASE FOR DATA CONFIDENTIALITY USING ENCRYPTED DATA CONTROLLER

Kammili Manasa
Final MTech,
Dept of Computer Science Engineering,
Sri Vasavi Engineering College
Pedatadepalli, Tadepalligudem,
Andhra Pradesh, India

Vedula Venkateswara Rao
Associate Professor,
Dept of Computer Science Engineering,
Sri Vasavi Engineering College
Pedatadepalli, Tadepalligudem,
Andhra Pradesh, India

***Abstract*— in today's database environment outsourcing is the major issue in sharing the data by users. We have cloud environment data centers, were centralized database is accessed and shared by multiple users. In this environment privacy and confidentiality are two main concerns. Traditionally these two concerns are implemented by encrypting data before outsourcing to a service provider through which multiple users are sharing the data. Traditionally software based cryptography systems were used for this, but for server side query processing on encrypted data there is a limitation as an improvement hardware based trusted database environment is designed that allows clients to execute SQL queries with privacy and confidentiality. The use of hardware for trusted database environment is cost overhead and results performance limitations.**

Now it is proposed a simulator which is a software program that uses the same processors to implement trustiness and database when sharing the data by users. This software simulative called a data controller located in server and keeps privacy, confidentiality and trust database when users are executing queries from clients .Our data controller not only keeps the database as a trusted but also optimized .The process of verifying trustiness , executing the queries on database .The data controller responsible for reducing cryptography cost and query cost. The data controller is designed with for creating data controller which mimics the hardware processor and it uses too level relational algebra for optimizing the queries.

***Index terms* - cloud, privacy, Cryptography, encryption, decryption, authentication, confidentiality, Optimized Query Execution, Query Cost.**

I. INTRODUCTION

The overview of outsourcing and clouds are well known, significant challenges yet lie in the path of large-scale adoption since such services often require their customers to inherently trust the provider with full access to the outsourced data sets. numerous instances of illicit insider behaviour or data leaks have left clients reluctant to place sensitive data under the control of a remote, third-party provider, without practical assurances of privacy and confidentiality, especially in business, healthcare, and government frameworks. moreover, today's privacy guarantees for such services are at best declarative and subject customers to unreasonable fine-print clauses. it's allowing the server operator to use customer behaviour and content for commercial profiling or governmental surveillance purposes. tamper resistant designs, however, are significantly constrained in both computational ability and memory capacity which makes implementing fully featured database solutions using secure coprocessors (scpus) very challenging. despite the cost overhead and performance limitations of trusted hardware, we show that the costs per query are orders of magnitude lower than any (existing or) potential future software-only mechanisms. trusted is built and runs on actual hardware and its performance and costs are evaluated here. in most of these efforts, data are encrypted before outsourcing. Once encrypted however, inherent limitations in the types of primitive operations that can be performed on encrypted data lead to fundamental expressiveness and practicality constraints.

Data encryption is essential and a very important topic in modern day communication. It is very important to encrypt messages while sending them to a client from another client without being tracked or interpreted by a hacker. For example we can assume the situation where a bank manager is instructing his subordinates to credit an account, but in the mean while a hacker interpret the message and he uses the information to debit the account instead of crediting it. Again we can think of a situation, where a person wants to keep his passport information and other important documents safely secured with him all the time but he can not, may be because he is always exposed to outside intruders and threats. For this reason it is essential to use encryption to hide important data from the outside world and send it safely to the destination or keep it safe somewhere else. Encryption techniques are now a very important research field and, every now and then cryptography scientist are trying to come up with a good encryption technique (algorithm) so that no hacker / intruder

can interpret the encrypted message. The modern day cryptographic methods are of two types
(i) symmetric key cryptography, where the same key is used for encryption and for decryption purpose.
(ii) Public key cryptography, where we use one key for encryption and one key for decryption purpose. Symmetric key algorithms are well accepted in the modern communication network. The main advantage of symmetric key cryptography is that the key management is very simple. Only one key is used for both encryption as well as for decryption purpose. There are many methods of implementing symmetric key. In case of symmetric key method, the key should never be revealed / disclosed to the outside world other the user and should be kept secure. To deal with this problem we have introduced a new method of generating a code from the entered password, which will act as a key. In this present method the key generated from the password will act as first level of security of the encrypted message.

