WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Security & Privacy in Mobile Cloud Using Edge Computing

A.SURESH[1], D.RAJESHWARAN[2], E.SIVANESH [3], Ms.N.KANAGADURGA[4]

[1]UG Student, Dept. of CSBS., E.G.S Pillay Engineering College, Nagapattinam, TamilNadu, India
[2]UG Student, Dept. of CSBS., E.G.S Pillay Engineering College, Nagapattinam, TamilNadu, India
[3]UG Student, Dept. of CSBS., E.G.S Pillay Engineering College, Nagapattinam, TamilNadu, India
[4]Assistant Professor, Dept. of CSBS., E.G.S Pillay Engineering College, Nagapattinam, TamilNadu, India

ABSTRACT:

The security of cloud data has become a difficult problem that needs to be solved urgently. Data encryption is an effective means to ensure the security of data in the cloud. The existing Proxy server approaches enable multiple users to perform search operation to delay time process Problem not securely to searching the encrypted data in Overflow of cloud storage. The proposed many of the researchers to be motivated this work under the single data owner setting model and multi-owner data setting model. As Secured Data Encryption Algorithm (SDEA) This Algorithm used to more data are stored in the databases provided by a single cloud service provider and cloud server to perform access securely to searching the data with no cognizance about the real data. Data Access Algorithm (DAA) this algorithm used to easy data searching and access process. Cloud storage large data storing in the process DAA using searching and storage based of cloud encryption decryption process with the rapid development of cloud computing, organization prefers cloud storage services to reduce the overhead of storing data locally, from information retrieval to build a secure searchable index. Thus even though outsourcing data on cloud is inexpensive and reduces long duration storage and maintenance complexity. There is least assurance of data integrity, privacy, safety and availability on cloud servers.

INTRODUCTION :

Cloud Computing is primarily based on proprietary data centers, where hundreds of thousands of dedicated servers are setup to host the cloud services. In addition to the huge number of dedicated servers deployed in data centers, there are billions of underutilized Personal Computers (PCs), usually used only for a few hours per day, owned by individuals and organizations worldwide. The tutorial will review facts, goals and common architectures of mobile cloud computing systems, as well as introduce general mobile cloud services for app developers and marketers. What are the pros and cons of mobile cloud computing for designing apps, tools and infrastructures How does mobile cloud computing relate to improvement of app industry In addition, this tutorial will discuss opportunities and challenges of deploying an online app by cloud computing.

RELATED WORK :

1. Attribute-Based Encryption (ABE): ABE is a type of encryption that allows users to encrypt and decrypt data based on specific attributes rather than specific keys. This can be useful in a multi-user scenario where access control is based on attributes.
2. Homomorphic Encryption: This type of encryption allows computations to be performed on encrypted data without decrypting it first. This is particularly relevant in cloud scenarios where data may need to be processed without exposing the raw information.
3. Proxy Re-Encryption (PRE): PRE allows a third party to transform cipher text from one key to another without accessing the plaintext. This can be used in scenarios where a user wants to delegate access to their data securely.
4. Key Management Schemes: Efficient key management is crucial in multi-user environments. Various schemes, such as hierarchical key management or distributed key management, are explored to ensure secure and efficient access control.
5. Access Control Models: Research often focuses on developing access control models that work well in cloud environments, considering the dynamic nature of users and data sharing requirements.
6. Post-Quantum Cryptography: With the advancement of quantum computing, researchers are exploring cryptographic algorithms that are secure against quantum attacks. This is important for long-term security, especially in cloud storage scenarios where data may be stored for an extended period.

To find specific algorithms or implementations related to your mentioned title, you may want to search academic databases, such as IEEE Xplore, ACM Digital Library, or research repositories like arXiv. Look for recent publications or conference papers in the field of cloud security, encryption, and access control. Additionally, reaching out to experts in the field or checking for updates beyond my last knowledge update may yield more current information.

