ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering
(IJARMATE) Vol. 3, Special Issue 11, March 2017

AN EFFICIENT TRAITOR TRACING USING KERNEL BASED MINING WITH SIGNATURE AUTHENTICATION

S.Kruthik kshama[1], E.Nandakumar M.E.,(Ph.D)[2] M.Arulprakash M.Tech.,

[1]*Department of Computer Science, Sri Subramanya College of Engineering and Technology, Palani*

[23]*Department of Computer Science, Sri Subramanya College of Engineering and Technology, Palani*

[1]*divyakarthika5@gmail.com*

Abstract : *we address this issue using a new system model with anomaly detection, tracing revoking traitors. This cryptosystem provides two security mechanisms, traitor tracing and revocation, to support efficient digital forensics. Here we use RSA signature scheme for authenticating authorized user verification. In this paper kernel based mining used for tracing the traitors in the cloud sharing. This attack requires only accessibility to a few data entries within the organizations rather than requiring the encrypted administrative privileges typically found in the distribution of data mining scenarios. To the best of our knowledge , we are the first to explore this new insider threat in DKBDM the security and performance analysis shows that our construction is threshold provably secure and has following features : dynamic joining amnd revoking users , constant size cipher texts and decryption keys, lower overloads for large scale systems.*

Keywords : *identity based encryption , attribute based encryption,cloud stack.*

1. Introduction

Data-breaching problems related to insider attacks are one of the fastest growing attack types. According to the ``2015 Verizon Data Breach Investigations Report," attacks from ``insider misuse" have risen significantly, from 8% in 2013 to 20.6% in 2015. This near-triple rate of increase is astonishing when one considers that this rise has taken place over a span of only two years. As a result of this rapid increase, insider attacks are now among the top three types of data breaches. Insider attacks arise not from system security errors but from staff inside the company's enterprise data security circles. Thus, insider attacks, because of this lack of technical barriers, are simple to carry out successfully. For example, in a single 10-minute phone call to an enterprise chain store, a nontechnical employee can provide enough data to a potential attacker for that attacker to execute a virtual attack or worse an impersonation. One call is all it takes for the system to crumble.

A company may spend huge sums of hard-earned capital to find technical solutions to protect its perimeter yet still find it difficult to prevent an insider attack. Many data mining applications store huge amounts of per-sonal information; therefore, extensive research has primarily focused on dealing with potential privacy breaches. One prime area of research in preserving privacy is the Sup-port Vector

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering
(IJARMATE) Vol. 3, Special Issue 11, March 2017

Machine (SVM). SVM is a very popular data mining methodology used mainly with the kernel trick to map data into a higher dimensional feature space as well as maintain archives with better mining precision results. With privacy protection in mind, Vaidya et al. provided a state-of-the-art privacy-preserving distributed SVM scheme to securely merge kernels. Their proposal encoded and hid the kernel values in a noisy mixture during transmission such that the original data cannot be recovered even if these distributed organizations colluded.

Security is a problem that must be considered for deploying a file syncing-and-sharing service. Several recent surveys show that 88% potential cloud consumers worry about the privacy of their data, and security is often cited as the top obstacle for cloud adoption. At first, the multi-tenant nature of the cloud is vulnerable to data leaks, threats, and malicious attacks. Therefore, it is important for enterprises to have strong access control policies (such as Role-based Access Control (RBAC) or Attribute-based Access Control (ABAC)) in place to maintain the privacy and confidentiality of data for collaboration with teams. Sometimes cloud providers have access to the data stored in the cloud, and can control access to it by outside entities. When this is the case, the challenge is to maintain the confidentiality of data and limiting privileged user access to it. This can be achieved by encrypting the data before storing it in the cloud, and enforcing legal agreements and contractual obligations with the cloud service provider to ensure protection of data.

On the other hand, the protection of decoders is also becoming increasingly important due to huge potential commercial value of data stored in cloud. Compared with the traditional cryptographic technique, the encryption system used by the decoders should be a group-oriented cryptosystem that supports a large number of users. Considering openness of cloud environment and complexity of management for a large amount of users, it may also give rise to some new security risks in this group-oriented cryptosystem. For example, the redistribution of traitor's decoder, the forgery of decoder with a colluded decryption key, and the privilege attacks with changing and forging the role/identity key. Therefore, it is very necessary for the FSS service to provide the functionality of digital forensics.

As with more traditional computer forensics investigations, any form of encryption places a large burden on the forensics investigation and increases the complexity of the investigation. Related to encrypted data, a forensic analysis mechanism should be proposed within cloud environment to guide investigations, which is flexible enough to be able to work with future providers offering new services. There have been some work focused on this proposal from two aspects of traitor tracing and revocation based on key fingerprint in suspected decryption box. In the Fig. 2, the tracing algorithm can still identify at least one particular key (whose holder is called traitor) used for building the suspected decryption device. And then the revocation mechanism might ensure the normal running by revoking the right of the seized traitors.

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering
(IJARMATE) Vol. 3, Special Issue 11, March 2017

1. System Analysis

1.1 Existing System

For a large-scale group-oriented communication, broadcast encryption was first considered in 1991 and, subsequently, formally defined by Fiat and Naor in 1994. Since then, it has become one attractive topic in cryptography community. In symmetric-key setting, only trusted system designer can broadcast data to the receivers. However, the public-key scheme, first introduced by Bonehet al. in 1999, can publish a short public key, which enables anybody to broadcast data, thus overcome the deficiency of symmetric key setting. Also, However, these work did not take into account the hierarchy structure. Boneh and Franklin proposed the first fully identity-based encryption (IBE) in 2001, in which the public key can be an arbitrary string such as an email address. Unfortunately, IBE does not support broadcast function unless some members can share the same private-key when they hold the same identity. According to this idea, Boneh et al. provided a hierarchical identity-based encryption (HIBE) system to support an organizational hierarchy, but this kind of hierarchy must be a tree structure and cannot provide identity-based revocation and tracing due to the global sharing of hierarchical identity/privacy-key for all users. In addition, attribute-based encryption (ABE) is also considered as an effective group communication method, but the existing ABE schemes have not yet been able to support the hierarchical structure.

While it is challenging to enforce digital forensics analysis, Boneh and Waters introduced augmented broadcast encryption that is efficient for constructing traitor-tracing, and trace-and-revoke systems. The scheme is resistant to an arbitrary number of colluders and secure against adaptive adversaries. Attrapadung and Imai proposed a new cryptosystem, called Broadcast ABE (BABE), with direct revocation mechanism. Garg et al. presented a trace-and-revoke scheme based on prime order bilinear groups, and provided the first implementations of efficient fully collusion-resilient traitor tracing scheme. Liu et al. also presented a blackbox traceable ABE that achieves the traceability in $O(\sqrt{n})$,where nis the number of users in the system. There have been some cryptosystems constructed on the partial order relation. Kimet al. proposed a new key management system for multilevel security using various one-way functions in 2005. Chunget al proposed a hierarchy method based on the elliptic curve cryptosystem and one-way hash function to solve dynamic access problems in 2008. Another related field ishierarchical key management with time control. For example, Tzeng proposed a time-bound scheme based on Lucas function in 2002, but it is insecure against collusion attacks by Yi and Ye. Another similar schemes based on the tamper-resistant device and the hash function were proposed by Chien in 2004 and Bertino et al. in 2008, respectively. Santiset al.summarized and provided several provably-secure hierarchical key assignment schemes based on an existing schemes in 2007. Peeret al also propose an interesting method to represent data in multiple resolutions with each resolution secured with a different key in 1014. In all, these work cannot support common access control and digital forensics,

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering
(IJARMATE) Vol. 3, Special Issue 11, March 2017

but their techniques are worth learning for our construction.

