Efficient Data Security System for data sharing inWeb Portal

Nayana M K
Department of Computer Applications
AMC Engineering college
Bangalore, India nayanakumblesh.29@gmail.com

Dr.M.CharlesArockiaraj
Department of Computer ApplicationsAMC Engineering college
Bangalore, India

Abstract

This paper proposes a secure multi-keyword rankedsearch scheme for encrypted cloud data The increasing popularityof cloud computing has prompted data owners to consider outsourcing their data to cloud servers. This trend is primarily driven by the convenience and cost reduction benefits offeredby cloud computing.. However, to maintain privacy, sensitive data needs to be encrypted before outsourcing, which poses challenges for data utilization, such as keyword-based document retrieval. A tree-based index structure is constructed, and a "Greedy Depth-first Search" algorithm is introduced to enable efficient multi-keyword ranked search .In the proposed scheme, a secure kNN (k Nearest Neighbors) algorithm is employed to handle the encryption of index and query vectors while maintaining accurate relevance score calculation between them. The kNN algorithm is a widely used technique for similarity search and retrieval tasks. Statistical attacks refer to techniques where an attacker tries to gain insights or infer information by analyzing statistical patterns or properties of the encrypted data. The special tree-based index structure enables sub-linear search time and flexibility in handling document deletion and insertion operations. The efficiency of the proposed scheme is demonstrated through extensive experiments. By leveraging index construction techniques, query generation methods, and encryp- tion algorithms, the scheme enables data owners to maintainprivacy while still benefiting from the convenience and cost reduction offered by cloud computing.

Key words: *Stray Animals, NGOs, Volunteers, Pets*

I. INTRODUCTION

The increasing need for efficient data security systems has become a critical concern in web portals that facilitate data sharing. Web portals provide a platform for users to exchange and collaborate on various types of data, ranging from personalinformation to sensitive business data. However, the openness and accessibility of web portals also expose data to potential security risks and unauthorized access. The proposed data security system employs a combination of encryption techniques, access control mechanisms, and auditing functionalities to achieve comprehensive data protection. It focuses on three key aspects: confidentiality, integrity, and availability.

Confidentiality is maintained through the use of robust encryption algorithms that encrypt the data before it is stored or transmitted. This ensures that even if unauthorized individ- uals gain access to the data, they cannot decipher its content without the corresponding decryption keys.

Integrity is guaranteed through the implementation of data verification mechanisms. Hash functions and digital signaturesare employed to detect any unauthorized modifications or tampering of the shared data. This helps to maintain the trustworthiness and reliability of the information exchanged through the web portal.

Availability is ensured by incorporating secure access con- trol mechanisms. Users are authenticated and granted appro- priate access privileges based on their roles and responsibili- ties. Fine-grained access control policies are implemented to enforce data access restrictions and prevent unauthorized usersfrom accessing sensitive information.

Additionally, the proposed system includes auditing func- tionalities to track and monitor data activities within the web portal. Comprehensive logs are maintained to capture user ac- tions, data modifications, and access attempts. This facilitates the detection of any suspicious activities and provides an audit trail for forensic investigations if required.

The efficiency of the data security system is a crucial consideration. It aims to strike a balance between robust security measures and the performance requirements of a web portal. The system is designed to minimize the computational overhead and processing time associated with encryption, access control, and auditing operations.

In conclusion, the proposed data security system offers an efficient solution for addressing the security challenges inweb portals facilitating data sharing. By leveraging encryption,access control mechanisms, and auditing functionalities, it ensures the confidentiality, integrity, and availability of shared data while maintaining the system's performance. The subse- quent sections of this paper will provide a detailed explanationof the system's architecture, components, and algorithms, along with experimental results and performance evaluations.

II. LITERATURE SURVEY

1)However, despite its numerous advantages, security and privacy concerns remain major obstacles to the widespread adoption of cloud computing. In this paper, the authors high- light the critical security challenges associated with the public cloud and emphasize the need for extensive research and development of security solutions to establish a trustworthy environment for cloud computing. Given encrypted inputs, the scheme enables the efficient computation of a compact ciphertext that encrypts the result of any efficiently computablefunction. Normally, when you submit a query to a searchengine, the search engine has access to the plaintext queryand can analyze it to provide relevant results. However, with FHE, you can encrypt your query and send it to the search engine, which can then process the encrypted query and returna succinct encrypted answer without ever knowing the actual content of your query. This enables privacy-preserving search functionality, as the search engine cannot deduce the queryor the search terms being used. With this scheme, a search engine can provide a succinct encrypted answer to a user's query without knowing the query itself. allowing the server to retrieve only files that satisfy specific constraints, even withoutbeing able to decrypt the files independently. Moreover, fully homomorphic encryption improves the efficiency of secure multiparty computation. Through recursive self-embedding,the bootstrappable encryption is expanded to achieve fullyhomomorphic encryption. the authors address the problem of searching encrypted data using a public key encryption system.The scenario considered involves a user, Bob, sending anemail to another user, Alice, which is encrypted using Alice's public key. An email gateway needs to determine if the email contains a specific keyword, such as "urgent," in order toroute the email accordingly. However, Alice does not wantto grant the gateway the ability to decrypt all her messages. The PEKS mechanism has broader applications, such as in a scenario where a mail server stores various messages that are publicly encrypted by others for Alice. That's correct. Withthe PEKS mechanism, Alice can send a specific key to the mail server, enabling it to identify all messages containing a specific keyword without compromising the confidentiality of the message contents. This allows for efficient keyword-basedsearching on encrypted data while maintaining data privacy. The subsequent sections of the paper delve into the technical details of the PEKS mechanism and provide further insights into its constructions and properties.