II. EXISTING SYSTEM AND RELATED WORK

Clients of outsourced databases need query authentication (qa) guaranteeing the integrity (correctness and Completeness), and authenticity of the query results returned by potentially compromised providers. Existing results provide Query Authentication assurances for a limited class of queries by deploying several software cryptographic constructs. Here, We show that, to achieve Query Authentication, however, it is significantly cheaper and more practical to deploy server hosted, Tamper-proof Software Controller which is low cost and software based solution. Further, this provides the ability to handle arbitrary queries. To reach this insight, we extensively survey existing Query Authentication work and identify interdependencies and Efficiency relationships. We then introduce correct data base, a new data base system with full Query Authentication assurances, leveraging server hosted, Tamper-proof, trusted hardware in close proximity to the outsourced data.

A. Distributed Architecture for Secure Database Services

Researchers have recently discovered several interesting, self-organized regularities from the World Wide Web, ranging from the structure and growth of the Web to the access patterns in Web surfing. What remains to be a great challenge in Web log mining is how to explain user behavior underlying observed Web usage regularities. In this paper, we will address the issue of how to characterize the strong regularities in Web surfing
in terms of user navigation strategies, and present an information foraging agent based approach to describing user behavior. By experimenting with the agent-based decision models of Web surfing, we aim to explain how some Web design factors as well as user cognitive factors may affect the overall behavioral patterns in Web usage. In order to further characterize user navigation regularities as well as to understand the effects of user interests, motivation, and content organization on the user behavior. An information foraging agent based model that takes into account the interest profiles, motivation aggregation, and content selection strategies of users and, thereafter, predicts the emerged regularities in user navigation behavior. In summary, our work offers a means for explaining strong Web regularities with respect to user Interest Profiles, Web Content Distribution and coupling, and user navigation strategies. It enables us to predict the effects on emergent usage regularities if certain aspects of Web servers or user foraging behaviors are changed. While presenting an interesting and promising research direction, it has been point out that one of the useful extensions for future work would be to show how the quantitative representations or constructs as used in modeling Web contents and user interest profiles. The planning Techniques help to bridge the gap between the searching necessities and the Content Adaptation. To Monitor and Adapt the learning object of each learning route against unexpected contingencies.

B. *Existing System*

Existing research addresses several such security aspects, including access privacy and searches on encrypted data. In most of these efforts data is encrypted before outsourcing. Once encrypted however, inherent limitations in the types of primitive operations that can be performed on encrypted data lead to fundamental expressiveness and practicality constraints. Recent theoretical cryptography results provide hope by proving the existence of universal homeomorphisms, i.e., encryption mechanisms that allow computation of arbitrary functions without decrypting the inputs. Unfortunately actual instances of such mechanisms seem to be decades away from being practical.

C. *Proposed System*

A full-fledged, privacy enabling secure database leveraging server-side trusted hardware can be built and run at a fraction of the cost of any (existing or future) cryptography-enabled private data processing on common server hardware. It has been designed and built TrustedDB, a SQL database processing engine that makes use of tamperproof cryptographic coprocessors proximity to the outsourced data