Disadvantages

- These work did not take into account the hierarchy structure.
- The existing ABE schemes have not yet been able to support the hierarchical structure.
- In all, these work cannot support common access control and digital forensics, but their techniques are worth learning for our construction.

1.2 Proposed System

FSS service: provides users with the ability to remotely store their data and access the same cloud-based data. Enterprise or business class versions of FSS services provide these capabilities in a secure manner that gives IT oversight and control.
Online player/editor: provides the ability to access this data from any location and any of their devices, including smart-phones and tablets, without having to go through a corporate VPN or firewall (shown in the middle module in the figure).
End users: The FSS service also provide the ability to share information with other users, both inside and outside the organization.

This kind of FSS service could be built on the open-source cloud platforms, such as, OpenStack and CloudStack 1, in which computing, networking and storage resources are integrated and managed as a unified system. These platforms provide a prefect interface with cloud service providers and tenants, but do not provide a direct interface with end users. As a more flexible and convenient way, online player/editor is developed as the bridge between FSS service and end users. They may be built a lot of different ways, such as web service, virtual desktop, and client/server-based applications.

First, we will illustrate in detail the privacy breach scenario through an example. There are three roles: the SVM server, hospitals (organizations), and patients (members of organization). The SVM server provides the SVM service, which builds a global SVM model and performs classification. Organizations in this example are represented by three hospitals, which store their patient records separately. Organizations such as hospitals apply an SVM service to their data for data analysis. Some of the members are labeled as patients, while others consist of staff including doctors and nurses, each of whom has a part of the overall patient data records. Some members are insiders, who may then collude with outsiders to launch attacks. For example, a member within an organization such as an irresponsible doctor may sell patient records to outsiders. In such a situation, the semi-trusted SVM server acts as an outside attacker, attempting to acquire the entire private patient data with the help of the portion of the patients' records already obtained from the doctor.

There are three players in the investigated threat scenario:

1. Data Owners—Organizations or Clients: These organizations own the data and can be trusted. In a distributed computing environment, they may also participate in data mining tasks.

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering
(IJARMATE) Vol. 3, Special Issue 11, March 2017

2. Insiders: Members within the data owner's organization are semi-trusted. They may leak their own data to outsiders. The insiders leak nothing but the data content. For example, the data indices do not need to be leaked.

3. Outsider: The entity does not belong to the data owner's organization. This group is semi-trusted and may collude with insiders. In a distributed environment, the data mining server, which coordinates sharing among the different subset of affiliate groups, may act as a potential outsider. This outsider (e.g. data mining server) knows the parameters of the mining data, but does not have access to the data content because that has been packed into a kernel format.

Advantages

- Our PHE construction also supports the revocation mechanism not only for the groups but also for the users along with key hierarchy.
- Our PHE scheme provides several new secure features, such as public user label, constant-size user key storage, fast tracing, lower computational costs and communication bandwidths.
- Our cryptosystem also takes full advantage of RBAC, which provides a well-designed and easy-to-manage approach for accessing cloud resources without user intervention.

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com
International Journal of Advanced Research in Management, Architecture, Technology and Engineering
(IJARMATE) Vol. 3, Special Issue 11, March 2017

3. System Design

3.1 Flow diagram

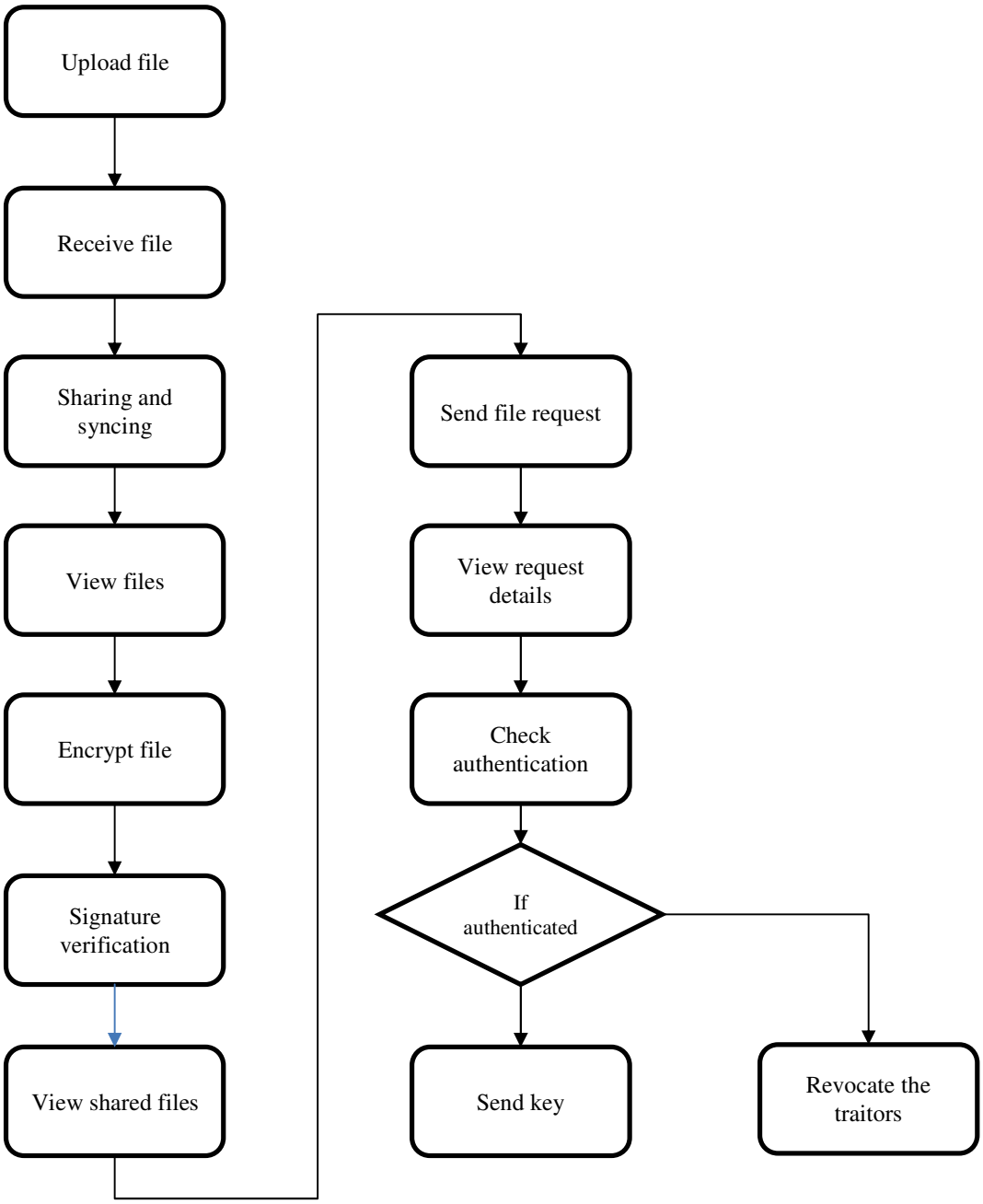
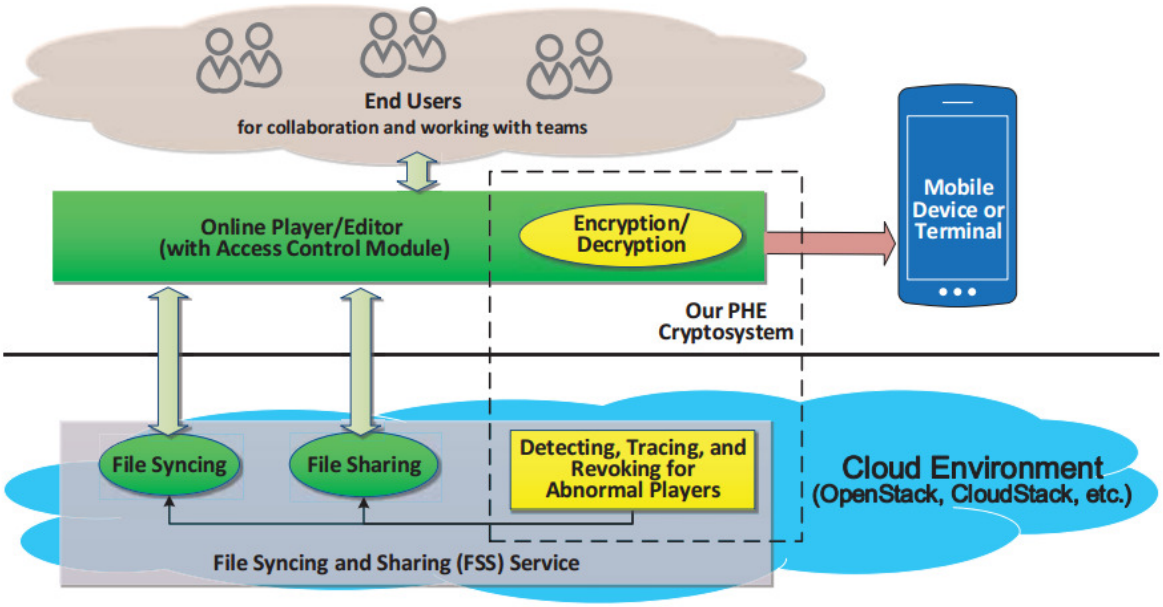


