INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 3 ISSUE 3 (2017) PAGES 2426 - 2431
RECEIVED : 25.04.2017 PUBLISHED : 29.05.2017
May 29, 2017

EFFECTIVE AND EXPRESSIVE KEYWORD SEARCH OVER HASHED VALUES

R.Meena[1], J. Sujatha[2],
[1]PG Scholar, Department of MCA., Arulmigu Meenakshi Amman College of Engineering, Anna University, Vadamavandal (near kanchipuram), India,
[2]Associate Professor, Department of MCA., Arulmigu Meenakshi Amman College of Engineering, Anna University, Vadamavandal, India.

ABSTRACT

When Data owners are up-loading their confidential data's in cloud the risk factor is increased, when users are searching for any document if their search terms are matched with the content of confidential data's the data's are displayed to the users to avoid this issue in our proposed system, if data owners are uploading a file at that time they need to give a set of keywords to upload the file at that time the key words will be converted to the hash values. If data owners need to down their file they should enter their set of keywords which they have given at the time of uploading their file if the key words are matched the corresponding file will be displayed and if they need to download the file a verification key will be send to their registered mail after matching the verification key the file will be downloaded.In this application, to upload a file they should be register first and after the registration process they need to login to upload their files while they are uploading their files it will ask for keywords at that time they need to give a set of keywords relevant to the uploading file after finishing certain credentials the keywords will be converted to hash values, once the keywords are have been changed to hash values the file will be uploaded successfully .Then if they need to download the file in the future means they need to login and enter the keyword in the search box, if the setoff keywords matched their requested document means the document will be displayed and if they click the download link means a OTP will be send to their mail-id they need to enter that OTP in the textbox if the OTP matched means the selected file will be downloaded.

Key Words: OTP, System, Data Owner, Link**.**

1. INTRODUCTION

This project is based upon hashing the keywords when the keywords are have been hashed it cannot be read by any users based upon the keywords only the files are searched and displayed to the particular users. If the keyword doesn't match the files will not be displayed to the user. Searchable encryption allows a cloud server to conduct keyword search over encrypted data on behalf of the data users without learning the underlying plaintexts. However, most existing searchable encryption schemes only support single or conjunctive keyword search, while a few other schemes that are able to perform expressive keyword search are computationally inefficient since they are built from bilinear pairings over the

composite-order groups.

In this paper, we propose an expressive public-key searchable encryption scheme in the prime-order groups, which allows keyword search policies (i.e., predicates, access structures) to be expressed in conjunctive, disjunctive or any monotonic Boolean formulas and achieves significant performance improvement over existing schemes. We formally define its security, and prove that it is selectively secure in the standard model. Also, we implement the proposed scheme using a rapid prototyping tool called Charm, and conduct several experiments to evaluate it performance. The results demonstrate that our scheme is much more efficient than the ones built over the composite-order groups.

MVC

The Model-View-Controller (MVC) is an architectural pattern that separates an application into three main logical components: the model, the view, and the controller. Each of these components are built to handle specific development aspects of an application. MVC is one of the most frequently used industry-standard web development framework to create scalable and extensible projects.

MVC Components:

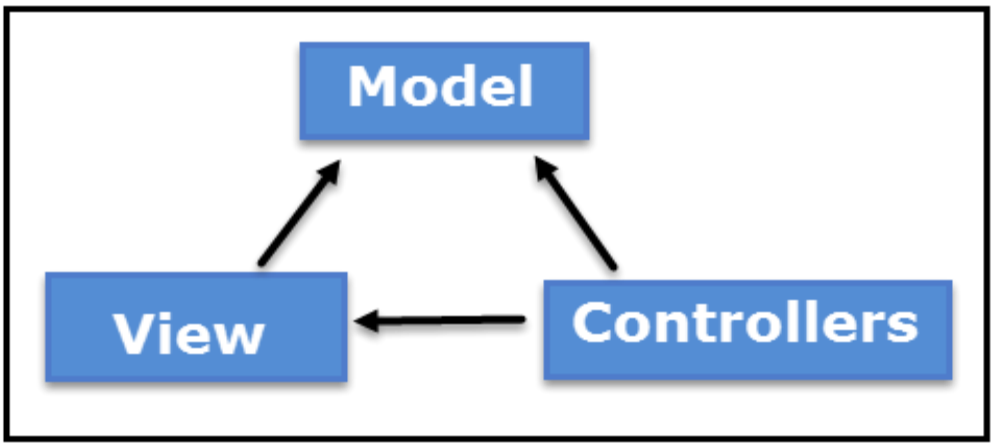
Model: The Model component corresponds to all the data related logic that the user works with. This can represent either the data that is being transferred between the View and Controller components or any other business logic related data. For example, a Customer object will retrieve the customer information from the database, manipulate it and update it data back to the database or use it to render data.

