International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 12
August 2016

EnDAS: Efficient Encrypted Data Search as a Mobile Cloud Service

CHANDRA SEKHAR PATTURU
EmaillId: patturu@gmail.com
CollegeName: SIR C.V RAMAN INSTITUTE OF TECHNOLOGY & SCIENCES Tadipatri, Anantapur (Dist.), A.P.

P.SWATHI
EmailID: swathi.jaya53@gmail.com
Designation: Assistant Prof.
CollegeName: SIR C.V RAMAN INSTITUTE OF TECHNOLOGY & SCIENCES Tadipatri, Anantapur (Dist.),A.P

Abstract— Document storage in the cloud infrastructure is rapidly gaining popularity throughout the world. However, it poses risk to consumers unless the data is encrypted for security. Encrypted data should be effectively searchable and retrievable without any privacy leaks, particularly for the mobile client. Although recent research has solved many security issues, the architecture cannot be applied on mobile devices directly under the mobile cloud environment. This is due to the challenges imposed by wireless networks, such as latency sensitivity, poor connectivity, and low transmission rates. This leads to a long search time and extra network traffic costs when using traditional search schemes. This study addresses these issues by proposing an efficient Encrypted Data Search (EnDAS) scheme as a mobile cloud service. This innovative scheme uses a lightweight trapdoor (encrypted keyword) compression method, which optimizes the data communication process by reducing the trapdoor's size for traffic efficiency. In this study, we also propose two optimization methods for document search, called the Trapdoor Mapping Table (TMT) module and Ranked Serial Binary Search (RSBS) algorithm, to speed the search time. Results show that EnDAS reduces search time by as well as network traffic. The ranked keyword search will return documents to the relevance score. Zero et al. proposed a novel technique that makes the server side carry out the search operation. However, it should send many unrelated documents back and let the user filter them. This is a waste of traffic, which is unsuitable for the mobile cloud. Bowers et all. proposed a distributed cryptographic system that preserved the security of the document retrieval process and the high availability of The system, but this system suffers from two network round trips and calculation complexity for target documents. Wang et al. proposed a single round trip encrypted search scheme, but their system is not secure enough, as it leaks the keyword and associated document information from multiple keyword searches. Li et al. proposed a single-keyword encryption search scheme utilizing ranked keyword search, which network communication between the user and the cloud by transferring the computing burden from the user to the cloud.

INTRODUCTION

SINCE cloud computing can support elastic services and provide an economical use of storage and computation resources, it is rapidly gaining popularity. With powerful cloud services, many data providers can populate their data in clouds instead of directly serving users. The cloud also allows providers to delegate important tasks such as document searches. To protect data security, the documents and their indexes are usually encrypted before outsourcing to the cloud for searches,.When users need to query certain documents, they first send keywords to the original data provider.

The provider then generates encrypted keywords (also called trapdoors) and returns the trapdoors to the user. The user then sends these trapdoors to the cloud. Upon receiving the trapdoors, the Cloud uses a special search algorithm to select a set of desired documents (encrypted) based on the encrypted indexes and given trapdoors. Finally, the user receives these encrypted search results and uses the private key from the provider to decrypt documents. This architecture, as depicted in this system, protects data security while entitling the providers to use both the computation and storage power of the Cloud for document searches. Due to these advantages, this architecture has already been

well-adopted in privacy preserving search systems Mobile devices (e.g. smart phones and tablets) were estimated to surpass two billion growth (0.3 billions for PCs) in the year 2014, which dominates the overall shipment of consumer electronics devices. Nowadays, users heavily utilize mobile devices to request document search services. In general, mobile devices connect to the Internet mainly via wireless networks (WiFi/3G/4G/LTE), which incurs some challenges as compared to traditional wired networks. These challenges include:

1) Latency sensitivity: these wireless networks incur longer network latency, which can slow down a single search request if the search request requires many network round trips. For example, in the traditional design shown in Figure 1, a single search requires three round trips and results in notable latency for wireless communication.

2) Poor connectivity: Mobile devices are normally incapable of maintaining a long-running connection with the Cloud, mostly for energy-saving purposes. Multiple search requests could incur numerous re-connection operations and extra authentication costs.

3) Low network transmission rate: Mobile devices are normally equipped with low-power transmission components, bringing slower transmission rates.