Fig 3.1 Flow Diagram

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com
International Journal of Advanced Research in Management, Architecture, Technology and Engineering
(IJARMATE) Vol. 3, Special Issue 11, March 2017

3.2. System Architecture



3.2 System Architecture

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com
International Journal of Advanced Research in Management, Architecture, Technology and Engineering
(IJARMATE) Vol. 3, Special Issue 11, March 2017

3.3 Use case diagram

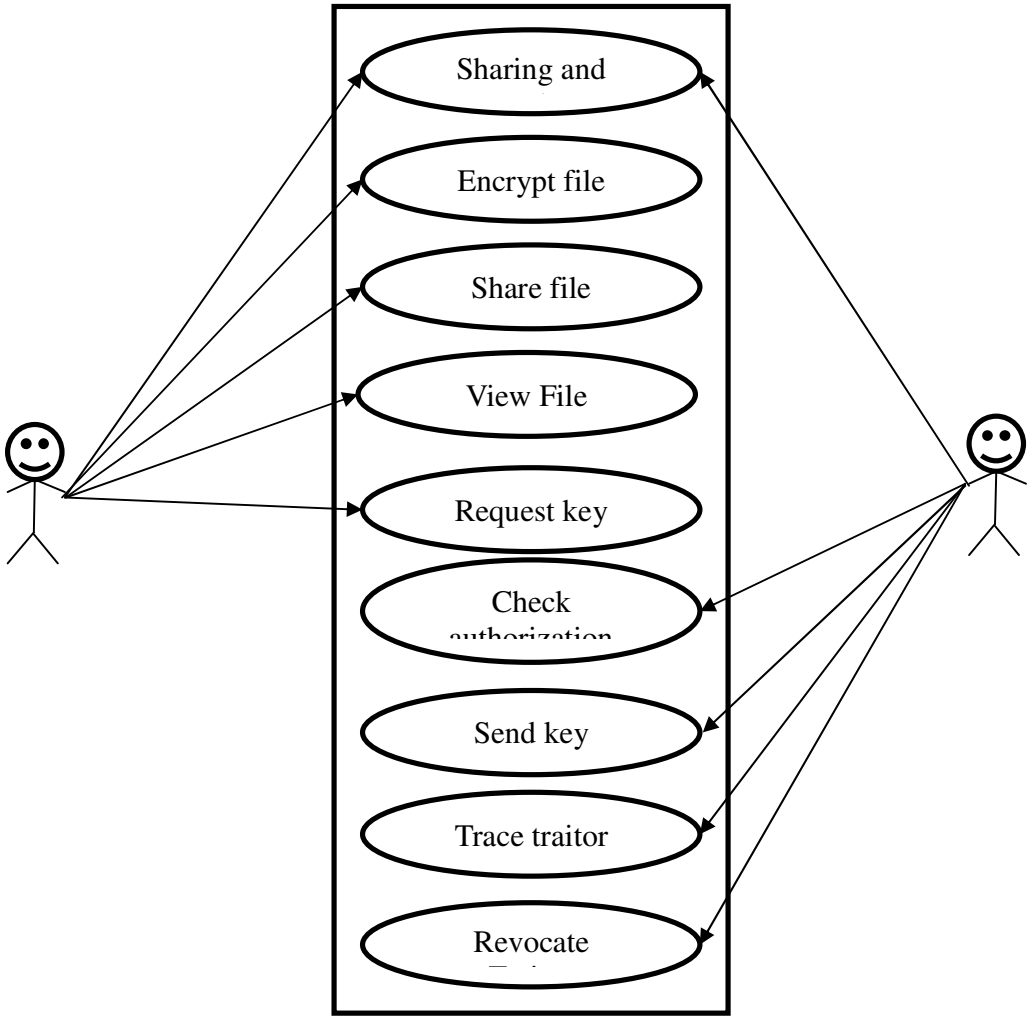


Fig 3.3 Use Case Diagram

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com
International Journal of Advanced Research in Management, Architecture, Technology and Engineering
(IJARMATE) Vol. 3, Special Issue 11, March 2017

