Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol.12 Issue 12, DECEMBER 2023

Securing Privacy and Maintaining Data Confidentiality are Fundamental Principles for Establishing a Trustworthy Database

Balla Aswani Devi
Assistant Professor,
Depertment of Artificial Intelligence & Machine Learning,
Swarnandhra College of Engineering and Technology,
Narasapur,

Chennam Chandrika Surya
Assistant Professor,
Depertment of Artificial Intelligence & Machine Learning,
Swarnandhra College of Engineering and Technology,
Narasapur,

Sudha S P
Assistant Professor,
Depertment of Artificial Intelligence & Machine Learning,
Swarnandhra College of Engineering and Technology,
Narasapur,

Gumpula Jhansi
Assistant Professor,
Depertment of Artificial Intelligence & Machine Learning,
Swarnandhra College of Engineering and Technology,
Narasapur,

ABSTRACT
Traditionally, when prioritizing confidentiality, data is encrypted before being outsourced to a service provider. Within this service provider, a three-tiered information structure is maintained to ensure secure interactions between users and a reliable database. Advanced encryption standards are employed for the encryption process. The deployment of software-based cryptographic constructs for server-side query processing on encrypted data inherently constrains query efficiency. To address this, we introduce a Customer Relationship Management (CRM) model for data input. In this model, we incorporate Trusted Database with Advanced Encryption Standard (AES), creating an outsourced data paradigm that allows clients to execute SQL queries with privacy and adherence to regulatory compliance. This is achieved by leveraging server-hosted, tamper-proof trusted hardware during critical query processing stages, eliminating constraints on the types of supported queries. Despite the associated cost overhead and performance limitations of trusted databases, our analysis demonstrates that the costs per query are orders of magnitude lower than any existing or potential future software-only mechanisms. The trusted database is constructed and evaluated on an actual server for performance assessment.

Keywords: **SQL,Trusted Database, AES, CRM, software-based, tamper-proof.**

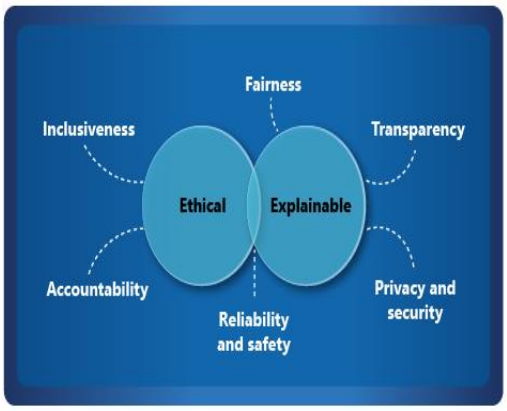
I INTRODUCTION

Data storage allows users to store their information remotely and access on-demand high-quality cloud applications without the burden of managing local hardware and software. While the benefits are evident, this service introduces new security risks as users lose physical control over their outsourced data, impacting data correctness. To address this challenge and ensure secure and reliable information storage, we propose a flexible distributed storage integrity auditing mechanism. This mechanism utilizes homomorphic tokens and distributed erasure-coded data, enabling users to audit cloud storage with minimal communication and computation costs.

The proposed design not only guarantees robust data storage correctness but also facilitates fast error localization, identifying misbehaving servers. Recognizing that stored data is dynamic, the design supports secure and efficient dynamic operations on outsourced data, including block modification, deletion, and append.

Our analysis demonstrates the efficiency and resilience of the proposed approach against Byzantine failure, malicious data modification attacks, and even colluding server attacks. Additionally, we undertake the design and development of a secure, relational knowledgebase, ensuring full data confidentiality and unrestricted query quality. We incorporate detailed query optimization techniques in a hardware-based execution model.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol.12 Issue 12, DECEMBER 2023



As a result, we posit that a comprehensive privacy-enabled secure database, leveraging server-side secure hardware, can be designed and operated at a fraction of the cost compared to existing or future cryptography-enabled private processing on standard server hardware. To validate this, we introduce TrustedDB, an SQL database processing engine that utilizes tamper-proof cryptographic coprocessors like the IBM 4764 in close proximity to the outsourced data. TrustedDB maximizes the use of common unsecured server resources, overcoming the challenges posed by the limited processing and memory capabilities of tamper-resistant designs.

