Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.199

IJCSMC, Vol. 8, Issue. 9, September 2019, pg.219 – 225

Trust Enhanced Secure Cloud Data Storage Using Cryptographic Role-Based Access Control Mechanism

G.DEEPIKA[1]; MR.DANIEL NESAKUMAR[2]; MRS.ARUNA[3]
[1]PG Student, PG & Research Department of Computer Application, Hindusthan College of Arts and Science
[2]Assistant Professor, PG & Research Department of Computer Application, Hindusthan College of Arts and Science
[3]Assistant Professor, Department of IT, Coimbatore Institute of Engineering & Technology
deepikaganesan654@gmail.com [1]; danielnesakumar@gmail.com [2]; arunadani7@gmail.com [3]

Abstract*— In a cloud data storage system, the data owners would wish to specify the policies as to who can access their data and the cloud providers are required to correctly enforce the policies that the data owners have specified. In order to enforce the specified access control policies before putting the data onto the cloud, the data owners can encrypt the data in the way that only users that the owners wished to allow as specified in the access control policies are able to decrypt and access the data. In this paper, we propose trust models to reason about and to improve the security for stored data in cloud storage systems that use cryptographic RBAC schemes. The trust models provide an approach for the owners and roles to determine the trustworthiness of individual roles and users, respectively, in the RBAC system. The proposed trust models consider role inheritance and hierarchy in the evaluation of trustworthiness of roles. We present a design of a trust-based cloud storage system, which shows how the trust models can be integrated into a system that uses cryptographic RBAC schemes. We have also considered practical application scenarios and illustrated how the trust evaluations can be used to reduce the risks and to enhance the quality of decision making by data owners and roles of cloud storage service.

I. INTRODUCTION

CLOUD COMPUTING IS A TYPE OF COMPUTING THAT RELIES ON SHARING COMPUTING RESOURCES RATHER THAN HAVING LOCAL SERVERS OR PERSONAL DEVICES TO HANDLE APPLICATIONS. CLOUD COMPUTING IS COMPARABLE TO GRID COMPUTING, A TYPE OF COMPUTING WHERE UNUSED PROCESSING CYCLES OF ALL COMPUTERS IN A NETWORK ARE HARNESSES TO SOLVE PROBLEMS TOO INTENSIVE FOR ANY STAND-ALONE MACHINE. IN CLOUD

COMPUTING, THE WORD CLOUD (ALSO PHRASED AS "THE CLOUD") IS USED AS A METAPHOR FOR "THE INTERNET," SO THE PHRASE CLOUD COMPUTING MEANS "A TYPE OF INTERNET-BASED COMPUTING," WHERE DIFFERENT SERVICES — SUCH AS SERVERS, STORAGE AND APPLICATIONS — ARE DELIVERED TO AN ORGANIZATION'S COMPUTERS AND DEVICES THROUGH THE INTERNET.

II. EXISTING SYSTEM & PROPOSED SYSTEM

EXISTING SYSTEM

In a typical service-oriented computing, the server defines some functions including the implementation, the parameters, and the interfaces. If a user wants to use the remote service, she calls one of the functions by following the function interface. After the server finishes the task of the function, the result will be sent back to the user. In the following context, we use function and service interchangeably.

DRAW BACKS

- In existing user level security is not able to protect the sensitive secured document on the organization.
- It lacks in Remote service authentication
- It does not support remote access security by accessing information using remote access devices like mobile, Laptop, PDA's.
- It does not providing high level security in remote service.

PROPOSED SYSTEM

This section presents the system structure of the proposed adaptive secure access mechanism, which consists of two major components, an adaptive access control module and an adaptive function invocation module. The adaptive access control module enforces the access control policy. It constrains what a user can do, as well as what programs executing on behalf of the users are allowed to do.

ADVANTAGES OF PROPOSED SYSTEM

- It provides high level security for accessing document through remote access device.
- It Provides security in remote access by through various factor like Role, Time, Device used, OTP and location.
- High Accuracy
- Easy to maintain and less cost consumption

III.MODULES

The project entitled with "Trust Enhanced Secure Cloud Data Storage Using Cryptographic Role Based Access Control Mechanism" is divided into numerous modules. The detail description about the whole modules will be explained in below.

A. User Creation

In this module enables the web administrator to manage the user details on this application. The administrator can add new user and can able to edit or delete existing users by using this module. All the user details are stored in user database. The user detail includes role and designation of the user and the role of the user is main element of this application for providing the remote access security.

B. Upload Document

In this module enables the web administrator to upload the document to this application. The document includes document id, document title, and document file path and search keywords.

C. Role

In this module enables the web administrator to assign the role of the user. The role includes managing director, developers, team leaders and clients.

D. Location

In this module enables the web administrator to store the location master details on this application. The location indicates home, office and client place.