3.4 Class Diagram

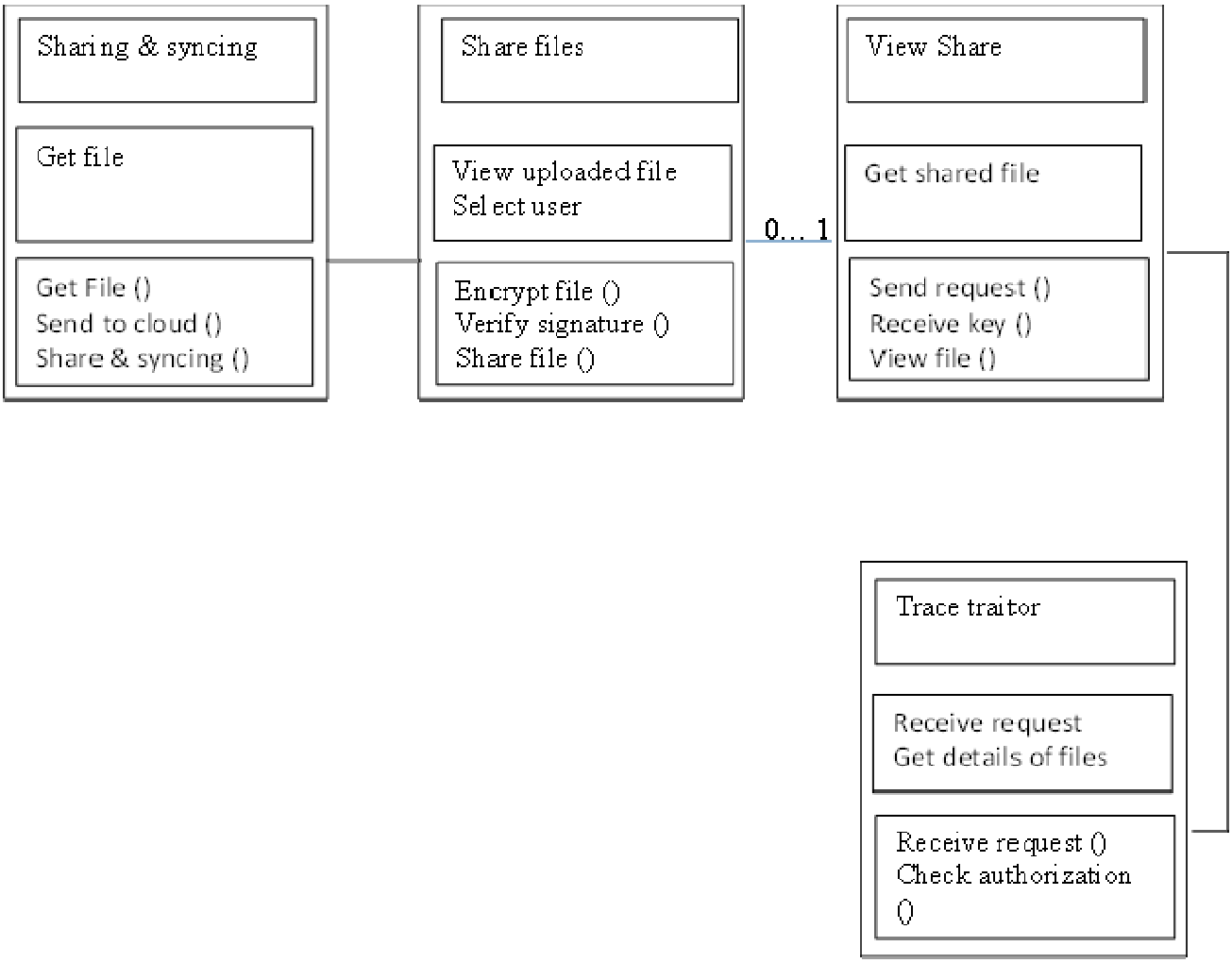


Fig 3.4 Class Diagram

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com
International Journal of Advanced Research in Management, Architecture, Technology and Engineering
(IJARMATE) Vol. 3, Special Issue 11, March 2017

3.5 Sequence diagram

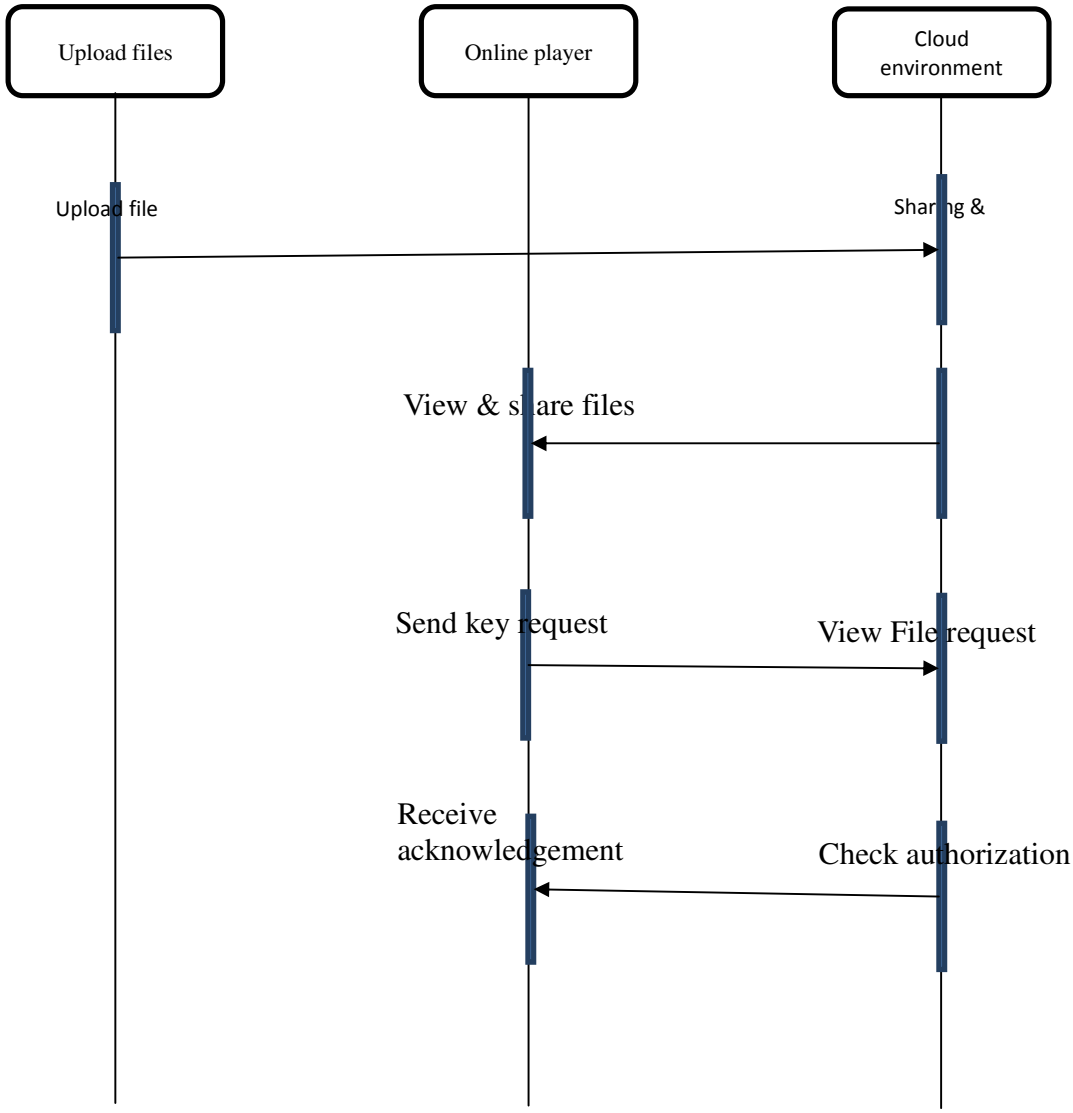


Fig 3.5 Sequence Diagram

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com
International Journal of Advanced Research in Management, Architecture, Technology and Engineering
(IJARMATE) Vol. 3, Special Issue 11, March 2017

4. System Testing

System testing is the stage of implementation, which aimed at ensuring that system works accurately and efficiently before the live operation commence. Testing is the process of executing a program with the intent of finding an error. A good test case is one that has a high probability of finding an error. A successful test is one that answers a yet undiscovered error.

Testing is vital to the success of the system. System testing makes a logical assumption that if all parts of the system are correct, the goal will be successfully achieved. The candidate system is subject to variety of tests-on-line response, Volume Street, recovery and security and usability test. A series of tests are performed before the system is ready for the user acceptance testing. Any engineered product can be tested in one of the following ways. Knowing the specified function that a product has been designed to from, test can be conducted to demonstrate each function is fully operational. Knowing the internal working of a product, tests can be conducted to ensure that "al gears mesh", that is the internal operation of the product performs according to the specification and all internal components have been adequately exercised.