The assurance of privacy and the preservation of data confidentiality stand as cornerstones in the creation of a dependable and credible database system. In an age where digital information forms the backbone of numerous operations, ensuring the security of sensitive data within databases is imperative. This introductory statement sets the stage for comprehending the significance of safeguarding privacy and maintaining data confidentiality as pivotal principles in establishing a database that users, stakeholders, and regulatory bodies can trust.

The essence of these fundamental principles lies in protecting sensitive information from unauthorized access, misuse, alteration, or theft. A trustworthy database upholds stringent measures to shield personal, proprietary, or confidential data, adhering to ethical standards, legal requirements, and industry best practices. This commitment not only fosters trust but also mitigates potential risks associated with data breaches, identity theft, or unauthorized exposure.

From encryption protocols and access controls to meticulous auditing and adherence to regulatory guidelines, the strategies employed to ensure privacy and confidentiality within a database are multifaceted. These strategies are designed to safeguard data throughout its lifecycle, from collection and storage to transmission and eventual disposal.

In an interconnected digital landscape where data holds immense value, understanding the paramount importance of securing privacy and maintaining data confidentiality lays the foundation for a robust, reliable, and trustworthy database infrastructure. This commitment underscores the ethical responsibility and accountability involved in handling sensitive information, promoting integrity, trustworthiness, and reliability within the database ecosystem.

II EXISTING SYSTEM

Our proposition revolves around the creation and operation of a comprehensive, privacy-enabled secure information system utilizing server-side trusted hardware. This system is envisioned to be engineered and operated at a significantly reduced cost compared to current or future cryptography-enabled private processing on conventional server hardware. To substantiate this claim, we undertook the design and construction of Trusted DB, an SQL data processing engine that leverages tamper-proof cryptographic coprocessors, such as the IBM 4764, in close proximity to the outsourced data.

While tamper-resistant designs pose challenges due to limitations in processing ability and memory capacity, Trusted DB overcomes these obstacles. We achieve this by maximizing the utilization of common, unsecured server resources. For instance, Trusted DB enables the secure coprocessor (SCPU) to access storage devices transparently while preserving data confidentiality through on-the-fly encryption. This eliminates constraints on the size of supported databases. Furthermore, client queries are preprocessed to identify sensitive components to be executed within the SCPU, while non-sensitive operations are offloaded to the entrusted host server. This approach significantly enhances performance and reduces transaction costs.

However, it's essential to note the disadvantages of relying on trusted hardware, including its impracticality due to performance limitations and higher acquisition costs. In many cases, efforts to implement such systems have stopped short of proposing or constructing fully-fledged data processing engines. While computation within secure processors is more cost-effective than equivalent cryptographic operations on the provider's unsecured server hardware, the initial acquisition cost of secure hardware remains a significant barrier.

III PROPOSED SYSTEM

The primary focus of the proposed system is on enhancing the security of information storage, a critical aspect of quality of service. The objective is to ensure the correctness of users' information within the storage through the introduction of an efficient and adaptable distributed framework with two distinctive features, distinguishing it from its predecessors. By employing homomorphic tokens and distributed verification of erasure-coded information, this framework achieves a dual goal of ensuring storage correctness and localizing information errors, specifically identifying misbehaving servers.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol.12 Issue 12, DECEMBER 2023

Key Components of the Proposed System:
1. Efficient and Adaptable Distributed Framework:
The primary aim is to identify and implement an efficient and adaptable distributed framework with explicit support for dynamic information. This framework is crucial for confirming the correctness of users' information within the storage.

2. Dynamic Information Support:
Acknowledging that an information storage service is more than just a third-party warehouse, as users frequently update data (insertion, deletion, modification, appending, etc.), ensuring storage correctness under dynamic information updates becomes crucial. Traditional integrity assurance techniques are rendered futile, necessitating innovative solutions.

3.Analysis of Efficiency and Resilience:
A comprehensive analysis demonstrates that the proposed framework is highly efficient and resilient. It proves to be robust against challenges such as Byzantine failure, malicious information modification attacks, and even collusion among servers.

Advantages of the Proposed System:
Achieving Storage Data Integrity and Availability:
The proposed system aims to provide assurances regarding the integrity and availability of storage data. By incorporating dynamic information support and advanced security features, it effectively addresses challenges posed by frequent data updates and potential malicious activities, enhancing the overall reliability of the storage system.

Adopting an Effective and Flexible Distributed Storage Verification Scheme:
The proposed system emphasizes the adoption of an effective and flexible distributed storage verification scheme explicitly designed to support dynamic data.

Ensuring Correctness and Availability of Users' Data:
Ensuring the correctness and availability of users' data within the storage is a central objective of the proposed system.

