B. THOMAS GOLISANO COLLEGE OF COMPUTING & INFORMATION SCIENCES

HippoCrypt Database Management System

Vishvesh Karwa, Rohit Kunjilikattil, Nihal Parchand ■ ■ ■ Advisor: Dr. Rajendra K. Raj rkr@cs.rit.edu

Computer Science

Introduction

- Data security in bank databases is extremely important.
- New types of databases like Hippocratic databases are becoming mainstream.
- This project is focused on the security of bank databases by implementing preventive measures using CryptDB server and principles of Hippocratic databases.

Hippocratic Principles

- The Hippocratic database principles empowers the users by providing the right to select the amount of shared information.
- The rules and regulations focused on limiting the data gathered, analyzed, and retained by the companies.
- Hippocratic principles also require complete disclosure of how the customer data is used and for what purpose.
- The implemented system includes a terms and conditions page that explains the purpose and the storage time for each recorded attribute.

Role-based Access Control

Role	Tables accessed	Scope of access
Manager	Customer	Personal information of customers
Accountant	Customer | Account	Account information of customers
Sales	Customer	Limited personal information of customers

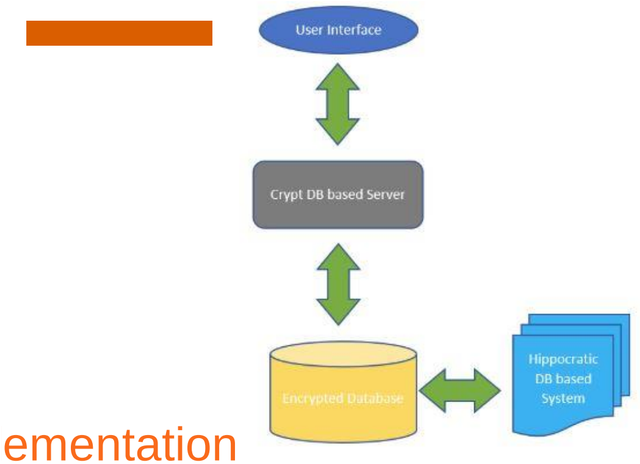
- Role-based access control (RBAC) is one of the fundamental security measures to prevent unauthorized data access.
- Hippocratic principles dictate that a user must only have access to the data he is entitled to, which is achieved by implementing RBAC.
- The implemented system defines roles for bank employees such as Manager, Accountant, and Sales.
- The customer and bank employees are differentiated using two types of login: Customer and Admin.
- RBAC in conjunction with the CryptDB server makes the bank application robust and highly secure.

Motivation

- The motivation behind the HippoCrypt DBMS is to provide a state-of-the-art security mechanism to strengthen the privacy for bank databases.
- A new era of banking database can be assured by leveraging the advantages of Hippocratic principles, role-based access control, and data encryption.

System Architecture

- New users have to sign up for creating a new account.
- Users can view, update, or delete their personal details through the user interface.
- Customers can transfer or withdraw money from their account.
- Admins can view and delete the expired information.
- Hippocratic principles and data encryption ensures user information security.



Implementation

Data Encryption

	TXN_ID	AMOUNT	TXN_DATE	TXN_TYPE	ACCOUNT_ID
▶	Go7yUw==|E1aDAw57M81WxXbLZSIZ/g==	Mcbz7T2p|ro90Kgk9bQ9uPCbUVibNFA==	6Id0WuXGP73kyA==|Mm3TVPWpjvWp9I3WZ/S...	/O1Q3w==|LnU5E4XqYvdYar0BVURPJw==	smTK|t5HnT9YIO6V4rGytIvKd5Q==
	Vw/1XQ==|eIHi+9wzbTSuRgyQ/7jyA==	Uis=|DLDBkNa7hCCYJDc+/AfN2Q==	6Id0WuXGP73kyA==|Mm3TVPWpjvWp9I3WZ/S...	dPCi6w==|tWQ1r1Ikyz83uuRnGeVZFw==	smTK|t5HnT9YIO6V4rGytIvKd5Q==
	WWJNpA==|53VkaeCGz6UYGFR4RQkh1w==	ehVZAA==|EZ9u/OSB63hJyhdCoYz6w==	6Id0WuXGP73kyA==|Mm3TVPWpjvWp9I3WZ/S...	dPCi6w==|tWQ1r1Ikyz83uuRnGeVZFw==	smTK|t5HnT9YIO6V4rGytIvKd5Q==
	mgFQpg==|Bw02Iqu+izk+2dqH9AtZ8g==	9urOXA==|GEvHkI46zUkLuH4TFEgneQ==	6Id0WuXGP73kyA==|Mm3TVPWpjvWp9I3WZ/S...	dPCi6w==|tWQ1r1Ikyz83uuRnGeVZFw==	smTK|t5HnT9YIO6V4rGytIvKd5Q==
	7L5XgA==|9VxvAys/bKO3iONjZbmOjA==	ehVZAA==|EZ9u/OSB63hJyhdCoYz6w==	6Id0WuXGP73kyA==|Mm3TVPWpjvWp9I3WZ/S...	/O1Q3w==|LnU5E4XqYvdYar0BVURPJw==	72Ah|h81DJdJbQmuwubJlDkqC1g==
	JizWMg==|lOc/FvaLRj7UdqOpgxm1Tw==	VdhTUg==|/v9Xg4JXQ6N8SuSIf8c4Zg==	6Id0WuXGP73kyA==|Mm3TVPWpjvWp9I3WZ/S...	dPCi6w==|tWQ1r1Ikyz83uuRnGeVZFw==	72Ah|h81DJdJbQmuwubJlDkqC1g==
	j9Nt7w==|nZzZ+403VPmw4fFWf/1gtg==	8xg=|FvhnLP0JHg8p4cearmacA==	6Id0WuXGP73kyA==|Mm3TVPWpjvWp9I3WZ/S...	dPCi6w==|tWQ1r1Ikyz83uuRnGeVZFw==	smTK|t5HnT9YIO6V4rGytIvKd5Q==

- The entire database was encrypted using the AES encryption with the help of Python scripts.
- AES is a symmetric block cipher that provides high speed and relatively high security in terms of bits.

Results

- The resulting end product of the whole project is a system that handles encryption and decryption of data stored in the database.
- The finished system is also responsible for incorporating the principles of a Hippocratic database in turn giving user complete authority over their information.

Future Work

Dynamic Attribute-based control access

- Replaces assigning roles to users by some predefined rules with complex Boolean set of rules.

Non-deterministic encryption techniques

- Non-deterministic techniques create different keys for the same string which upgrades the system security.

Allowing users to decide the data storage time

- The users can decide what information can be stored by the companies and for how long to increase

Summary

- The results prove that the Hippocrypt DBMS enforces strict security mechanisms.
- The advantages of secure encryption, RBAC, and enhanced user data control are successfully implemented through this system.
- This provides a platform for an enhanced banking experience that focuses on user satisfaction.
- This project can act as an inspiration for future work that aims to provide complete database security using CryptDB and Hippocratic databases.

References

- Agrawal, Rakesh & Kiernan, Jerry & Srikant, Ramakrishnan & Xu, Yirong. (2002). Chapter 14. Hippocratic Databases. DOI: 10.1016/B978-155860869-6/50021-4
- Raluca Ada Popa, Catherine M. S. Redfield, Nickolai Zeldovich, and Hari Balakrishnan. 2011. CryptDB: protecting confidentiality with encrypted query processing.. DOI:https://doi.org/10.1145/2043556.2043566