4.1 Types of Testing

4.1.1 Unit Testing

Unit testing is the testing of each module and the integration of the overall system is done. Unit testing becomes verification efforts on the smallest unit of software design in the module. This is also known as 'module testing'. The modules of the system are tested separately. This testing is carried out during the programming itself. In this testing step, each model is found to be working satisfactorily as regard to the expected output from the module. There are some validation checks for the fields. For example, the validation check is done for verifying the data given by the user where both format and validity of the data entered is included. It is very easy to find error and debug the system.

4.1.2 Integration Testing

Data can be lost across an interface, one module can have an adverse effect on the other sub function, when combined, may not produce the desired major function. Integrated testing is systematic testing that can be done with sample data. The need for the integrated test is to find the overall system performance. There are two types of integration testing. They are:

i) Top-down integration testing.
ii) Bottom-up integration testing.

4.1.3 White Box Testing

White Box testing is a test case design method that uses the control structure of the procedural design to drive cases. Using the white box testing methods, we derived test cases that

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com
International Journal of Advanced Research in Management, Architecture, Technology and Engineering
(IJARMATE) Vol. 3, Special Issue 11, March 2017

guarantee that all independent paths within a module have been exercised at least once.

4.1.4 Black Box Testing

- Black box testing is done to find incorrect or missing function
- Interface error
- Errors in external database access
- Performance errors
- Initialization and termination errors

In 'functional testing', is performed to validate an application conforms to its specifications of correctly performs all its required functions. So this testing is also called 'black box testing'. It tests the external behavior of the system. Here the engineered product can be tested knowing the specified function that a product has been designed to perform, tests can be conducted to demonstrate that each function is fully operational.

4.1.5 Validation Testing

After the culmination of black box testing, software is completed assembly as a package, interfacing errors have been uncovered and corrected and final series of software validation tests begin validation testing can be defined as many, but a single definition is that validation succeeds when the software functions in a manner that can be reasonably expected by the customer.

4.1.6 User Acceptance Testing

User acceptance of the system is the key factor for the success of the system. The system under consideration is tested for user acceptance by constantly keeping in touch with prospective system at the time of developing changes whenever required.

4.1.7.Output Testing

After performing the validation testing, the next step is output asking the user about the format required testing of the proposed system, since no system could be useful if it does not produce the required output in the specific format. The output displayed or generated by the system under consideration. Here the output format is considered in two ways. One is screen and the other is printed format. The output format on the screen is found to be correct as the format was designed in the system phase according to the user needs. For the hard copy also output comes out as the specified requirements by the user. Hence the output testing does not result in any connection in the system.

5. System Implementation

Implementation of software refers to the final installation of the package in its real environment, to the satisfaction of the intended users and the operation of the system. The people are not sure that the software is meant to make their job easier.

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering
(IJARMATE) Vol. 3, Special Issue 11, March 2017

- The active user must be aware of the benefits of using the system
- Their confidence in the software built up
- Proper guidance is impaired to the user so that he is comfortable in using the application

Before going ahead and viewing the system, the user must know that for viewing the result, the server program should be running in the server. If the server object is not running on the server, the actual processes will not take place.

5.1 User Training

To achieve the objectives and benefits expected from the proposed system it is essential for the people who will be involved to be confident of their role in the new system. As system becomes more complex, the need for education and training is more and more important.

Education is complementary to training. It brings life to formal training by explaining the background to the resources for them. Education involves creating the right atmosphere and motivating user staff. Education information can make training more interesting and more understandable.

5.2 Training on the Application Software

After providing the necessary basic training on the computer awareness, the users will have to be trained on the new application software. This will give the underlying philosophy of the use of the new system such as the screen flow, screen design, type of help on the screen, type of errors while entering the data, the corresponding validation check at each entry and the ways to correct the data entered. This training may be different across different user groups and across different levels of hierarchy.

5.3 Operational Documentation

Once the implementation plan is decided, it is essential that the user of the system is made familiar and comfortable with the environment. A documentation providing the whole operations of the system is being developed. Useful tips and guidance is given inside the application itself to the user. The system is developed user friendly so that the user can work the system from the tips given in the application itself.

5.4 System Maintenance

The maintenance phase of the software cycle is the time in which software performs useful work. After a system is successfully implemented, it should be maintained in a proper manner. System maintenance is an important aspect in the software development life cycle. The need for system maintenance is to make adaptable to the changes in the system environment. There may be social, technical and other environmental changes, which

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com
International Journal of Advanced Research in Management, Architecture, Technology and Engineering
(IJARMATE) Vol. 3, Special Issue 11, March 2017

affect a system which is being implemented. Software product enhancements may involve providing new functional capabilities, improving user displays and mode of interaction, upgrading the performance characteristics of the system. So only thru proper system maintenance procedures, the system can be adapted to cope up with these changes. Software maintenance is of course, far more than "finding mistakes".

5.4.1 Corrective Maintenance

The first maintenance activity occurs because it is unreasonable to assume that software testing will uncover all latent errors in a large software system. During the use of any large program, errors will occur and be reported to the developer. The process that includes the diagnosis and correction of one or more errors is called Corrective Maintenance.

5.4.2 Adaptive Maintenance

The second activity that contributes to a definition of maintenance occurs because of the rapid change that is encountered in every aspect of computing. Therefore Adaptive maintenance termed as an activity that modifies software to properly interfere with a changing environment is both necessary and commonplace.

5.4.3 Perceptive Maintenance

The third activity that may be applied to a definition of maintenance occurs when a software package is successful. As the software is used, recommendations for new capabilities, modifications to existing functions, and general enhancement are received from users. To satisfy requests in this category, Perceptive maintenance is performed. This activity accounts for the majority of all efforts expended on software maintenance.

5.4.4 Preventive Maintenance

The fourth maintenance activity occurs when software is changed to improve future maintainability or reliability, or to provide a better basis for future enhancements. Often called preventive maintenance, this activity is characterized by reverse engineering and re-engineering techniques.

6 Modules

1. Sharing & syncing
2. Share files
3. Access Share files
4. Tracing Traitor

6. Module description

6.1 Sharing & syncing

- In this module organization upload files with some authorization.
- Select File and send to cloud environment
- Receive file with sharing & syncing in cloud environment.

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com
International Journal of Advanced Research in Management, Architecture, Technology and Engineering
(IJARMATE) Vol. 3, Special Issue 11, March 2017

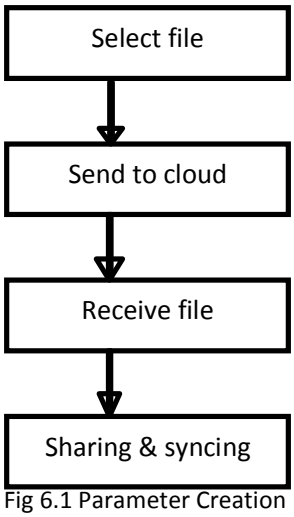
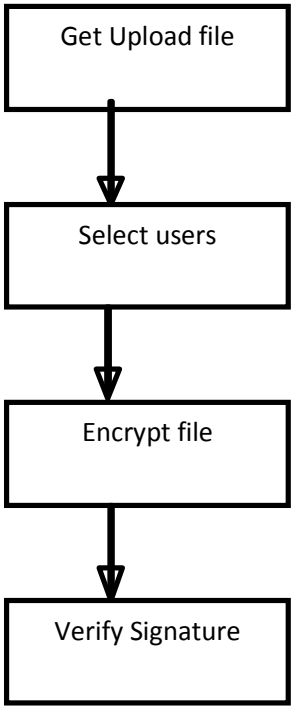


Fig 6.1 Parameter Creation

6.2 Share file

- This module design for user usage purpose.
- Get upload files in the cloud and select the file.
- Select the users to share the files.