III. SYSTEM ARCHITECTURE

The following explains the system architecture for implementation

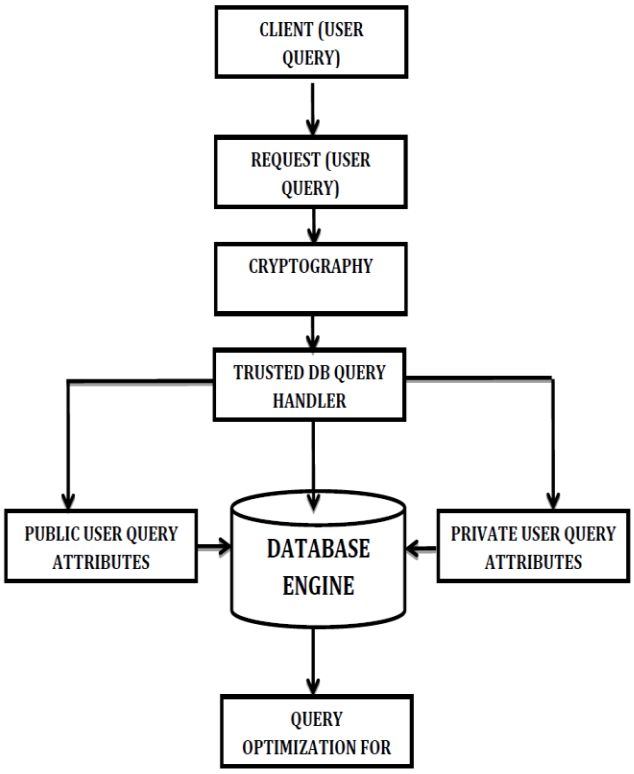

Figure 3.1 System Architecture

The system can be portioned into following modules

1) Data Base Module
2) Cloud Module
3) Authentication using Cryptography
4) Query Optimizer

The outsourced data stored in Data base located in Cloud Authentication module provides authentication of data base and provides trustiness on data base for users to execute queries

A QUERY PARSING AND EXECUTION

In the first stage a client defines a database schema and partially populates it. Sensitive attributes are marked using the SENSITIVE keyword which the client layer transparently processes by encrypting the corresponding attributes later, a client sends a query request to the host server through a standard SQL interface. The query is transparently encrypted at the client site using the public key of the authentication module. The host server thus cannot decrypt the query. The host server forwards the encrypted query to the Request Handler inside the authentication module The Request Handler decrypts the query and forwards it to the Query Parser. The query is parsed generating a set of plans. Each plan is constructed by rewriting the original client query into a set of sub-queries, and, according to their target data set classification, each sub-query in the plan is identified as being either public or private. The Query Optimizer then estimates the execution costs of each of the plans and selects the best plan (one with least cost) for execution forwarding it to the dispatcher. The Query Dispatcher forwards the public queries to the host server and the private queries to the authentication module database engine while handling dependencies. The net result is that the maximum possible work is run on the host server's cheap cycles.

B QUERY OPTIMIZATION PROCESS

The Query Plan constructs to multiple plans for the client query. The constructed plan the Query Cost Estimator computes an estimate of the execution cost of that plan. The selected and passed on to the Query Plan Interpreter for execution. The Query Cost Estimator due to the logical partitioning of data. At a high level query optimization in a database system works as follows. The Query Plan Generator constructs possibly multiple plans for the client query. For each constructed plan the Query Cost Estimator computes an estimate of the execution cost of that plan. The best plan i.e., one with the least cost, is then selected and passed on to the Query Plan Interpreter for execution. The query optimization process in Trusted Database works similarly with key differences in the Query Cost Estimator

IV. PROPOSED METHOD

Secure and privacy-assured service outsourcing A secure and privacy-assured service outsourcing is used in cloud computing which uses linear programming and Compressed sensing techniques to transform images, which aims to take security, complexity, and efficiency into Consideration from the very beginning of the service flow. Because data explosion is the fast-growing trend to Outsource the image management systems to cloud and leverage its economic yet abundant computing resources to Efficiently and effectively acquire, store, and share images from data owners to a large number of data users. Although outsourcing the image services is quite promising, in order to become truly successful, it still faces a Number of fundamental and critical challenges, among which security is the top concern. To initiate the Investigation for these challenges and propose a novel outsourced image recovery service (oirs) architecture with Privacy assurance. For the simplicity of data acquisition at data owner side, oirs is specifically designed under the compressed sensing framework. The acquired image samples from data owners are later sent to cloud, which can be considered as a central data hub and is responsible for image sample storage and provides on-demand image Reconstruction service for data users. But it makes more complexity because the data is sent in its raw

form to one Cloud. The cryptography schemes are computationally more complex.