Advantages:

we proposed a novel encrypted search system EnDAS over the mobile cloud, which improves network traffic and search time efficiency compared with the traditional system. We started with a thorough analysis of the traditional encrypted search system and. analyzed its bottlenecks in the mobile cloud: network traffic and search time inefficiency. Then we developed an efficient architecture of EnDAS which is suitable for the mobile cloud to address these issues, where we utilized the TMT module. RSBS algorithm to cope with the inefficient search time issue, while a trapdoor compression method was employed to reduce network traffic costs. Finally our evaluation study experimentally demonstrates the performance advantages of EnDAS

FLOW DIAGRAM

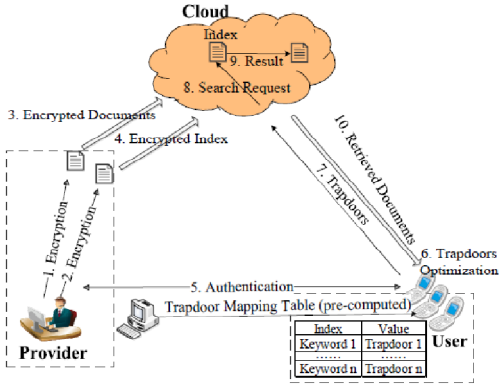

Figure 3. EnDAS system over mobile cloud

IMPLEMENTATION

1.DataUser Module

2.Data Owner Module

3. FileUpload Module Encryption

4. Rank Search Module

5. File Download ModuleDecryption

6. View Uploaded and Downloaded File

1. DataUser Module This module include the user registration login details.

2. Data Owner Module This module helps the owner to register them details and also include login details

3. FileUpload Module This module help the owner to upload his file with encryption using RSA algorithm.This ensure the files to be protected from unauthorized user.

4.Rank Search Module This module ensure the user to search the file that are searched frequently using rank search.

5.File Download Module This module allows the user to download the file using his secret key to decrypt the downloaded data.

4. View Uploaded and Downloaded File This module allows the Owner to view the uploaded files and downloaded files

PRELIMINARY INVESTIGATION

The first and foremost strategy for development of a project starts from the thought of designing a mail enabled platform for a small firm in which it is easy and convenient of sending and receiving messages, there is a search engine ,address book and also including some entertaining games. When it is approved by the organization and our project guide the first activity, ie. preliminary investigation begins. The activity has three parts:

- Request Clarification
- Feasibility Study
- Request Approval

REQUEST CLARIFICATION

After the approval of the request to the organization and project guide, with an investigation being considered, the project request must be examined to determine precisely what the system requires.

Here our project is basically meant for users within the company whose systems can be interconnected by the Local Area Network(LAN). In today's busy schedule man need everything should be provided in a readymade manner. So taking into consideration of the vastly use of the net in day to day life, the corresponding development of the portal came into existence.

FEASIBILITY ANALYSIS

An important outcome of preliminary investigation is the determination that the system request is feasible. This is possible only if it is feasible within limited resource and time. The different feasibilities that have to be analyzed are

- Operational Feasibility
- Economic Feasibility
- Technical Feasibility

Operational Feasibility

Operational Feasibility deals with the study of prospects of the system to be developed. This system operationally eliminates all the tensions of the Admin and helps him in effectively tracking the project progress. This kind of automation will surely reduce the time and energy, which previously consumed in manual work. Based on the study, the system is proved to be operationally feasible.

Economic Feasibility

Economic Feasibility or Cost-benefit is an assessment of the economic justification for a computer based project. As hardware was installed from the beginning & for lots of purposes thus the cost on project of hardware is low. Since the system is a network based, any number of employees connected to the LAN within that organization can use this tool from at anytime. The Virtual Private Network is to be developed using the existing resources of the organization. So the project is economically feasible.

Technical Feasibility

According to Roger S. Pressman, Technical Feasibility is the assessment of the technical resources of the organization. The organization needs IBM compatible machines with a graphical web browser connected to the Internet and Intranet. The system is developed for platform Independent environment. Java Server Pages, JavaScript, HTML, SQL server and WebLogic Server are used to develop the system. The technical feasibility has been carried out. The system is technically feasible for development and can be developed with the existing facility.

4.3.3 REQUEST APPROVAL

Not all request projects are desirable or feasible. Some organization receives so many project requests from client users that only few of them are pursued. However, those projects that are both feasible and desirable should be put into schedule. After a project request is approved, it cost, priority, completion time and personnel requirement is estimated and used to determine where to add it to any project list. Truly speaking, the approval of those above factors, development works can be launched.

SYSTEM DESIGN AND DEVELOPMENT

INPUT DESIGN

Input Design plays a vital role in the life cycle of software development, it requires very careful attention of developers. The input design is to feed data to the application as accurate as possible. So inputs are supposed to be designed effectively so that the errors occurring while feeding are minimized. According to Software Engineering Concepts, the input forms or screens are designed to provide to have a validation control over the input limit, range and other related validations.

