ISSN 2395-1621

System to Ensure Data Privacy Using Special Hardware

[#1]Prof. K Reddy, [#2]Suraj Pinjan, [#3]Mayur Manjare, [#4]Vikas Talekar, [#5]Priyanka Nichit

[1]kamalreddy94@gmail.com
[2]surajbpinjan92@gmail.com
[3]mayurmanjare4232@gmail.com
[4]talekarvikas9011@gmail.com
[5]priyankanichit7@gmail.com

[#12345]Department of Computer Engineering Siddhant College of Engineering, Sudumbare.
Savitribai Phule Pune University

ABSTRACT

Traditionally, as shortly as confidentiality becomes a priority, data are encrypted before outsourcing to a service supplier. Any software-based cryptographic constructs then deployed, for server-side query processing on the encrypted information, inherently limit query expressiveness and efficiency of processing. Here, Trusted DB has been introduced, an outsourced database prototype that allows client to exe- cute SQL queries with privacy and beneath restrictive compliance constraints by leverage server-hosted, tamper-proof trusted hardware in important query processing stages, thereby removing any limitations on the sort of supported queries. Tofurther enhance the performance,the data attributes are classified as secure and unsecure attributes. The values of unsecure attributes are encrypted before storing on he remote server. The encrypted data attributes are operated upon in the SCPU and the unsecure data attributes are processed with the host computational resources. This dramatically improves the performance of the system. Despite the value overhead and performance limitations of trusted hardware, it has been shown that the prices per question are orders of magnitude less than any (existing or) potential future software-only mechanisms. Theoretical cost analysis shows that, the cost for execution of a simple operation on TrustedDB is much less than the processing using software based **cryptographic construct. Further, these theoretical results are approved by the experiments performed on the system prototype**.

Keywords— Data security,Creptography, SCPU(secure query processing CPU), SQL Database,Privacy

ARTICLE INFO

Article History

Received :29th February 2016

Received in revised form :

1st March 2016

Accepted :3th March, 2016

Published online :

4th March 2016

I. INTRODUCTION

In the current scenarios, where sensitive data is kept on the remote data servers of service providers by the clients, the data privacy is not guaranteed at all.The problem is that, cloud service providers are able to use the sensitive data of clients as they want. Outsourcing bank data is one such example, where the valuable data of bank clients is stored remotely by the bank administration.The loss of such valuable data of clients such as the online banking passords can result in great losses. The unrestricted access, for the data, allowed to the cloud service provider in todays cloud scenario, is somewhat injustice to the client. And, looking at the cost of encrypted data processing using a cryptographic construct, it seems unbearable for the cloud service providers for which profit matters a lot. Current approaches to address this problem includes using cryptographic homomorphism and transfer of whole data back to the client for processing.Among these approaches, the use of data transfer and homomorphisms are perticularly costlier as studied by Simmons and Bajaj in [1].

II.EXISTING SYSTEM

The current existing approaches to this problem includes 1) Transfering the entire encrypted data back to client before

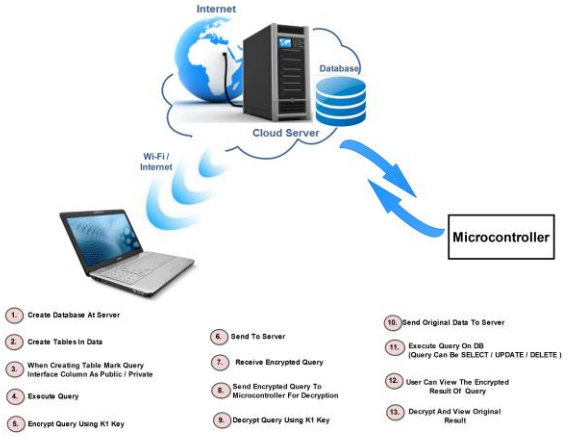
processing 2) Deploying cryptographic constructs server side that can process the encrypted data without decryption.

Problem with approach 1: Transfering large volumes of encrypted data back to the client requires lots of network time, hence it too costly to apply.

Problem with approach 2: Performing simple operations on encrypted data without decrypting ,for example aggrigation operation, needs many many cpu cycles; hence it is also a costly approach to implement.

III.ARCHITECTURE

Usage scenario:
The administrator creates the database on the server side.
Tables with fixed schema is created by the admin. The private attribute columns are labled as ”private” ,similarly the public key attributes columns are labeled as “public”. Before sending data to the server , client encrypts the private attribute data values using a symetric key. The client query is encrypted again by another algorithm. At server the client query is decrypted. If query is to be operated on private data it is executed on microcontroller . Elese , it is executed on server cpu.Result is communicated back to client.



IV.CONCLUSION

The problem of securing very private business data of banking sector on remote server is a challange which can be done by using the secure c processor inside the host server.
The implementation of such a system is a challenging task and the issues have been studied thoroughly.The problem is analysed a found to be the P type of problem. The designing of system has been acomplished and has been shown to fit in budget and given time.
Software Testing plan has been constructed which will ensure that the system performs acording to the recuirments of the target audiances.

ACKNOWLEDGEMENT

This paper could not have been written without the help of our guide Prof. Kamal Reddy and Head of Dept. Shubhangi Vairagar.

REFRENCES

[1]TrustedDB: A Trusted Hardware based Database with Privacy and Data Confidentiality Sumeet Bajaj, Radu Sion

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

[3] Marten Van Dijk, Craig Gentry, Shai Halevi, and Vinod Vaikuntanathan. Fully homomorphic

encryption over the integers. In Henri Gilbert, editor, EUROCRYPT, volume 6110 of Lecture Notes in Computer Science, pages 24–43. Springer, 2010.

[4]Encryption, Wikipedia