The Authentication process can be explained as follows.

End User (U): User, who aims to stores encrypted credentials to the cloud storage. So to encrypt data user should authenticate itself to the Trusted Gateway. **Remote User:** Remote User, who access the cloud storage outside the internal enterprise network. **Trusted Gateway (TG):** Trusted gateway is the work station having TPM which maintains the data to be encrypted comes from end users and encrypt them and store to the cloud storage and vice versa. **Authentication Server (AS):** Authentication Server verifies user's access right in database; create ticket granting ticket and session key. **Ticket Granting Server (TGS):** Ticket Granting Server issues ticket to request the Trusted Gateway.

Database: The Kerberos service must have a database to store user id (ID) and hashed passwords. The details of the Kerberos Authentication Service Exchange are: *A. Authentication Service Exchange to obtain ticket-granting Ticket*

(1) **U → AS** : IDu, IDtgc, TS1
(2) **AS → U** : E (Ku , [Ku,tgs||IDtgs||TS2 ||Lifetime2 ||Tickettgs])

Tickettgs= E(Ktgs, [Ku,tgs||IDu||ADu||IDtgs||TS2 ||Lifetime2]) *B. Ticket-granting service Exchange to obtain trusted gateway service-granting ticket*
(3) **U → TGS** : IDtg||Tickettgs||Authenticatoru
(4) **TGS → U** : E(Ku,tgs,[Ku,tg||IDtg||TS4 ||Tickettg])

Tickettg= E(Ktg,[Ku,tg||IDu||ADu||IDtg||TS4 ||Lifetime4]) Authenticatoru= E(Ku,tgs||IDu||ADu||TS3)

C. User /trusted gateway Authentication Exchange to obtain cloud service
(1) **U → TG** : Tickettg||Authenticatoru
(2) **TG → U** : E(Ku,tg,[TS5 +1])

Authentication= E(Ku,tg||IDu||ADu||TS5)

Once the session is created between end user and trusted gateway then the end user can send data to store in the cloud in encrypted form and also can retrieve data from the cloud with the help of Trusted Gateway. Records of data sent and retrieved to the cloud from various end users is maintains by the Trusted Gateway. As we clarify that the data which is stored in the cloud in the encrypted form in highly confidential so to keep the security of data we assume that the remote users who want to retrieve the data from cloud have TPM chip in his system. So remote users have to authenticate itself to the trusted gateway and then it can exchange keys, by which it can retrieve data directly from the cloud and decrypt itself