E. Security Settings

In this module enables the web administrator to make security setting for all the users on this application. The security setting depends on the role associated on the user. For example the managing director can have all rights to access the document from this share point at any time. But others are not having all rights to access documents. The documents access by through remote devices and remote accessing the system will be consider as this security setting when accessing the documents.

F. Reports

In this module enables the web administrator to generate various necessary reports in this application. The reports include user details, document details and security settings details.

G. Download Document

In this module enables the users to download the document from this SharePoint. The download will be based on the security settings provided by the administrator.

IV. INPUT DESIGN

The input design is the process of entering data to the system. The input design goal is to enter to the computer as accurate as possible. Here inputs are designed effectively so that errors made by the operations are minimized. The inputs to the system have been designed in such a way that manual forms and the inputs are coordinated where the data elements are common to the source document and to the input. The input is acceptable and understandable by the users who are using it .Input design is the process of converting user-originated inputs to a computer-based format input data are collected and organized into group of similar data. Once identified, appropriate input media are selected for processing. The input design also determines the user to interact efficiently with the system. Input design is a part of overall system design that requires special attention because it is the common source for data processing error. The goal of designing input data is to make entry easy and free from errors.

V. OUTPUT DESIGN

Output design is the process of converting computer data into hard copy that is understood by all. The various outputs have been designed in such a way that they represent the same format that the office and management used to. Computer output is the most important and direct source of information to the user. Efficient, intelligible output design should improve the systems relationships with the user and help in decision making. A major form of output is the hardcopy from the printer. Output requirements are designed during system analysis. A good starting point for the output design is the Data Flow Diagram (DFD). Human factors educe issues for design involves addressing internal controls to ensure readability. The output form in the system is either by screen or by hard copies. Output design aims at communicating the results of the processing of the users. The reports are generated to suit the needs of the users. The reports have to be generated with appropriate levels.

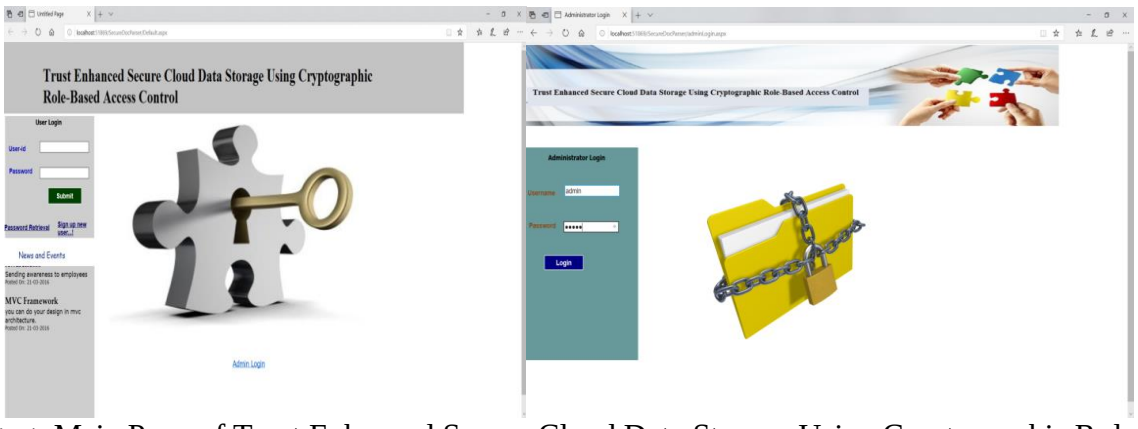

Fig 1: Main Page of Trust Enhanced Secure Cloud Data Storage Using Cryptographic Role - Based Access Control Mechanism.