III. SYSTEM STUDY

3.1 EXISTING SYSTEM

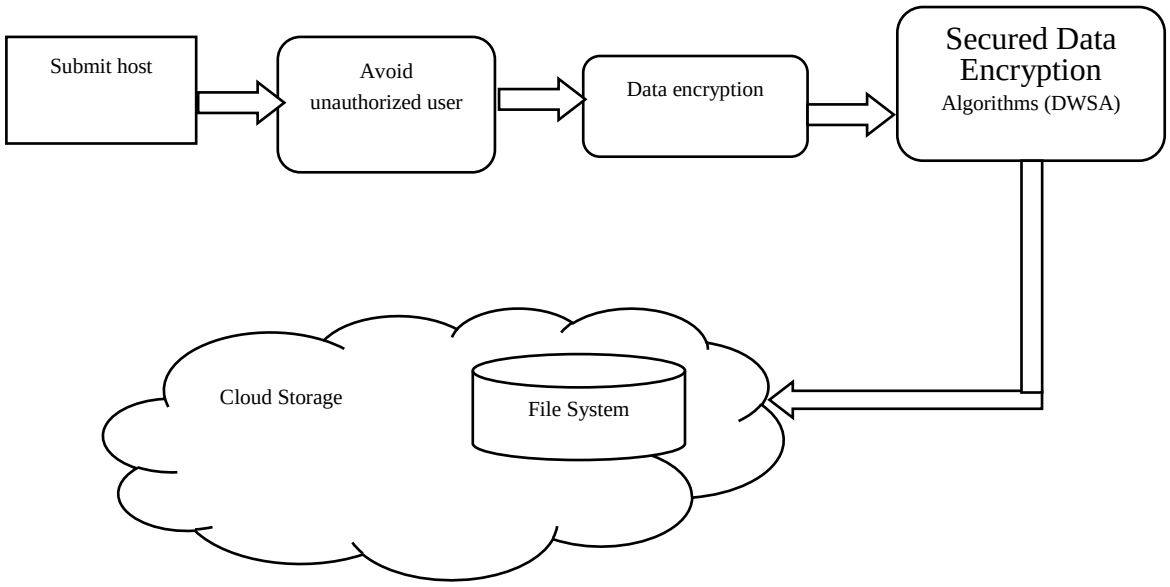
Cloud computing adopts a virtualized, dynamically scalable paradigm for organizing, distributing, and using computing resources. Thus transmission process used to cloud data unauthorized user access and cloud storage data overflow less secure of the cloud process. Moreover, we compare with existing approaches on large datasets and show that this approach reduces the average query communication cost between the authorized user and service provider, as only a single round of communication is required by the proposed approach. Database outsourcing is a popular paradigm of cloud computing.

3.2 PROPOSED SYSTEM

Database outsourcing is a popular paradigm of cloud computing. In this work, we are trying to achieve a balance between data confidentiality at the server and efficient query processing. Further to protect the score information, one-to-many order-preserving mapping techniques has developed and explored the relevance score, from information retrieval to build a secure searchable index. Thus even though outsourcing data on cloud is inexpensive and reduces long duration storage and maintenance complexity. As Secured Data Encryption Algorithm (SDEA) This Algorithm used to more data are stored in the databases provided by a single cloud service provider and cloud server to perform access securely to searching the data with no cognizance about the real data.

3.2.1 Secured Data Encryption Algorithm

Cloud the data and information by the owner and then outsourcing the details to the cloud seems to be good but it leads some Data transmission problem. There may be loss of data and corruption by third party providers. An efficiently implemented and secured data sharing by using the Secured data encryption algorithm used to Cloud data secured and authorized user only access so encryption and decryption. Proposed system used to more data storage user convenient data access and reliable of process. The cloud computing used to authorized user only data access any place access to cloud data avoid to unauthorized user. Security is the critical issue when the user outsources their data to the cloud. Cloud service providers can give unrestricted access of information to the user and controls are required to address the risk of approved user access leading to compromised user data. Thus can be all information secure transmission and secure access of a process so searching duration is less so SEDA algorithm use many problem solved.



IV. SYSTEM DESIGN

4.1 Introduction

The System Design Document describes the system requirements, operating environment, system and subsystem architecture, files and database design, input formats, output layouts, human-machine interfaces, detailed design, processing logic, and external interfaces.

4.2 Project Executive Summary

This section provides a description of the project from a management perspective and an overview of the framework within which the conceptual system design was prepared. If appropriate, include the information discussed in the subsequent sections in the summary.

4.3 System Overview

This section describes the system in narrative form using non-technical terms. It should provide a high-level system architecture diagram showing a subsystem breakout of the system, if applicable. The high-level system architecture or subsystem diagrams should, if applicable, show interfaces to external systems. Supply a high-level context diagram for the system and subsystems, if applicable. Refer to the requirements trace ability matrix (RTM) in the Functional Requirements Document (FRD), to identify the allocation of the functional requirements into this design document.

4.4 Design Constraints

This section describes any constraints in the system design (reference any trade-off analyses conducted such, as resource use versus productivity, or conflicts with other systems) and includes any assumptions made by the project team in developing the system design.