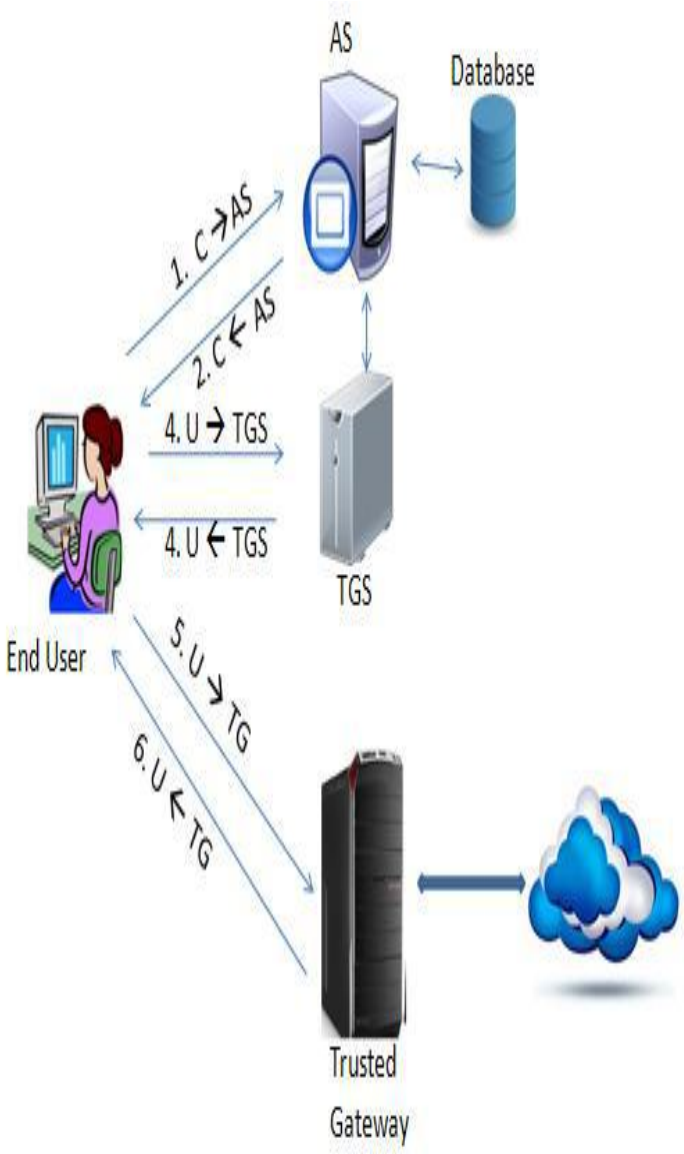

Figure 4.1 Authentication Process

 DOI:10.15693/ijaist/2016.v5i9.50-56

The following diagram explains remote session with cloud for accessing data base with authentication.

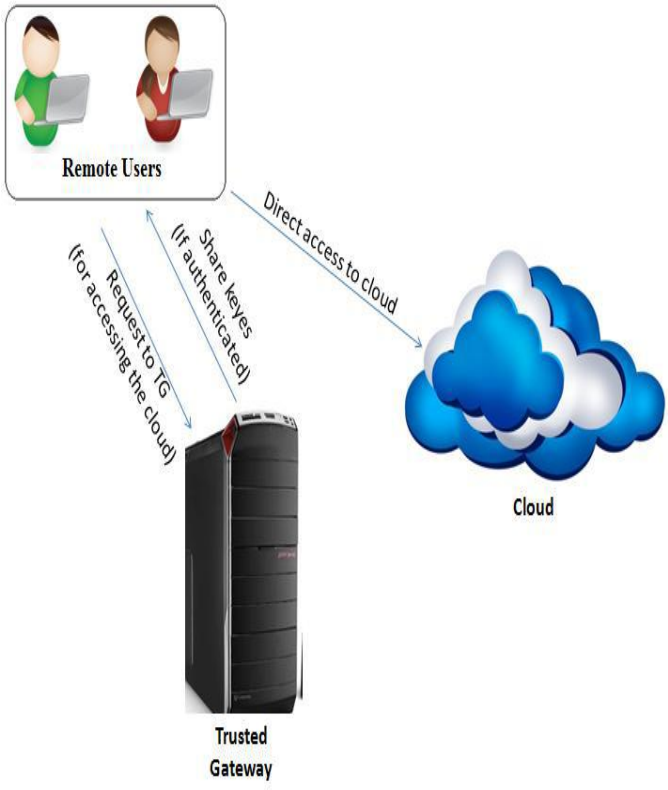

Figure 4.2 Remote session with cloud.

V. EXECUTION AND RESULTS ANALYSIS

This demonstration will show how trusted data base enables generalized query processing over encrypted data. The demonstration will cover

- ➔ Running queries, perform data manipulation and data
- ➔ Querying over outsourced encrypted data.
- ➔ Measuring the security mechanisms employed to ensure the execution of queries over sensitive data in a remote secure environment.

The following diagrams explians the accessing of trusted data base by user.