This system has input screens in almost all the modules. Error messages are developed to alert the user whenever he commits some mistakes and guides him in the right way so that invalid entries are not made. Let us see deeply about this under module design. Input design is the process of converting the user created input into a computer-based format. The goal of the input design is to make the data entry logical and free from errors. The error is in the input are controlled by the input design. The application has been developed in user-friendly manner. The forms have been designed in such a way during the processing the cursor is placed in the position where must be entered. The user is also provided with in an option to select an appropriate input from various alternatives related to the field in certain cases. Validations are required for each data entered. Whenever a user enters an erroneous data, error message is displayed and the user can move on to the subsequent pages after completing all the entries in the current page

OUTPUT DESIGN

The Output from the computer is required to mainly create an efficient method of communication within the company primarily among the project leader and his team members, in other words, the administrator and the clients. The output of VPN is the system which allows the project leader to manage his clients in terms of creating new clients and assigning new projects to them, maintaining a record of the project validity and providing folder level access to each client on the user side depending on the projects allotted to him. After completion of a project, a new project may be assigned to the client. User authentication procedures are maintained at the initial stages itself. A new user may be created by the administrator himself or a user can himself register as a new user but the task of assigning projects and validating a new user rests with the administrator only. The application starts running when it is executed for the first time. The server has to be started and then the internet explorer in used as the browser. The project will run on the local area network so the server machine will serve as the administrator while the other connected systems can act as the clients. The developed system is highly user friendly and can be easily understood by anyone using it even for the first time.

SYSTEM TESTING

TESTING METHODOLOGIES

The following are the Testing Methodologies:

Unit Testing.

Integration Testing.

User Acceptance Testing.

Output Testing.

Validation Testing.

Unit Testing

Unit testing focuses verification effort on the smallest unit of Software design that is the module. Unit testing exercises specific paths in a module's control structure to

ensure complete coverage and maximum error detection. This test focuses on each module individually, ensuring that it functions properly as a unit. Hence, the naming is Unit Testing.

During this testing, each module is tested individually and the module interfaces are verified for the consistency with design specification. All important processing path are tested for the expected results. All error handling paths are also tested.

Integration Testing

Integration testing addresses the issues associated with the dual problems of verification and program construction. After the software has been integrated a set of high order tests are conducted. The main objective in this testing process is to take unit tested modules and builds a program structure that has been dictated by design.

The following are the types of Integration Testing:

1. Top Down Integration

This method is an incremental approach to the construction of program structure. Modules are integrated by moving downward through the control hierarchy, beginning with the main program module. The module subordinates to the main program module are incorporated into the structure in either a depth first or breadth first manner.

In this method, the software is tested from main module and individual stubs are replaced when the test proceeds downwards.

2. Bottom-up Integration

This method begins the construction and testing with the modules at the lowest level in the program structure. Since the modules are integrated from the bottom up, processing required for modules subordinate to a given level is always available and the need for stubs is eliminated. The bottom up integration strategy may be implemented with the following steps:

The low-level modules are combined into clusters into clusters that perform a specific Software sub-function.

A driver (i.e.) the control program for testing is written to coordinate test case input and output.

The cluster is tested.

Drivers are removed and clusters are combined moving upward in the program structure

The bottom up approaches tests each module individually and then each module is module is integrated with a main module and tested for functionality.

User Acceptance Testing

User Acceptance of a system is the key factor for the success of any system. The system under consideration is tested for user acceptance by constantly keeping in touch with the prospective system users at the time of developing and making changes wherever required. The system developed provides a friendly user interface that can easily be understood even by a person who is new to the system.

Output Testing

After performing the validation testing, the next step is output testing of the proposed system, since no system could be useful if it does not produce the required output in the specified format. Asking the users about the format required by them tests the outputs generated or displayed by the system under consideration. Hence the output format is considered in 2 ways – one is on screen and another in printed format.

Validation Checking

Validation checks are performed on the following fields.

Text Field:

The text field can contain only the number of characters lesser than or equal to its size. The text fields are alphanumeric in some tables and alphabetic in other tables. Incorrect entry always flashes and error message.

Numeric Field:

The numeric field can contain only numbers from 0 to 9. An entry of any character flashes an error messages. The individual modules are checked for accuracy and what it has to perform. Each module is subjected to test run along with sample data. The individually tested modules are integrated into a single system. Testing involves executing the real data information is used in the program the existence of any program defect is inferred from the output. The testing should be planned so that all the requirements are individually tested.

A successful test is one that gives out the defects for the inappropriate data and produces and output revealing the errors in the system.

Preparation of Test Data

Taking various kinds of test data does the above testing. Preparation of test data plays a vital role in the system testing. After preparing the test data the system under study is tested using that test data. While testing the system by using test data errors are again uncovered and corrected by using above testing steps and corrections are also noted for future use.

Using Live Test Data:

Live test data are those that are actually extracted from organization files. After a system is partially constructed, programmers or analysts often ask users to key in a set of data from their normal activities. Then, the systems person uses this data as a way to partially test the system. In other instances, programmers or analysts extract a set of live data from the files and have them entered themselves.

