International Journal of Science and Research Archive

eISSN: 2582-8185

Cross Ref DOI: 10.30574/ijsra

Journal homepage: https://ijsra.net/

(REVIEW ARTICLE)

Check for updates

Database security at cache layer

Mamta Rani *

Department of Computer Science, Gopichand Arya Mahila College, South Avenue Hanumangarh Road, Abohar, Distt. Fazilka, Punjab, 152116, India.

International Journal of Science and Research Archive, 2023, 09(02), 016–019

Publication history: Received on 18 May 2023; revised on 28 June 2023; accepted on 01 July 2023

Article DOI: https://doi.org/10.30574/ijsra.2023.9.2.0506

Abstract

As database security is the main concern, we are going to place an encryption module at the cache layer. All the encryption and decryption will be done at the cache layer before storing that data to the database, which will provide more security to the database Higher level security should be provided to the database so here we are placing an idea of Elliptical Curve Cryptography. A database is a collection of data that helps us to collect, retrieve, organize and manage the data in an efficient and effective manner. Databases are critical assets. They store client details, financial information, personal files, company secrets and other data necessary for business. Today database security is getting greater importance than the past which is the amount of data is stored in a corporate database is increasing.People are depending more on the corporate data for making a decision, management of customer service and supply chain management etc. Data stored in databases is usually very vulnerable data so it becomes very important and crucial to maintain this data securely. There are many front end applications that fetch data from secondary storage to main memory for processing and from main memory, data is stored in cache for temporary processing. Any loss or unavailability of data may seriously affect its performance. The database security should provide protected access to the contents of a database and should preserve the integrity, availability, consistency, and quality of the data. In this paper, I present a model where data is protected even on cache layer.

Keywords: Database; Security; Cache Layer; ECC; RSA

1. Introduction

The database is an integral part of any application, it is a repository of very crucial data so it becomes very important to maintain the security of this data, there exist many algorithms which provide security of the database at secondary storage but as in today's era, due to the advancement to technology, many faster memory types has been invented. One such kind of memory is Cache Memory, which is used in almost all computing machines in order to increase the processing speed of computers. So, it becomes very important to maintain the security of data in the cache layer as well. In this paper, I provide a solution to maintain the security of data in the cache layer. In this paper, an algorithm is given using Elliptical Curve Cryptography encryption algorithm.

2. Our solution

This describes the architecture based on placing the Elliptical curve cryptography module insidedatabase management software (DBMS), just above the database cache. Using this method only selected part of the database can be encrypted instead of the whole database. This architecture allows achieving a high level of data security while offering enhanced performance.

The encryption operation can take place at different layers.

* Corresponding author: Mamta Rani

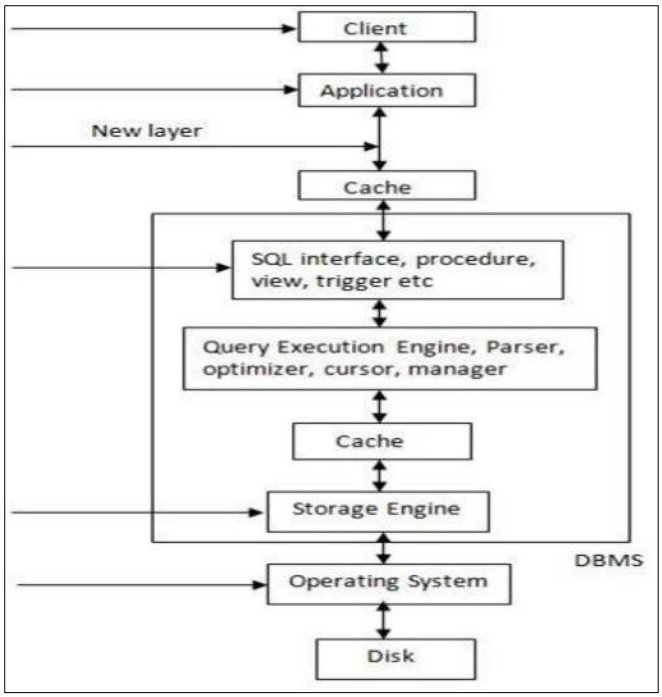

Figure 1 Existing Layers of Encryption

2.1. Operating System

In this layer, the pages are encrypted/decrypted by the operating system when they are written/read from disk.

This layer is totally transparent, therefore avoiding any changes to the DBMS and to existingapplications.