- Encrypt the selected file and share the file in the cloud with signature verification.



ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com
International Journal of Advanced Research in Management, Architecture, Technology and Engineering
(IJARMATE) Vol. 3, Special Issue 11, March 2017

6.3Access share files

- View the shared files in this module.
- Select any file and send request to the cloud environment.
- Receive key and decrypt the file.

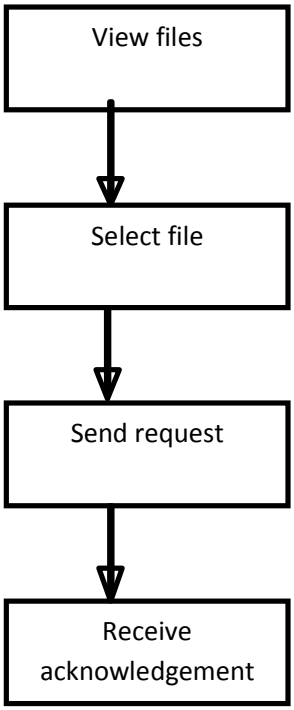


Fig 6.3 access share file

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com
International Journal of Advanced Research in Management, Architecture, Technology and Engineering
(IJARMATE) Vol. 3, Special Issue 11, March 2017

6.4 Tracing Traitor

- In this module receive players request and view the request details.
- Also view file details using the request information.
- Check the authorization request, if authorized then send key to the user.
- If it is unauthorized user then assign the shared user as traitor and revocate the traitor user.

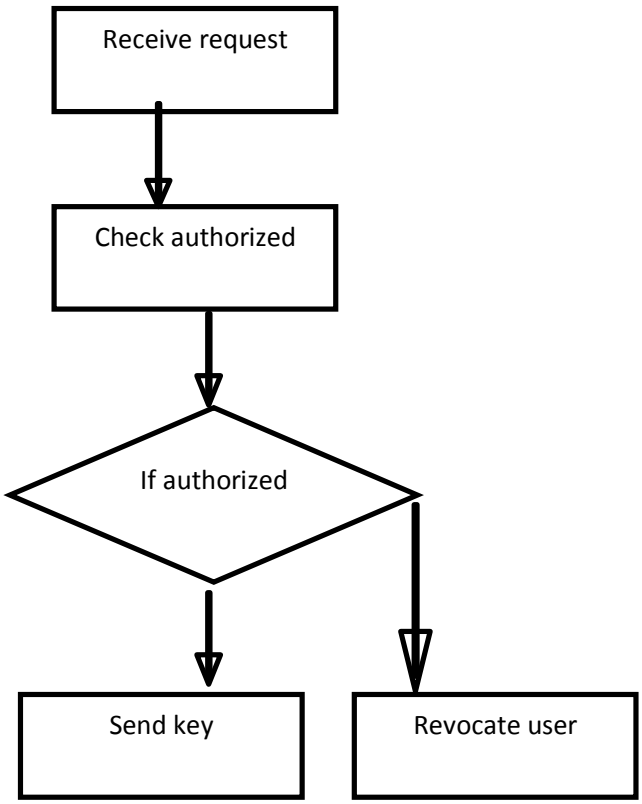


Fig 6.4 tracing traitors

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering
(IJARMATE) Vol. 3, Special Issue 11, March 2017

7 SYSTEM REQUIREMENTS

7.1 Software Requirements

- O/S : Windows XP.
- Languag : Java.
- IDE : Net Beans 6.9.1
- Data Base : MySQL

7.2 Hardware Requirements

- System : Pentium IV 2.4 GHz
- Hard Disk : 160 GB
- Monitor : 15 VGA color
- Mouse : Logitech.
- Keyboard : 110 keys enhanced
- Ram : 2GB

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering
(IJARMATE) Vol. 3, Special Issue 11, March 2017

7.4 Java

Java is a programming language originally developed by James Gosling at Sun Microsystems (now a subsidiary of Oracle Corporation) and released in 1995 as a core component of Sun Microsystems' Java platform. The language derives much of its syntax from C and C++ but has a simpler object model and fewer low-level facilities. Java applications are typically compiled to byte code (class file) that can run on any Java Virtual Machine (JVM) regardless of computer architecture. Java is a general-purpose, concurrent, class-based, object-oriented language that is specifically designed to have as few implementation dependencies as possible. It is intended to let application developers "write once, run anywhere." Java is currently one of the most popular programming languages in use, particularly for client-server web applications.

7.5 Java Platform

One characteristic of Java is portability, which means that computer programs written in the Java language must run similarly on any hardware/operating-system platform. This is achieved by compiling the Java language code to an intermediate representation called Java byte code, instead of directly to platform-specific machine code. Java byte code instructions are analogous to machine code, but are intended to be interpreted by a virtual machine (VM) written specifically for the host hardware.

End-users commonly use a Java Runtime Environment (JRE) installed on their own machine for standalone Java applications, or in a Web browser for Java applets. Standardized libraries provide a generic way to access host-specific features such as graphics, threading, and networking.

A major benefit of using byte code is porting. However, the overhead of interpretation means that interpreted programs almost always run more slowly than programs compiled to native executables would. Just-in-Time compilers were introduced from an early stage that compiles byte codes to machine code during runtime.

Just as application servers such as Glass Fish provide lifecycle services to web applications, the Net Beans runtime container provides them to Swing applications. All new shortcuts should be registered in "Key maps/Net Beans" folder. Shortcuts installed INS Shortcuts folder will be added to all key maps, if there is no conflict. It means that if the same shortcut is mapped to different actions in Shortcut folder and current key map folder (like Key map/Net Beans), the Shortcuts folder mapping will be ignored.

* Database Explorer Layer API in Database Explorer

* Loaders-text-dB schema-Actions in Database Explorer

* Loaders-text-sql-Actions in Database Explorer

* Plug-in Registration in Java EE Server Registry

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering
(IJARMATE) Vol. 3, Special Issue 11, March 2017

The keyword public denotes that a method can be called from code in other classes, or that a class may be used by classes outside the class hierarchy. The class hierarchy is related to the name of the directory in which the .java file is located.

The keyword static in front of a method indicates a static method, which is associated only with the class and not with any specific instance of that class. Only static methods can be invoked without a reference to an object. Static methods cannot access any class members that are not also static. The keyword void indicates that the main method does not return any value to the caller. If a Java program is to exit with an error code, it must call System. Exit () explicitly.

The method name "main" is not a keyword in the Java language. It is simply the name of the method the Java launcher calls to pass control to the program. Java classes that run in managed environments such as applets and Enterprise JavaBeans do not use or need a main () method. A Java program may contain multiple classes that have main methods, which means that the VM needs to be explicitly told which class to launch from.

The Java launcher launches Java by loading a given class (specified on the command line or as an attribute in a JAR) and starting its public static void main(String[]) method. Stand-alone programs must declare this method explicitly. The String [] args parameter is an array of String objects containing any arguments passed to the class. The parameters to main are often passed by means of a command line.

7.6 Java a High-level Language

A high-level programming language developed by Sun Microsystems. Java was originally called OAK, and was designed for handheld devices and set-top boxes. Oak was unsuccessful so in 1995 Sun changed the name to Java and modified the language to take advantage of the burgeoning World Wide Web.

Java source code files (files with a .java extension) are compiled into a format called byte code (files with a .class extension), which can then be executed by a Java interpreter. Compiled Java code can run on most computers because Java interpreters and runtime environments, known as Java Virtual Machines (VMs). Byte code can also be converted directly into machine language instructions by a just-in-time compiler (JIT).