III. EXISTING SYSTEM

Encrypting Data for Outsourcing: One common approachto ensure data confidentiality is to encrypt the data before outsourcing it to a cloud server. These dynamic schemes are crucial as data owners often need to update their data or mod- ify their document collections. By supporting such operations,the schemes ensure that the searchable encryption system remains flexible and adaptable to changing data requirements. Overall, the combination of encrypting data before outsourc- ing and utilizing searchable encryption schemes provides a comprehensive approach to protect data confidentiality while enabling efficient keyword searches on the encrypted data. Theongoing development of dynamic schemes further enhances the usability and practicality of searchable encryption in scenarios where data updates and modifications are common.

IV. PROPOSED SYSTEM

1.Multi-keyword Ranked Search:the supports multi- keyword ranked search, o search for multiple keywords and obtain ranked results based on their relevance. This enables more precise and comprehensive search capabilitiesin encrypted cloud data. 2. Tree-based Index Structure: The system utilizes a tree-based index structure to optimize search efficiency. This index structure allows for sub-linear search time, meaning the search process becomes faster and more efficient. It enables scalable and flexible handling of document insertion and deletion operations within the encrypted cloud data. 3. A document is represented by the weight of that term in the document's vector. and query generation processes

.This combination enhances the accuracy and effectivenessof the multi-keyword ranked search, ensuring relevant results are retrieved based on the relevance scores calculated fromthe index.

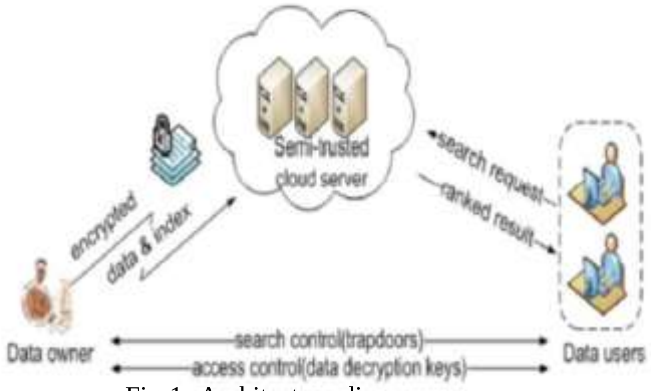
Semi-trusted cloud server
encrypted data & index
search request
ranked result
Data owner
search control(trapdoors)
access control(data decryption keys)
Data users

Fig 1: Architecture diagram

V. RELATED WORK

Access Control and Authentication:Role-Based AccessControl (RBAC): RBAC provides a framework for managing user permissions and access rights based on predefined roles. Access decisions are made based on user roles rather than individual 17 permissions. Attribute-Based Access Control (ABAC): ABAC uses attributes associated with users, resources, and the environment to make access control decisions. It offers fine-grained access control based on various attributes. Two-Factor Authentication (2FA): 2FA adds an extra layer of security by requiring users to provide two different types of authentication factors (e.g., password and a one-time password) to access the system. Data Privacy and Anonymization: Differential Privacy: Differential privacy techniques add noise to query responses to protect individual data privacy while still providing useful aggregate results. Data Anonymization Techniques: Techniques such as k-anonymity, l-diversity, and t-closeness can be appliedto anonymize sensitive data before sharing it in the web portal. Privacy-Preserving Data Mining: Privacy- preserving data mining techniques allow analysis and mining of datawhile preserving the 21 privacy of individual records.

Privacy-Preserving Data Mining: Privacy- AND RESULT preserving data mining techniques allow analysis and mining of data while preserving the 21 privacy of individual records. Audit and Logging: Logging and Monitoring: Implementing comprehensive logging and monitoring mechanisms to track user activities, detect anomalies, and investigate security incidents. Security Information and Event Management (SIEM) systems: SIEM systems collect and analyze security events and logs. Secure Data Transmission and Storage: Secure File Transfer Protocol (SFTP): SFTP provides secure file transfer capabilities, ensuring data integrity and confidentiality during file uploads and downloads. Secure Data Storage: Implementing secure storage mechanisms, such as encrypted databases, to protect data confidentiality and integrity. , you can develop a comprehensive and effective security system to protect sensitive data during sharing and storage.