Drawbacks

We cannot encrypt specific portions of the database.

2.2. Storage Engine

Similar to the operating system layer, pages in this layer are encrypted/decrypted when they are written/read from disk. However, as opposed to the operating system layer, encryption/decryption operations areperformed by the DBMS, at the cell-level granularity.

2.3. SQL Interface

At this layer, data is encrypted using predefined stored procedures, views and triggers. Drawback Encryption takes place above the query execution engine, and thus some database mechanisms (e.g., indexes and foreign keys) may not function properly.

2.4. Application

In this layer, sensitive data is encrypted in the application layer before it is sent to the database and decrypted before usage. Drawback of encryption at application layer:

As encryption takes place above the query execution engine, different database mechanisms cannotfunction properly and need to be re-implemented by the application.

2.5. Client

In this layer, only legitimate user is able to access sensitive data. However, it implies limiting the ability of the database server to process the encrypted data and in extreme cases, to use the database server for storage only.

2.6. Cache layer (new layer)

Data will encrypted and decrypted using elliptical curve cryptography (ECC) at cache layer before storing it to the database. Using this technique we can encrypt or decrypt particular part of the database.

2.7. Elliptical Curve Cryptography (ECC)

It is a public key cryptography. Key generation in this technique is done by using Elliptical curveequation which is as follows:

- -E -> Elliptic Curve
- -P -> Point on the curve
- -n -> Maximum limit (This should be a prime number)

Short key is faster and requires less computing power than other existing techniques. Security providedby RSA using 1024 bits key is equal to security provided by ECC technique using 256 bits key. In this way ECC provided more security than existing encryption technique.

-256 bit (ECC) = 1024 bit (RSA)

3. Evidence the solution works

The following Figure 2. shows the graph of cache time and disc time required for ECC algorithm. The x-axis shows the number of records and y-axis shows the time in ms.

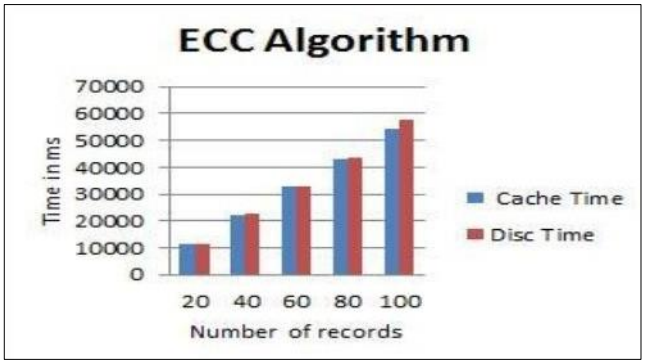

Figure 2 Graph for ECC algorithm

4. Competitive approaches

Security provided by RSA using 1024 bits key is equal to security provided by ECC technique using 256 bits key. In this way ECC provided more security than existing encryption technique.

-164 bit (ECC) = 1024 bit (RSA)

5. Current status

Elliptical curve cryptography is one of the powerful techniques used for encryption and decryption of data. ECC is already implemented to encrypt and decrypt the data at database layer but not at cache layer. So here we are placing an idea to encrypt and decrypt the data at cache layer which will provide more security to the database along with higher performance.

6. Next steps

In this paper, we likewise proposed a novel building design for database encryption, which is focused around putting the encryption module inside the Database Management, Programming (DBMS), just over the database cache, and utilizing a devoted method to scramble every database cell esteem together with its organizes. In future exploration, we

can extend our system for mobile applications or cloud computing for proving client-side encryption. We can also use our application for a website that requires advanced authentication.

7. Conclusion

In this paper a novel solution has been given to maintain the security of the database at the cache layer, In the future this algorithm can be extended for cloud computing and mobile applications to provide security of data. This study helps in maintaining the security of data even when the data is being accessed on the cache layer.

Compliance with ethical standards

Disclosure of conflict of interest

I have no conflict of interest to declare.

References

[1] Tarun Narayan Shankar, G. Sahoo, Cryptography with Elliptic Curves, International Journal Of Computer Science And Applications Vol. 2, No. 1, April / May 2009,ISSN: 0974-1003

[2] Fast point multiplication on Koblitz curves: Parallelization method and implementations.

[3] Gaikwad T, Raut A. A Review on Database Security [Internet]. International Journal of Science and Research;

[4] Ashour A N Mostafa. Security of Database Management Systems [Internet]. ResearchGate. unknown; 2016.