ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 10| Issue: 6| June 2024|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2024: 8.402 || ISI Value: 1.188

SANITIZABLE ACCESS CONTROL AGAINST MALICIOUS DATA PUBLISHERS

K. Vichitha Bhanu[1], Dr. Devi. A[2]

[1]*Department of Computer Science and Application, Reva University, Bangalore, India*
[2]*Associate Professor REVA University, Department of Computer Science and Application, Bangalore, India*

Article DOI: https://doi.org/10.36713/epra17533
DOI No: 10.36713/epra17533

ABSTRACT

Significant worries about data security and privacy have arisen because of the quick expansion of data sharing and interchange across a variety of applications. Sensitive information is seriously threatened by malicious data publishers, who compromise data security and integrity. This research study offers a fresh paradigm for "Sanitizable Access Control Against Malicious Data Publishers," which gives recipients of data the ability to efficiently filter and cleanse data they obtain from sources they don't trust. The suggested system makes use of access control methods and cryptographic techniques to offer a safe and adaptable setting for data exchange. Techniques for data encryption and sanitization guarantee that private information is kept safe even when handled by unscrupulous publications. To avoid unwanted access, trust management and verification procedures confirm the identity of data publishers and recipients.The sterile access management system

KEYWORDS—*Data security, Trust management, Access control policies, Sensitive information*

I. INTRODUCTION

Sensitive data must be protected against unwanted access due to the explosion of digital information and the quick development of data-driven applications. To implement security regulations and guarantee that only authorized entities may access certain resources, access control techniques are frequently used. But these conventional Access control systems frequently aren't strong enough to prevent hostile data publishers from purposefully introducing false or damaging material into the system. This study article suggests a unique solution to this problem called "Sanitizable Access Control Against Malicious Data Publishers." This framework's main objective is to enable data receivers to effectively filter and sanitize information from unreliable sources while maintaining data integrity and confidentiality. Through the integration of cutting-edge data sanitization methods with conventional access control concepts

II.LITERATURE SURVEY

The research study "Sanitizable Access Control Against Malicious Data Publishers" conducted a literature assessment that uncovered a significant amount of material pertaining to data security and privacy in the context of access control methods. Numerous scholars have examined various strategies to tackle the obstacles presented by malevolent data producers and guarantee the secrecy and integrity of data. A prominent area of study is secure program partitioning, which processes data on untrusted hosts while maintaining secrecy Lorch et.al [2]

Other research has looked at useful methods for decrypting data so that receivers may access information without disclosing private information Song et.al [1]

Researchers have suggested ways to do data mining activities while maintaining data privacy, which has also generated interest in confidentiality-preserving data mining Li et.al [3] Furthermore, to improve privacy beyond k-anonymity and l-diversity, the idea of "t-closeness" has been proposed, guaranteeing that sensitive information cannot be deduced from quasi-identifiers Li et.al [4]

Secure provenance, which aims to track the origin and access history of data in the cloud, has been highlighted as a crucial component of data forensics in the context of cloud computing Lu et.al [6] It has also been suggested to use Crypt DB, a solution for encrypted query processing that preserves secrecy, to secure private information while allowing query operations Bindschaedler et.al [7]

Additionally, developments in completely homomorphic encryption systems have made it possible to do calculations on encrypted data directly, adding another degree of privacy protection Gentry et.al [8]. Research has been done on atomic proxy cryptography and divergent protocols, which enable middlemen to handle encrypted data on behalf of the data owner. Guaranteeing safe handling and use of data Blaze et.al [5]

Additionally, to manage access to certain parts inside XML data structures, fine-grained access control systems for XML documents have been studied Damiani et.al [10]. To safeguard users' identities and facilitate easy access to a range of services, privacy-enhancing identity management strategies have also been investigated Fischer-Hübner et.al [9]

III. EXISTING WORK

"Privacy-Preserving Access Control Against Malicious Data Publishers in Cloud Computing Environments "The authors of this study suggest a privacy-preserving access management system for cloud computing environments that is intended to shield sensitive data from unscrupulous data publishers. The mechanism guarantees that receivers of data may effectively access and make use of cleaned data while preserving confidentiality and data integrity.

The main elements of the suggested framework are policies for access control, trust management, and data encryption and sanitization. Sensitive information is kept safe during transmission and storage thanks to data encryption, which also prevents unwanted parties from accessing it. By using sanitization procedures, data recipients can reduce the risk posed by malicious data publishers by filtering and removing information from the received data that may be dangerous or unneeded.

When it comes to confirming the legitimacy and validity of data producers, trust management is essential. By keeping track of data publishers' actions over time, the system creates a reputation database that helps data receivers recognize potentially dangerous sources and take necessary action.

Policies for access control specify who can access particular data and under what circumstances. In order to enforce limitations on data consumption based on the identities and responsibilities of the receivers, the framework includes fine-grained access controls. It also allows updates for dynamic access control, which helps it adjust to changing needs and prevent security lapses.

IV. METHODOLOGY

The goal of the suggested technique is to create a sanitizable access control system that is both secure and effective in protecting sensitive information from nefarious data publishers. The following are the main steps in the methodology: Encryption and Data Sanitization: Before being made public by data, the sensitive information is first cleaned and encrypted. A few sanitization strategies, including k-anonymity, l-diversity, and t-closeness, can be used to anonymize the data without compromising its privacy or usefulness. Modern encryption techniques like homomorphic encryption and proxy re-encryption are also used to guarantee the privacy of the data both during transmission and storage
Trust Management and Verification: To confirm the legitimacy of data publishers, a trust management system is put in place. In order to do this, trust measures and reputation ratings must be defined using past data publication patterns and user reviews.