It is difficult to obtain live data in sufficient amounts to conduct extensive testing. And, although it is realistic data that will show how the system will perform for the typical processing requirement, assuming that the live data entered are in fact typical, such data generally will not test all combinations or formats that can enter the system. This bias toward typical values then does not provide a true systems test and in fact ignores the cases most likely to cause system failure.

Using Artificial Test Data:

Artificial test data are created solely for test purposes, since they can be generated to test all combinations of formats and values. In other words, the artificial data, which can quickly be prepared by a data generating utility program in the information systems department, make possible the testing of all login and control paths through the program.

The most effective test programs use artificial test data generated by persons other than those who wrote the programs. Often, an independent team of testers formulates a testing plan, using the systems specifications.The package "Virtual Private Network" has satisfied all the requirements specified as per software requirement specification and was accepted.

The Comparison of Search Time Breakdown (U as User, P as Provider, C as Cloud)

Overall Search Process	Traditional (ms)	EnDAS (ms)
Authentication	55.52	55.61
Transmitting a Keywor	28.27	N/A
Building a Trapdoor	174.42	109.79
Transmitting a	44.77	N/A
Transmitting	42.68	25.73
Searching	69.44	17.21
Documents Retrieval	90.78	87.45
TotalSearch Time	505.88	295.79

CONCLUSION

In this work, we proposed a novel encrypted search system EnDAS over the mobile cloud, which improves network traffic and search time efficiency compared with the traditional system. We started with a thorough analysis of the traditional encrypted search system and analyzed its bottlenecks in the mobile cloud: network traffic and search time inefficiency. Then we developed an efficient architecture of EnDAS which is suitable for the mobile cloud to address these issues, where we utilized the TMT module and the RSBS algorithm to cope with the inefficient search time issue, while a trapdoor compression method was employed to reduce network traffic costs. Finally our evaluation study experimentally demonstrates the performance advantages of EnDAS.

REFERENCES

[1] D. Huang, "Mobile cloud computing," IEEE COMSOC Multimedia Commun. Tech. Committee (MMTC) E-Letter, vol. 6, no. 10, pp. 27– 31, 2011.

[2] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data," in Proc. Int. Conf. Comput. Commun. (INFOCOM), Apr. 2011, pp. 829–837.

[3] C. Wang, N. Cao, K. Ren, and W. Lou, "Enabling secure and efficient ranked keyword search over outsourced cloud data," IEEE Trans. Parallel Distrib. Systems, vol. 23, no. 8, pp. 1467–1479, 2012.

[4] C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, "Secure ranked keyword search over encrypted cloud data," in Proc. IEEE Int. Conf. Distrib. Comput. Syst. (ICDCS), Jun. 2010, pp. 253–262.

[5] C. Gentry and S. Halevi, "Implementing gentrys fullyhomomorphic encryption scheme," in Advances in Cryptology– EUROCRYPT 2011, 2011, pp. 129–148.

[6] C. O¨ rencik and E. Savas¸, "Efficient and secure ranked multikeyword search on encrypted cloud data," in Proc. Joint EDBT/ICDT Workshops, Mar. 2012, pp. 186–195.

[7] Gartner, "Worldwide traditional pc, tablet, ultramobile and mobile phone shipments on pace to

grow 7.6 percent in 2014," http://www.gartner.com/newsroom/id/2645115.

[8] Trellian, "Keywords number," http://www.keyworddiscovery. com/keyword-stats.html?date=2014-03-01.

[9] V. Rijmen and J. Daemen, "Advanced encryption standard," Federal Information Processing Standard, pp. 19–22, 2001.

[10] X. Lai, "On the design and security of block ciphers," Ph.D. dissertation, Diss. Techn. Wiss ETH Z¨ urich, Nr. 9752, 1992. Ref.: JL Massey; Korref.: H. B¨ uhlmann, 1992.

[11] K. Nyberg, "Fast accumulated hashing," in Proc. Int. Workshop Fast Softw. Encryption (FSE), Feb. 1996, pp. 83–87.

[12] Nyberg and Kaisa, "Commutativity in cryptography," in Proc. Int. Workshop Funct. Anal., 1995.

[13] J. Benaloh and M. De Mare, "One-way accumulators: A decentralized alternative to digital signatures," in Advances in Cryptology-EUROCRYPT 1993, 1994, pp. 274–285.

[14] C. O¨ rencik and E. Savas¸, "An efficient privacy-preserving multikeyword search over encrypted cloud data with ranking," Distrib. Parallel Databases, vol. 32, no. 1, pp. 119–160, Mar. 2014.

[15] P. Wang, H. Wang, and J. Pieprzyk, "An efficient scheme of common secure indices for conjunctive keyword-based retrieval on encrypted data," pp. 145–159, 2009.