Audit Storage Service with Minimal Communication and Computation Cost:
The system aims to audit the storage service with very light communication and computation costs, ensuring efficiency in the verification process.
Access Control: Implement strict access controls by defining roles and permissions. Not everyone should have access to all data within the database. Role-based access control (RBAC) ensures that users only have access to the data they need for their specific roles.

Designing Support for Secure and Efficient Dynamic Operations:
The proposed system is designed to provide further support for secure and efficient dynamic operations on outsourced data, including block modification, deletion, and append.

IV RELATED WORK

1. User Registration and Control

- Used for registering users in custom modules supporting personalization and user specific handling.
- Registration includes checks for username availability and assignment of a unique ID.
- Users can create their own accounts.

2.User Control:
- Involves controlling logins with usernames and passwords from the registration process.
- After login, users can encrypt original data, store it in the database, and retrieve it based on a unique ID and searched data.
- User logins determine rights for viewing, editing, updating, or deleting resource contents.

3.Security Concerns:
- Confidential data is part of stored information.
- Storing data on cloud services may pose a risk of data leakage.
- No guaranteed tracking of original data in case of hacking.

V CRM SERVICE:

1. Definition of CRM:
Customer Relationship Management (CRM) focuses on creating, developing, and enhancing individualized customer relationships.
- Aims to understand, anticipate, and manage the needs of current and potential customers.
- Comprehensive integration of marketing, sales, customer services, and field support.

2. Purpose of CRM:
- Maximize the total customer lifetime value.
- Shift from traditional marketing, emphasizing customer retention alongside acquiring new customers.
- Creates a competitive advantage over similar product or service providers.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol.12 Issue 12, DECEMBER 2023

3. System Components:

- Consists of index, registration, and login pages.
- Users register with details, send encrypted original data for storage, and retrieve data by decrypting it with a decryption key.

Encryption/Decryption Service

1. Encryption Process:

- Encrypts and stores user data in response to user requests.
- Enhances confidentiality and prevents unauthorized access.

2.Decryption Process:

- Authenticates user ID and search data ownership.
- Decrypts encrypted data using a decryption key if authenticated and sends the original data to the user.

Accessing Storage Service

Data Storage and Retrieval:

- Original user data is encrypted and stored with the user ID to prevent misuse.
- During retrieval, the storage service system checks for identical user ID and search data.
- Encrypted data is sent to the Encryption/Decryption Service System for decryption before being delivered to the user.
- User interacts with the database through the CRM service.
- This system aims to provide secure user registration, controlled access, and seamless integration with CRM functionalities, ensuring the confidentiality of stored data through encryption and controlled access to storage service.

VI CONCLUSION

In this paper, we have delved into the critical domain of information security within cloud data storage, a complex and distributed storage system. Our focus has been on addressing the challenges related to data integrity and accessibility in cloud environments, aiming to establish a reliable standard for cloud storage services that ensures user confidence. To tackle the issues surrounding cloud data integrity and availability, we have introduced a robust and adaptable distributed framework. This framework incorporates explicit dynamic data support, including functionalities such as block updates, deletions, and appends. A key aspect of our approach involves the implementation of erasure-correcting code within the file distribution arrangement. This technique generates redundancy parity vectors, contributing to the assurance of data reliability. Our proposed system also integrates homomorphic tokens with distributed verification of erasure-coded data. This integration serves to achieve a dual objective: storage correctness assurance and precise data error localization. Specifically, when data corruption is identified during the storage correctness verification across distributed servers, our system enables the simultaneous identification of the misbehaving server(s). In conclusion, our proposed distributed framework addresses the complexities of cloud data storage, providing users with a secure and reliable service. By incorporating erasure-correcting code and homomorphic tokens, our system not only ensures data integrity but also facilitates the identification of anomalies in the storage environment. This contributes to building trust in cloud storage services, offering users confidence in the integrity and availability of their data.

VII REFERENCE

[1] "Database Security and Auditing: Protecting Data Integrity and Accessibility" by Hassan A. Afyouni.
[2] "Principles of Database Security" by Kan Zhang.
[3] "Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World" by Bruce Schneier.
[4] "Database Security: What Students Need to Know" by Silvana Castano, Danilo Bruschi, and Fabio Massacci.
[5] "Database Security" on Coursera.
[6] "Introduction to Cyber Security Specialization" on edX might cover topics relevant to securing databases and ensuring data confidentiality.