4.5 Software Detailed Design

A software module is the lowest level of design granularity in the system. Depending on the software development approach, there may be one or more modules per system. This section should provide enough detailed information about logic and data necessary to completely write source code for all modules in the system (and/or integrate COTS software programs).
If there are many modules or if the documentation is extensive, place it in an appendix or reference a separate document. Add additional diagrams and information, if necessary, to describe each module, its functionality, and its hierarchy. Industry-standard module specification practices should be followed. Include the following information in the detailed module designs:
A narrative description of each module, its function(s), the conditions under which it is used (called or scheduled for execution), its overall processing, logic, interfaces to other modules, interfaces to external systems, security requirements, etc.; explain any algorithms used by the module in detail
For COTS packages, specify any call routines or bridging programs to integrate the package with the system and/or other COTS packages (for example, Dynamic Link Libraries)Data elements, record structures, and file structures associated with module input and output
Graphical representation of the module processing, logic, flow of control, and algorithms, using an accepted diagramming approach (for example, structure charts, action diagrams, flowcharts, etc.)
Data entry and data output graphics; define or reference associated data elements; if the project is large and complex or if the detailed module designs will be incorporated into a separate document, then it may be appropriate to repeat the screen information in this section

V.FUTURE ENHANCEMENTS:

The future, we will extend our algorithm to support real time Secured Data Encryption and will compare our algorithm with the existing available techniques. Speed of transmission is very low when we are dumping the files into big data. So we need to concentrate about the speed of transmission. As Secured Data Encryption Algorithm (SDEA) This Algorithm used to more data are stored in the databases provided by a single cloud service provider and cloud server to perform access securely to searching the data with no cognizance about the real data.

VI.CONCLUSION:

The presented a Deadline and Budget distribution based Data sending flow and speed improvement correct destination send in the process. We also described workflow partitioning and overall deadline and budget partitioning optimized execution planning and efficient run-time rescheduling.

VII.REFERENCES:

1. Dong H.,"Flux: Overcoming Scheduling Challenges for Exascale Workflows" 2018 IEEE pg.no 10-19.
2. FahimaBhuyan,"ScalableProvenanceStorageandQueryingUsingPigLatinforBigDataWorkflows" 2017 IEEE pg.no 459.
3. Matthew Brehmer,"Matches, Mismatches, and Methods: Multiple-View Workflows for Energy Portfolio Analysis" 2016 IEEE pg.no 1-10.
4. Oliver Ru bel,"Feature-Based Analysis of Plasma-Based Particle Acceleration Data" 2014 IEEE pg.no 196-210.

5. Domenico Talia,"How Distributed Data Mining Tasks can thrive as Knowledge Services" 2010 pg.no 1-6.
6. Christina Hoffa,"On the Use of Cloud Computing for Scientific Workflows" 2014 pg.no 1-7.
7. S. Lohr,"Google and IBM Join in Cloud Computing Research," New York Times, 2007.
8. Giuseppe Agapito "High Performance Analysis of Omics Data" IEEE2017 pg.no 929.
9. Foster, T. Freeman, et al., "Virtual Clusters for Grid Communities," CCGRID, 2006.
10. Foster, R. Figueiredo, et al., "A case for grid computing on virtual machines," ICDCS 2003.
11. K. Keahey, K. Doering, et al., "From sandbox to playground: dynamic virtual environments in the grid," 2004, pp. 34-42.
12. G. B. Berriman, E. Deelman, et al., "Montage: A Grid Enabled Engine for Delivering Custom Science-Grade Mosaics On Demand," in SPIE Conference 5487: 2004.
13. E. Deelman, G. Mehta, et al., "Pegasus: Mapping Large-Scale Workflows to Distributed Resources," in Workflows in eScience, I. Taylor, E. Deelman, et al., Eds.: Springer, 2006.
14. E. Deelman, G. Singh, et al., "The Cost of Doing Science on the Cloud: The Montage Example," in SC'08 Austin, TX2008.
15. P. Barham, B. Dragovic, et al., "Xen and the art of virtualization," ACM SOSP, pp. 164-177, 2003.
16. B. Clark, T. Deshane, et al., "Xen and the art of repeated research," USENIX Annual Technical Conference, FREENIX Track, pp. 135–144, 2004.
17. Norton, D. Vanderster, et al., "Evaluation of Virtual Machines for HEP Grids," Computing in HEP, 2006.
18. C.G.R. Geddes, "Plasma Channel Guided Laser Wakefield Accelerator," PhD dissertation, UC Berkeley, 2005.
19. W.P. Leemans, B., "GeV Electron Beams from a Centimetre-Scale Accelerator," Nature Physics, vol. 2, pp. 696-699, 2006.
20. S.McKenna, Design activity framework for visualization design. IEEE Tran2014 2191–2200.