View: The View component is used for all the UI logic of the application. For example, the Customer view would include all the UI components such as text boxes, dropdowns, etc. that the final user interacts with.

Controller: Controllers act as an interface between Model and View components to process all the business logic and incoming requests, manipulate data using the Model component and interact with the Views to render the final output. For example, the Customer controller would handle all the interactions and inputs from the Customer View and update the database using the Customer Model. The same controller would be used to view the Customer data. ASP.

NET supports three major development models: Web Pages, Web Forms and MVC (Model View Controller). The ASP.NET MVC framework is a lightweight, highly testable presentation framework that is integrated with existing ASP.NET features, such as master pages, authentication, etc. Within .NET, this framework is defined in the System.Web.Mvc assembly. The latest version of the MVC Framework is 5.0. We use Visual Studio to create ASP.NET MVC applications which can be added as template in Visual Studio.

INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 3 ISSUE 3 (2017) PAGES 2426 - 2431
RECEIVED : 25.04.2017 PUBLISHED : 29.05.2017
May 29, 2017



ASP.NET MVC Features

The ASP.NET MVC provides the following features:

- Ideal for developing complex but light weight applications
- It provides an extensible and pluggable framework which can be easily replaced and customized. For example, if you do not wish to use the in-built Razor or ASPX View Engine, then you can use any other third-party view engines or even customize the existing ones.
- Utilizes the component-based design of the application by logically dividing it into Model, View and Controller components. This enables the developers to manage the complexity of large-scale projects and work on individual components.
- The MVC structure enhances the test-driven development and testability of the application since all the components can be designed interface-based and tested using mock objects. Hence the ASP.NET MVC Framework is ideal for projects with large team of web developers.
- Supports all the existing vast ASP.NET functionalities such as Authorization and Authentication, Master Pages, Data Binding, User Controls, Memberships, ASP.NET Routing, etc.
- It does not use the concept of View State (which is present in ASP.NET). This helps in building applications which are light-weight and gives full control to the developers.

Thus, you can consider MVC Framework as a major framework built on top of ASP.NET providing a large set of added functionality with focus on component-based development and testing.

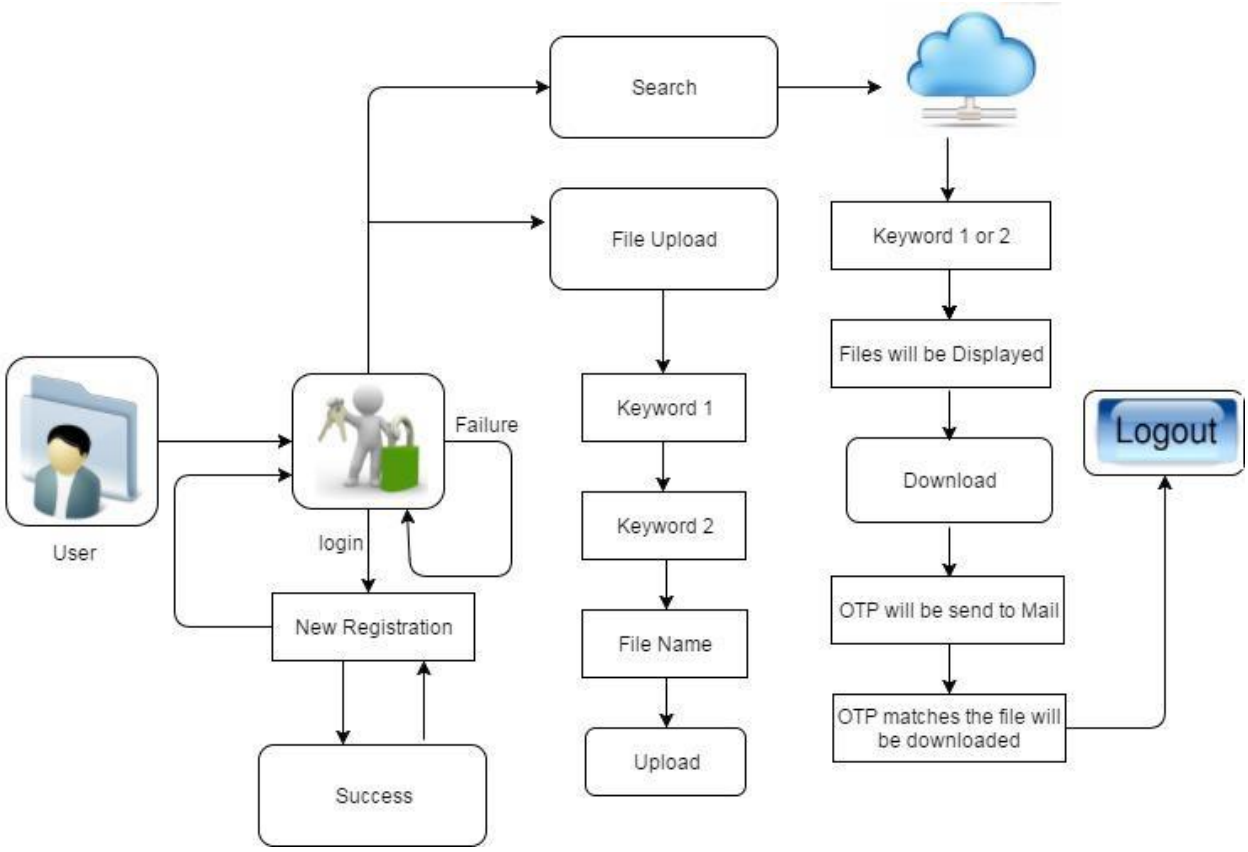
INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 3 ISSUE 3 (2017) PAGES 2426 - 2431
RECEIVED : 25.04.2017 PUBLISHED : 29.05.2017
May 29, 2017