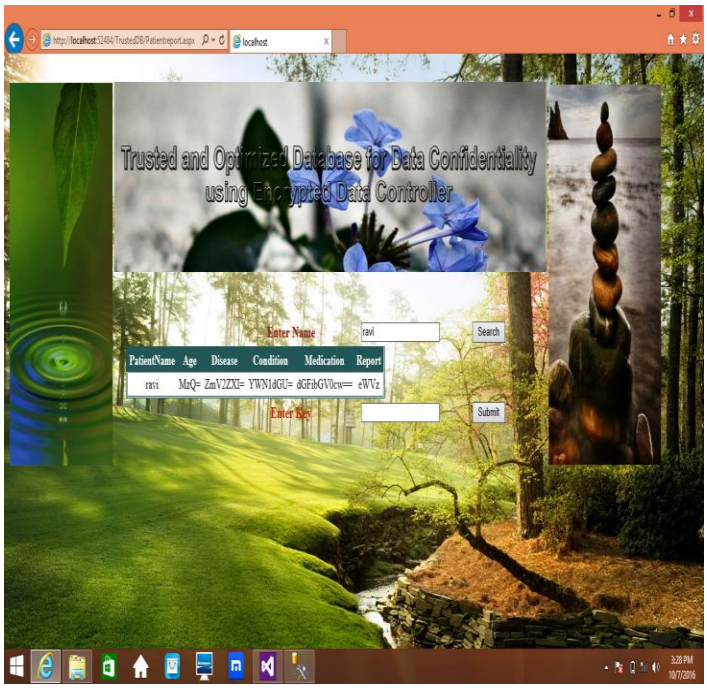

Figure 5.1 Query Result In Encrypted Form without Authentication

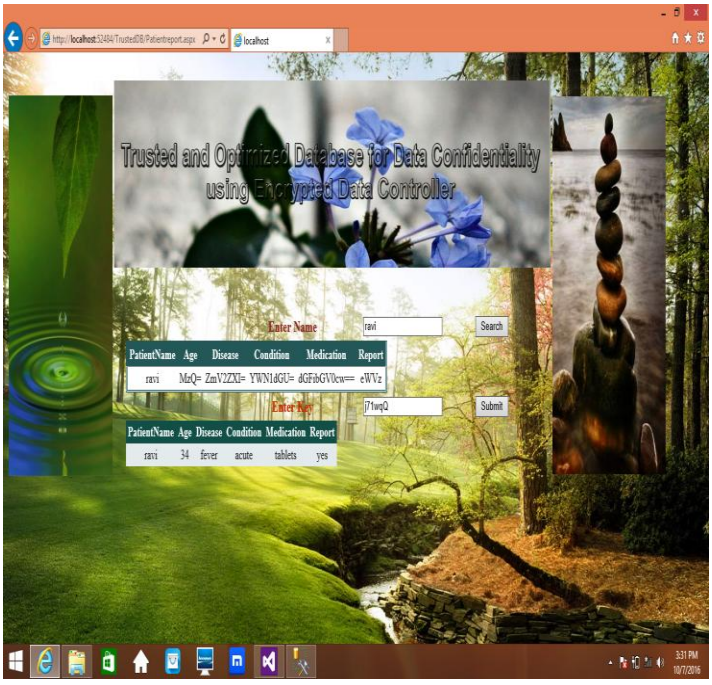

Figure 5.2 Query Result in Original Form with authentication

The following diagram explains cost of authentication using Hard ware based authentication.

 DOI:10.15693/ijaist/2016.v5i9.50-56

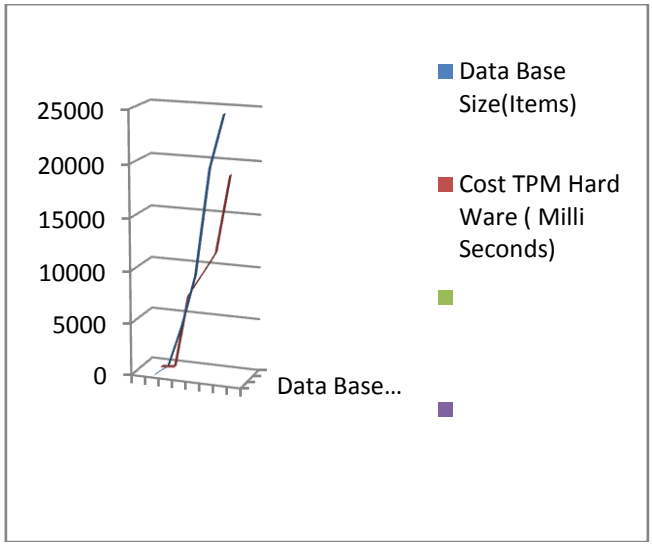

Figure 5.3 Cost of Authentication using Hardware based encryption (TPM)

The following diagram explains cost of authentication using Encrypted authentication.