Java is a general purpose programming language with a number of features that make the language well suited for use on the World Wide Web. Small Java applications are called Java applets and can be downloaded from a Web server and run on your computer by a Java-compatible Web browser, such as Netscape Navigator or Microsoft Internet Explorer.

Object-Oriented Software Development using Java: Principles, Patterns, and Frameworks contain a much applied focus that develops skills in designing software-particularly in writing well-designed, medium-sized object-oriented programs. It provides a broad and coherent coverage of object-oriented technology, including object-oriented

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering
(IJARMATE) Vol. 3, Special Issue 11, March 2017

modeling using the Unified Modeling Language (UML) object-oriented design using Design Patterns, and object-oriented programming using Java.

7.7 Net Beans

The **Net Beans Platform** is a reusable framework for simplifying the development of Java Swing desktop applications. The Net Beans IDE bundle for Java SE contains what is needed to start developing Net Beans plug-in and Net Beans Platform based applications; no additional SDK is required.

Applications can install modules dynamically. Any application can include the Update Center module to allow users of the application to download digitally-signed upgrades and new features directly into the running application.

The platform offers reusable services common to desktop applications, allowing developers to focus on the logic specific to their application. Among the features of the platform are:

- User interface management (e.g. menus and toolbars)
- User settings management
- Storage management (saving and loading any kind of data)
- Window management
- Wizard framework (supports step-by-step dialogs)
- Net Beans Visual Librar

7.8 J2EE

A **Java EE application** or a **Java Platform, Enterprise Edition application** is any deployable unit of Java EE functionality. This can be a single Java EE module or a group of modules packaged into an EAR file along with a Java EE application deployment descriptor.

Enterprise applications can consist of the following:

- EJB modules (packaged in JAR files);
- Web modules (packaged in WAR files);
- connector modules or resource adapters (packaged in RAR files);
- Session Initiation Protocol (SIP) modules (packaged in SAR files);
- application client modules
- Additional JAR files containing dependent classes or other components required by the application;

7.9 Wamp Server

WAMPs are packages of independently-created programs installed on computers that use a Microsoft Windows operating system.

Apache is a web server. MySQL is an open-source database. PHP is a scripting language that can manipulate information held in a database and generate web pages dynamically each time content is requested by a browser. Other programs may also be included in a package, such as phpMyAdmin which provides a graphical user interface for the MySQL database manager, or the alternative scripting languages Python or Perl.

7.10 MySQL

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com
International Journal of Advanced Research in Management, Architecture, Technology and Engineering
(IJARMATE) Vol. 3, Special Issue 11, March 2017

The MySQL development project has made its source code available under the terms of the GNU General Public License, as well as under a variety of proprietary agreements. MySQL was owned and sponsored by a single for-profit firm, the Swedish company MySQL AB, now owned by Oracle Corporation.

Free-software-open source projects that require a full-featured database management system often use MySQL. Applications which use MySQL databases include: TYPO3, Joomla, WordPress, phpBB, Drupal and other software built on the LAMP software stack.

7.11 Platforms and interfaces

Many programming languages with language-specific APIs include libraries for accessing MySQL databases. These include MySQL Connector/Net for integration with Microsoft's Visual Studio (languages such as C# and VB are most commonly used) and the JDBC driver for Java. In addition, an ODBC interface called MyODBC allows additional programming languages that support the ODBC interface to communicate with a MySQL database, such as ASP or ColdFusion. The MySQL server and official libraries are mostly implemented in ANSI C/ANSI C++.

7.12 FEASIBILITY STUDY

The feasibility study is carried out to test whether the proposed system is worth being implemented. The proposed system will be selected if it is best enough in meeting the performance requirements.

The feasibility carried out mainly in three sections namely.

• Economic Feasibility

• Technical Feasibility

• Behavioral Feasibility

Economic Feasibility

Economic analysis is the most frequently used method for evaluating effectiveness of the proposed system. More commonly known as cost benefit analysis. This procedure determines the benefits and saving that are expected from the system of the proposed system. The hardware in system department if sufficient for system development.

Technical Feasibility

This study center around the system's department hardware, software and to what extend it can support the proposed system department is having the required hardware and software there is no question of increasing the cost of implementing the proposed system. The criteria, the proposed system is technically feasible and the proposed system can be developed with the existing facility.

Behavioral Feasibility

People are inherently resistant to change and need sufficient amount of training, which would result in lot of expenditure for the organization. The proposed system can generate reports with day-to-

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com
International Journal of Advanced Research in Management, Architecture, Technology and Engineering
(IJARMATE) Vol. 3, Special Issue 11, March 2017

day information immediately at the user's request, instead of getting a report, which doesn't contain much detail.

8 System Implementation

Implementation of software refers to the final installation of the package in its real environment, to the satisfaction of the intended users and the operation of the system. The people are not sure that the software is meant to make their job easier.

- The active user must be aware of the benefits of using the system
- Their confidence in the software built up
- Proper guidance is impaired to the user so that he is comfortable in using the application

Before going ahead and viewing the system, the user must know that for viewing the result, the server program should be running in the server. If the server object is not running on the server, the actual processes will not take place.

8.1 User Training

To achieve the objectives and benefits expected from the proposed system it is essential for the people who will be involved to be confident of their role in the new system. As system becomes more complex, the need for education and training is more and more important. Education is complementary to training. It brings life to formal training by explaining the background to the resources for them. Education involves creating the right atmosphere and motivating user staff. Education information can make training more interesting and more understandable.

8.2 Training on the Application Software

After providing the necessary basic training on the computer awareness, the users will have to be trained on the new application software. This will give the underlying philosophy of the use of the new system such as the screen flow, screen design, type of help on the screen, type of errors while entering the data, the corresponding validation check at each entry and the ways to correct the data entered. This training may be different across different user groups and across different levels of hierarchy.

8.3 Operational Documentation

Once the implementation plan is decided, it is essential that the user of the system is made familiar and comfortable with the environment. A documentation providing the whole operations of the system is being developed. Useful tips and guidance is given inside the application itself to the user. The system is developed user friendly so that the

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com
International Journal of Advanced Research in Management, Architecture, Technology and Engineering
(IJARMATE) Vol. 3, Special Issue 11, March 2017

user can work the system from the tips given in the application itself.

9 Conclusion

We propose SOTS for trustworthy resource matchmaking across multiple clouds. We have shown that SOTS yields very good results in many typical cases. How-ever, there are still some open issues we can apply to the cur-rent scheme. First, we are interested in combining our trust scheme with reputation management to address concerns in users' feedback. A universal measurement and quantitative method to assess the security levels of a resource is another interesting direction. Evaluation of the proposed scheme in a larger-scale multiple cloud environments is also an important task to be addressed in future research.

10 References

[1] F. R. Institute, "Personal data in the cloud: A global survey of consumer attitudes," http://www.fujitsu.com/downloads/SOL/fai/ reports/fujitsu/personal-data-in-thecloud.pdf, 2010.

[2] D. Quick and K. R. Choo, "Google drive: Forensic analysis of data remnants,"J. Network and Computer Applications, vol. 40, pp. 179–193, 2014.

[3] H. Chung, J. Park, S. Lee, and C. Kang, "Digital forensic investigation of cloud storage services,"Digital Investigation, vol.9,no.2,pp. 81–95, 2012.

[4] D. Boneh and M. K. Franklin, "An efficient public key traitor tracing scheme," in CRYPTO, 1999, pp. 338–353.

[5] D.Boneh,A.Sahai,andB.Waters,"Fully collusion resistant traitor tracing with short ciphertexts and private keys," inEUROCRYPT,2006, pp. 573–592.