VI. METHODOLOGY AND RESULT

The following methodology can be considered: System Requirements Analysis: Conduct a thorough analysis of the web portal’s data sharing requirements, including the types of data to be shared, access control needs, encryption requirements, privacy considerations, and compliance requirements. Threat Modeling: Identify potential security threats and risks to the data sharing process, considering factors such as unauthorized access, data breaches, insider threats, and data leakage. Access Control Design: Design an access 30 control mechanism that enforces appropriate user permissions and restrictions based on roles, attributes, or other relevant factors. Implement authentication mechanisms such as RBAC or ABAC to ensure only authorized users 25 can access the data. Utilize differential privacy methods to provide aggregate results while preserving individual data privacy. Audit and Logging: Implement a comprehensive logging and monitoring system to track user activities, detect security incidents, and support forensic investigations. Use SIEM systems to collect and analyze security events and logs. Ensure secure storage mechanisms are in place, such as encrypted databases or file systems, toprotect data at rest. Testing and Evaluation: Conduct rigorous testing of the data security system to verify its effectiveness and identify any vulnerabilities. Perform penetration testing, vulnerability assessments, and security audits to ensure the system’s robustness. Results: The results of implementing an efficient data security system for data sharing in a web portal should include: Enhanced Data Confidentiality: Sensitive data shared through the web portal should remain encrypted during transmission and storage, ensuring confidentiality and protection against unauthorized access. Controlled Access: The implemented access control mechanisms should restrict data access to authorized users based on their roles,

. Compliance: The data security system should adhere to relevant regulations and compliance requirements, such as GDPR or HIPAA, depending on the 20 nature of the shared data. Efficient Performance: The system should provide efficient data sharing capabilities without significant impact on performance, ensuring smooth and timely access to shared data.

VII. CONCLUSION

The key elements include access control mechanisms, en- cryption techniques, data anonymization and privacy preser- vation methods, audit and logging systems, secure data trans- mission and storage protocols, and compliance with relevant regulations. By integrating these elements, organizations can achieve several significant outcomes. Enhanced Data Con- fidentiality: The use of encryption and secure transmission protocols ensures that sensitive data remains confidential and inaccessible to unauthorized entities. Controlled Access: Ac- cess control mechanisms, such as role-based or attribute-basedaccess control, enable organizations to enforce appropriate permissions and restrictions, allowing only authorized users to access specific data. Privacy Preservation: Techniques like data anonymization and differential privacy protect the privacy of individuals and sensitive data, reducing the risk of personally identifiable information (PII) exposure. Compliance with Reg- ulations: By adhering to relevant data protection regulations and industry standards, organizations can demonstrate their commitment to privacy and security, mitigating legal and reputational risks. Auditability and Forensics: Logging and monitoring systems provide a comprehensive audit trail of user activities, facilitating the 15 detection and investigation of security incidents, and enabling the organization to take appropriate measures to mitigate risks. Efficient Performance: Balancing security measures with performance considerations ensures that data sharing operations in the web portal are efficient, minimizing latency and optimizing user experience. organizations can establish trust among users, protect sensitive information, and comply with legal and regulatory require- ments. It fosters a secure data sharing environment, mitigates the risk of data breaches, and safeguards the organization’s reputation. However, it’s important to recognize that data security is an ongoing process that requires continuous monitoring, regular updates, and adaptability to evolving threats. Organizations should regularly assess their security measures, conduct risk assessments, and implement appropriate controls to address newvulnerabilities and emerging risks. In conclu- sion, y. By incorporating the aforementioned elements and maintaining a proactive security posture, organizations canfoster secure data sharing practices and ensure the trust and confidence of their users.

REFERENCES

When it comes to efficient data security systems for data sharing inweb portals there are several references and resources that can provide valuable insights here are a few references you can explore secure data sharing mechanism for web portal by s umarani and m v saravanan international mobile computing paper discusses a secure data sharing mechanism that utilizes cryptography and access control techniques to protect sensitive data in a web portal a secure data sharing frameworkfor web portals by m s abirami and dr s srinivasan this paper presents a framework that incorporates techniques like encryption decryption and digital signatures to ensure secure data sharing in web portals. Privacy-preserving public auditing for secure cloud storage by c.wang q.wang k.ren and w.lou (ieee transactions on computers vol 62 no 2 february 2013) while this paper focuses on storage it discusses privacy- preserving techniques such as public auditing which can be applied to enhance data security in web portals. A secure data sharing model for online social networks by c zhang n cao and y zhang future generation computer systems vol 29 no 8 october 2013 although focused on online social networks this paper proposes a secure data sharing model that employs techniques like data encryption access control and secure queryprocessing these concepts can be applicable to web portal data security as well.