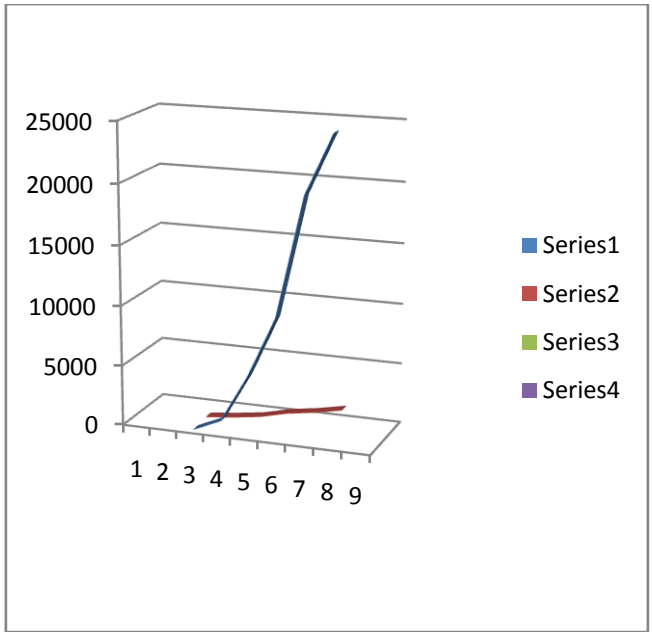

Figure 5.4 Cost of Authentication using Software based encryption

VI. CONCLUSION

Queries on encrypted data, propose division of data into secret partitions and rewriting of range queries over the original data in terms of the resulting partition identifiers. this balances a trade-off between client and server-side processing, as a function of the data segment size, the propose using tuples-level encryption and indexes on the encrypted tuples to support equality predicates. the main contribution here is the analysis of attribute exposure caused by query processing leading to two insights. the attribute exposure increases with the number of attributes used in an index, and the exposure decreases with the increase in database size.

The contributions of the paper are three 1) the implementation of software based trusted data base

2) the design and development of trusted data base with software trusted controller

3) the deployment of trusted database in cloud

4) optimized execution of queries with cost reduction

5) design of new cost models for cost reduction

In this paper we have proposed a model which helps to use trusted platform module widely for the security of cloud storage. We have design a new trust model which uses Software Controller that authenticates user to store encrypted data to the cloud and access data from cloud. The data will be safe in the public cloud also. Kerberos is the secure method to authenticating requests for any service, is used to authenticate end users to the trusted gateway. In

In future, in order to increase query functionality, a layered encryption scheme can be used and then dynamically adjusted (by revealing key to the server) according to client queries. Trusted DB, on the other hand, operates in an un trusted server model, where sensitive data are protected, both on disk and during processing. Data encrypted on disk but processed in server memory, compromise privacy during the processing interval. The disclosures risks in such solutions are analysed also propose a new query optimizer that takes into account both performance and disclosure risk for sensitive data. Individual data pages are encrypted by secret keys that are managed by a trusted hardware module. The decryption of the data pages and subsequent processing is done in server memory. Hence, the goal is to minimize the lifetime of sensitive data and keys in server memory after decryption.

REFERENCES

[1] Sumeet Bajaj and Radu Sion, A Trusted Hardware-Based Database with Privacy and Data Confidentiality , IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, VOL. 26, NO. 3, MARCH 2014

[2] TPC-H Benchmark, http://www.tpc.org/tpch/, 2013.

[3] IBM 4764 PCI-X Cryptographic Coprocessor, http://www-03. ibm.com/security/cryptocards/pcixcc/overview.shtml, 2007.