To ascertain the dependability of a certain data publisher and if the published data satisfies the necessary privacy criteria, data receivers can refer to the trust management system.

Access Control Policies: Access control policies are designed to manage access to data by considering user roles, permissions, and needs for sanitization. Based on their credentials and the reliability of the data publisher, receivers of the data are allowed access to the cleaned data. The purpose of the access control policies is to protect the privacy of the data by making sure that only authorized parties may access and use it.

Processing Sanitization Query: The system allows data receivers to submit sanitization queries that indicate the required level of sanitization as well as the data properties they want access to. The suggested architecture handles these requests while taking the data publishers' reliability and access control guidelines into account. The data receiver receives the cleaned data once it has been processed and meets their needs.

Accountability and Audit Trail: All access requests, query processing operations, and data disclosures are recorded in the system's audit trail. In the event of any security breaches or attempts at illegal access, this guarantees traceability and responsibility. Forensic analysis and the detection of potentially harmful activity may be conducted using the audit trail.

V. PROPOSED FRAMEWORK

A. Sanitization techniques

The framework leverages both static and dynamic sanitization techniques:
Static Sanitization: Predefined rules and patterns to remove known types of harmful content.
Dynamic Sanitization: Real-time monitoring and updating of sanitization rules based on detected threats.

B. Access Control Mechanisms

Policies that combine role-based, attribute-based, and context-awareness are used to impose access control. These safeguards guarantee that data may only be accessed or altered by authorized personnel, and that any modifications are recorded and looked for irregularities.

C. Anomaly Detection

To find irregularities in the patterns of data access, machine learning methods are used. Methods including regression analysis, categorization, and clustering aid in the detection of potentially harmful activity

VI. IMPLEMENTATION

system is essential to achieving the efficacy and efficiency of the suggested framework. In order to ensure data integrity and confidentiality while reducing the risks posed by hostile actors, the system is built to give data recipients the capacity to filter and sanitize data received from untrusted data publishers.

The first step in the implementation is the creation of a strong access control model that safeguards sensitive data using sanitization and encryption methods. To ensure that only authorized receivers may access and decode the data, the system encrypts the data at the source prior to transmission using cryptographic techniques. This stops fraudulent data publishers and other unauthorized parties from obtaining the raw data.

The system adds a trust management and verification component to enable sanitization. This part evaluates data publishers' credibility and reputation by looking at past performance along with other pertinent indicators. Data receivers can choose which publications' data they will accept by setting trust levels. A publisher's data is deemed untrustworthy and is either rejected or reported for additional examination if their trust rating is below the cutoff. Policies and procedures for access control are crucial to the implementation. Recipients of data can decide who can access certain data and under what circumstances by defining fine-grained access controls. These guidelines are dynamic and can be changed in response to evolving needs and degrees of confidence. To improve accountability and facilitate monitoring, the system keeps track of all access attempts and actions through an audit trail.

Because of the system's seamless connection with current infrastructures, it may be used in a variety of real-world settings, including cloud-based data storage, IoT networks, and healthcare data exchange. Considerations for scalability and performance are also made, maximizing the system's effectiveness to manage massive amounts of data streams and the need for real-time processing.

REFERENCES

1. *Song, D., Wagner, D., & Perrig, A. (2000). Practical techniques for searches on encrypted data. In IEEE Symposium on Security and Privacy (S&P).*
2. *Lorch, J. R., Smith, J. M., & Farber, D. J. (2003). Untrusted hosts and confidentiality: Secure program partitioning. In Proceedings of the 9th ACM Conference on Computer and Communications Security (CCS).*
3. *Li, N., Li, T., & Venkatasubramanian, S. (2005). Confidentiality-preserving data mining: A comprehensive survey. In Journal of Computer Science and Technology.*
4. *Li, N., Li, T., & Venkatasubramanian, S. (2007). t-Closeness: Privacy beyond k-anonymity and l-diversity. In IEEE International Conference on Data Engineering (ICDE).*
5. *Blaze, M., Bleumer, G., & Strauss, M. (1998). Divertible protocols and atomic proxy cryptography. In Proceedings of the 5th ACM Conference on Computer and Communications Security (CCS).*
6. *Lu, R., Lin, X., Liang, X., & Shen, X. S. (2013). Secure provenance: The essential of bread and butter of data forensics in cloud computing. In IEEE International Conference on Computer Communications (INFOCOM).*
7. *Bind Schaedler, V., Scherrer, Y., & Buhan, I. (2014). CryptDB: Protecting confidentiality with encrypted query processing. In ACM Symposium on Cloud Computing (SoCC).*
8. *Gentry, C. (2009). A fully homomorphic encryption scheme. In Science, 323(5910), 307-310*
9. *Fischer-Hübner, S., Krasemann, H., & Rannenberg, K. (2003). Privacy-enhancing identity management. In International Workshop on Privacy Enhancing Technologies (PET).*
10. *Damiani, E., di Vimercati, S. D. C., Paraboschi, S., & Samarati, P. (2003). A fine-grained access control system for XML documents. In ACM Transactions on Information and System Security (TISSEC).*