2. PROBLEMS IN EXISTING SYSTEM

The problems in existing system is when data's are have been uploaded to the cloud and data's are have been encrypted and it is not protected securely users can decrypt the data's easily and if the users search terms are matched with the confidential data's the confidential data's are also viewed to the users. It should not be viewed to the users.

- Files are not securely protected.
- Files are mismatched.
- Files are visible to every user if their search terms are matched with the content.
- Unnecessary files will be viewed to the user.

3. ARCHITECTURE DIAGRAM



4. SCOPE OF THE PROJECT

Scope of our project is to maintain data's securely without any leakage. To maintain the data's we are protecting them by using the keywords, user itself can provide their own keywords related to the file when they are uploading the files. After providing the key words the keywords will be converted to hash values this is achieved by using hash algorithm once the keywords are have been converted to hash values the keywords will not be in a readable format.

ANALYSIS MODEL

Mainly there are four phases in the "**Spiral Model**":

- Planning
- Evolutions
- Risk Analysis
- Engineering

Software Development India

Planning: In this phase, the aims, option and constraints of the project are determined and are documented. The aims and other specifications are fixed so as to determine the strategies/approaches to go after during the project life cycle.

Risk Analysis: It is the most significant phase of "Spiral Model". In this phase the entire possible option that are available and helpful in developing a cost efficient project are analyzed and strategies are determined to employ the available resources. This phase has been added particularly so as to recognize and resolve all the possible risks in the project**.** If any indication shows some uncertainty in needs, prototyping may be utilized to continue with the obtainable data and discover out possible **software development** solution so as to deal with the potential modification in the needs.

Engineering: In this phase, the specific **software development** of the project is worked out. The output of developed of modules by modules is passed through all the phases iteratively so as to obtain development in the same.

CONCLUSION & FUTURE WORK

In order to allow a cloud server to search on encrypted data without learning the underlying plaintexts in the public-key setting, Boneh [7] proposed a cryptographic primitive called public-key encryption with keyword search (PEKS). Since then, considering different requirements in practice, e.g., communication overhead, searching criteria and security enhancement, various kinds of searchable encryption systems have been put forth. However, there exist only a few public-key searchable encryption systems that support expressive keyword search policies, and they are all built from the inefficient composite-order groups [17]. In this paper, we focused on the design and analysis of public-key searchable encryption systems in the prime-order groups that can be used to search multiple keywords in expressive searching formulas. Based on a large universe key-policy attribute-based encryption scheme given in [18], we

presented an expressive searchable encryption system in the prime-order group which supports expressive access structures expressed in any monotonic Boolean formulas. Also, we proved its security in the standard model, and analyzed its efficiency using computer simulations.

REFERENCE

1. **FOR .NET INSTALLATION**
   www.support.mircosoft.com
2. **FOR DEPLOYMENT AND PACKING ON SERVER**
   www.developer.com

   www.15seconds.com
3. **FOR SQL**
   www.msdn.microsoft.com
4. **FOR ASP.NET**
   www.msdn.microsoft.com/net/quickstart/aspplus/default.com

   www.asp.net

   www.fmexpense.com/quickstart/aspplus/default.com
5. **FOR MVC**
   www.mvc.com
   www.msdn.microsoft.com/net/quickstart/aspplus/default.com