[4] G. Aggarwal, M. Bawa, P. Ganesan, H. Garcia-Molina, K. Kenthapadi, R. Motwani, U. Srivastava, D. Thomas, and Y. Xu, "Two Can Keep a Secret: A Distributed Architecture for Secure Database Services," Proc. Conf. Innovative Data Systems Research (CIDR), pp. 186-199, 2005.

[5] A. Iliev and S.W. Smith, "Protecting Client Privacy with Trusted Computing at the Server," IEEE Security and Privacy, vol. 3, no. 2,
pp. 20-28, Mar./Apr. 2005.
[6] M. Bellare, "New Proofs for NMAC and HMAC: Security Without Collision-Resistance," Proc. 26th Ann. Int'l Conf. Advances in Cryptology, pp. 602-619, 2006.
[7] B. Bhattacharjee, N. Abe, K. Goldman, B. Zadrozny, C. Apte, V.R. Chillakuru, and M. del Carpio, "Using Secure Coprocessors for
Privacy Preserving Collaborative Data Mining and Analysis," Proc. Second Int'l Workshop Data Management on New Hardware (DaMoN 06), 2006.
[8] M. Canim, M. Kantarcioglu, B. Hore, and S. Mehrotra, "Building Disclosure Risk Aware Query Optimizers for Relational Databases,"
Proc. VLDB Endowment, vol. 3, nos. 1/2, pp. 13-24, Sept. 2010.
[9] Y. Chen and R. Sion, "To cloud or Not to Cloud?: Musings on Costs and Viability," Proc. Second ACM Symp. Cloud Computing (SOCC '11), pp. 29:1-29:7, 2011.
[10] V. Ciriani, S.D.C. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, "Combining Fragmentation and Encryption to
Protect Privacy in Data Storage," ACM Trans. Information and System Security, vol. 13, no. 3, pp. 22:1-22:33, July 2010.
[11] T. Denis, Cryptography for Developers, Syngress, 2007.
[12] E. Damiani, C. Vimercati, S. Jajodia, S. Paraboschi, and P. Samarati, "Balancing Confidentiality and Efficiency in Untrusted Relational DBMSs," Proc. 10th ACM Conf. Computer and Communications Security (CCS '12), 2003.
[13] E. Mykletun and G. Tsudik, "Aggregation Queries in the Database-as-a-Service Model," Proc. 20th IFIP WG 11.3 Working Conf. Data and Applications Security, pp. 89-103, 2006.
[14] F.N. Afrati and V. Borkar, and M. Carey, and N. Polyzotis, and J.D. Ullman, "Map-Reduce Extensions and Recursive Queries," Proc.
14th Int'l Conf. Extending Database Technology (EDBT), pp. 1-8, 2011.
[15] V. Ganapathy, D. Thomas, T. Feder, H. Garcia-Molina, and R. Motwani, "Distributing Data for Secure Database Services," Proc. Fourth Int'l Workshop Privacy and Anonymity in the Information Soc.(PAIS '11), pp. 8:1-8:10, 2011.
[16] FIPS PUB 140-2, Security Requirements for Cryptographic Modules, http://csrc.nist.gov/groups/STM/cmvp/standards.html#02,
2013.

Authors Profile

Kammili Manasa studying final year MTech in Department of Computer Science Engineering at Sri Vasavi Engineering College, Tadepalligudem, Andhra Pradesh, India. Her Research interests includes cloud computing, Cryptography and Data Base Systems

Vedula Venkateswara Rao working as Associate Professor in Department of Computer Science Engineering at Sri Vasavi Engineering College, Tadepalligudem, Andhra Pradesh, India. He received Masters Degree in Computer Science Engineering from Jawaharlal Nehru Technological University Kakinada, Masters Degree in Information Technology from Punjabi University, Patiyala, India. His research interests include Cloud Computing and Distributed Systems, Data Mining, Big Data Analytics and Image Processing. He published several papers in International conferences and journals