[6] Z.Liu,Z.Cao,andD.S.Wong,"TraceableCP-ABE:howtotrace decryption devices found in the wild,"IEEE Trans. Information Forensics and Security, vol. 10, no. 1, pp. 55–68, 2015.

[7] D.BonehandM.K.Franklin,"Identity-basedencryptionfromthe weil pairing," inCRYPTO, 2001, pp. 213–229.

[8] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in EUROCRYPT, 2005, pp. 457–473.

[9] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in ACM Conference on CCS, 2006, pp. 89–98.

[10] R. Ostrovsky, A. Sahai, and B. Waters, "Attribute-based encryption with non-monotonic access structures," inACM Conference on Computer and Communications Security, 2007, pp. 195–203.

[11] S. Yamada, N. Attrapadung, G. Hanaoka, and N. Kunihiro, "Generic constructions for chosen-ciphertext secure attribute based encryption," inPublic Key Cryptography, 2011, pp. 71–89.

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering
(IJARMATE) Vol. 3, Special Issue 11, March 2017

[12] M. J. Atallah, M. Blanton, N. Fazio, and K. B. Frikken, "Dynamic and efficient key management for access hierarchies,"ACM Trans. Inf. Syst. Secur., vol. 12, no. 3, 2009.

[13] M. Blanton and K. B. Frikken, "Efficient multi-dimensional key management in broadcast services," inESORICS, 2010, pp. 424–440.

[14] D. Boneh, X. Boyen, and E.-J. Goh, "Hierarchical identity based encryption with constant size ciphertext," inAdvances in Cryptology (EUROCRYPT'2005), vol. 3494 of LNCS, 2005, pp. 440–456.

[15] S. Berkovits, "How to broadcast a secret," in Advances in Cryptology (EUROCRYPT'91), vol. 547 of LNCS. springer-verlag, 1991, pp. 536–541.

[16] A. Fiat and M. Naor, "Broadcast encryption," in Advances in Cryptology (CRYPTO'93), vol. 773 of LNCS. springer-verlag, 1994, pp. 480–491.

[17] D. Boneh, X. Boyen, and E.-J. Goh, "Hierarchical identity based encryption with constant size ciphertext," in Advances in Cryptology (EUROCRYPT'05), vol. 3494 of LNCS, http://eprint.iacr.org/2005/015, 2005, pp. 440–456.

[18] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," inIEEE Symposium on Security and Privacy, 2007, pp. 321–334.

[19] D. Boneh and B. Waters, "A fully collusion resistant broadcast, trace, and revoke system," in ACM Conference on Computer and Communications Security, 2006, pp. 211–220.

[20] N. Attrapadung and H. Imai, "Conjunctive broadcast and attribute-based encryption," inPairing-Based Cryptography - Pairing 2009, Third International Conference, Palo Alto, CA, USA, August 12-14, 2009, Proceedings, 2009, pp. 248–265.

[21] S. Garg, A. Kumarasubramanian, A. Sahai, and B. Waters, "Building efficient fully collusion-resilient traitor tracing and revocation schemes," inProceedings of the 17th ACM Conference on Computer and Communications Security, CCS 2010, Chicago, Illinois, USA, October 4-8, 2010, 2010, pp. 121–130.

[22] S. Akl and P. Taylor, "Cryptographic solution to a multilevel security problem," inAdvances in Cryptology (CRYPTO'82), 1982, pp. 237–249.

[23] H. Kim, B. Park1, J. Ha, B. Lee, and D. Park, "New key management systems for multilevel security," inICCSA 2005, vol. 3481 of LNCS, 2005, pp. 245–253.

[24] Y. Chung, H. Lee, F. Lai, and T. Chen, "Access control in user hierarchy based on elliptic curve cryptosystem,"Information Sciences, vol. 178, pp. 230–243, 2008.

[25] W. Tzeng, "A time-bound cryptographic key assignment scheme for access control in a hierarchy," IEEE Trans. on Knowledge and Data Engineering, vol. 14, no. 1, pp. 182–188, 2002.

[26] X. Yi and Y. Ye, "Security of tzeng's time-bound key assignment scheme for access

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering
(IJARMATE) Vol. 3, Special Issue 11, March 2017

control in a hierarchy,"IEEE Trans. Knowl. Data Eng., vol. 15, no. 4, pp. 1054–1055, 2003.

[27] H. Chien, "Efficient time-bound hierarchical key assignment scheme,"IEEE Trans. on Knowledge and Data Engineering,vol.16, no. 10, pp. 1301–1304, 2004.

[28] E. Bertino, N. Shang, and S. Wagstaff, "An efficient time-bound hierarchical key management scheme for secure broadcasting," IEEE Trans. on Dependable and Secure Computing,vol.5,no.2,pp. 65–70, 2008.

[29] A.D.Santis,A.L.Ferrara,and B.Masucci,"Efficientprovablysecure hierarchical key assignment schemes," inMFCS, 2007, pp. 371–382.

[30] C. D. Peer, D. Engel, and S. B. Wicker, "Hierarchical key management for multi-resolution load data representation," in2014 IEEE International Conference on Smart Grid Communications, SmartGridComm 2014, Venice, Italy, November 3-6, 2014, 2014, pp. 926–932.

[31] N. Provos, M. Friedl, and P. Honeyman, "Preventing privilege escalation," inProceedings of the 12th USENIX Security Symposium, Washington, D.C., USA, August 4-8, 2003, 2003.

[32] L. S. Liu, R. Moulic, and D. G. Shea, "Cloud service portal for mobile device management," inIEEE 7th International Conference on e-Business Engineering, ICEBE 2010, Shanghai, China, November 10-12, 2010, 2010, pp. 474–478.

[33] Y. Chen and B. Malin, "Detection of anomalous insiders in collaborative environments via relational analysis of access logs," in Proceedings of the First ACM Conference on Data and Application Security and Privacy,ser.CODASPY'11. NewYork,NY,USA: ACM, 2011, pp. 63–74.

[35] T. Asano, "Reducing receiver's storage in cs, sd and lsd broadcast encryption schemes,"IEICE Trans. on Fundamentals of Electronics, Communications and Computer Sciences, vol. 88, no. 1, pp. 203–210, 2005.

[36] D. Halevy and A. S. A, "The lsd broadcast encryption scheme," in Advances in Cryptology (Crypto'2002), vol. 2442 of LNCS. springerverlag, 2002, pp. 47–60.

[37] K. Ogawa, G. Hanaoka, and H. Imai, "Content and key management to trace traitors in broadcasting services," inSecurity and Trust Management - 11th International Workshop, STM 2015, Vienna, Austria, September 21-22, 2015, Proceedings, 2015, pp. 236–252.

[38] O. Goldreich,Foundations of Cryptography Volume II, Basic Application. Cambridge University Press, 2004.

[39] W.-G. Tzeng and Z.-J. Tzeng, "A public-key traitor tracing scheme with revocation using dynamic shares," inPublic Key Cryptography, 2001, pp. 207–224.

[40] E.F.Brickell,D.M.Gordon,K.S.McCurley,andD.B.Wilson, "Fast exponentiation

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering
(IJARMATE) Vol. 3, Special Issue 11, March 2017

with precomputation (extended abstract)," in EUROCRYPT, 1992, pp. 200–207.

[41] J. Demmel and P. Koev, "The accurate and efficient solution of a totally positive generalized vandermonde linear system,"SIAM J. Matrix Anal. Appl, vol. 27, pp. 142–152, 2005.