In this page various menus are included like

Home, Admin login, User login , User name and password,Admin login

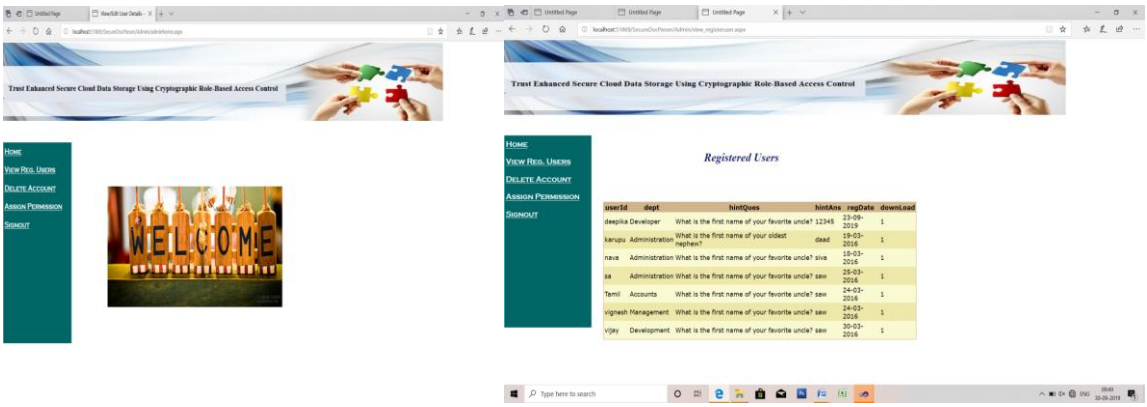

Fig 2:Admin home page and view Reg.user

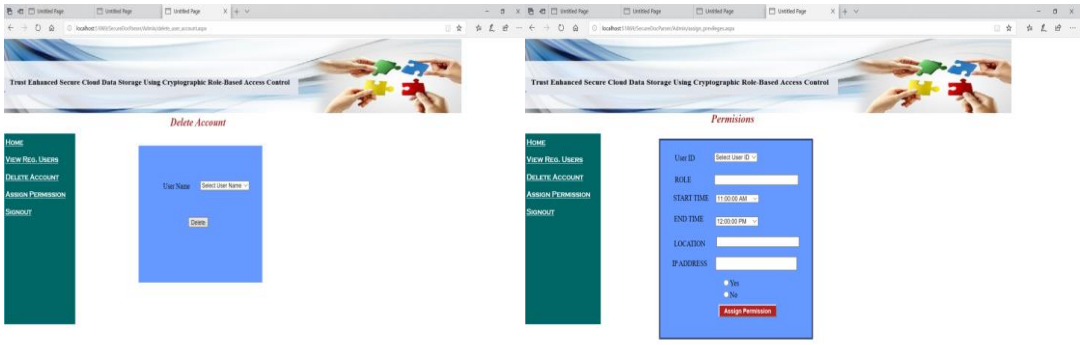

Fig 3:Delete Account and Permission

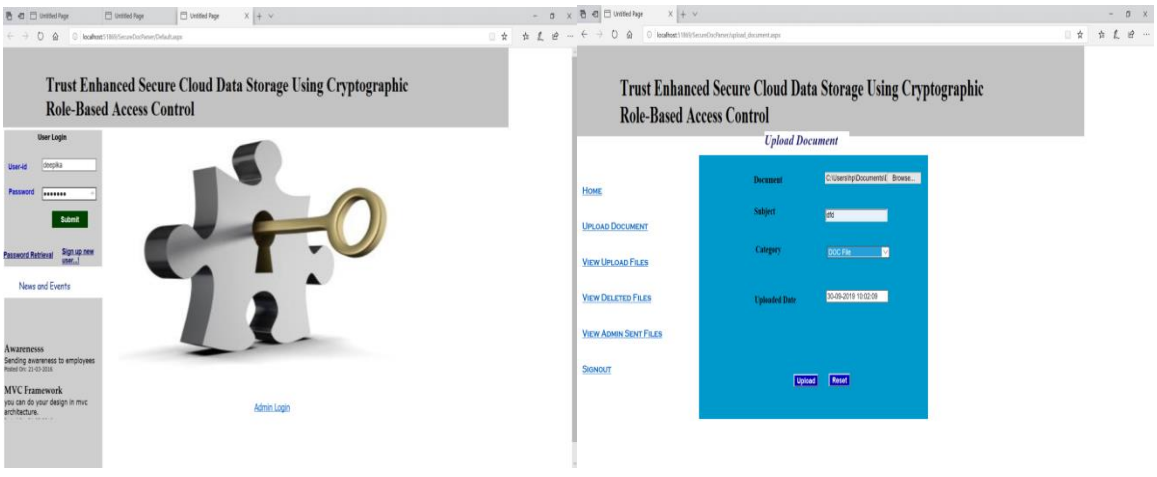

Fig 4:User Login and Upload Document

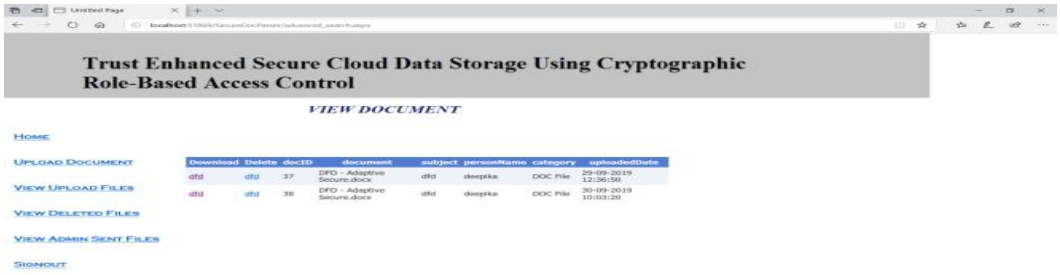

Fig 5:View Document

VI. CONCLUSIONS

In this project, we have addressed trust issues in cryptographic RBAC systems for securing data storage in a cloud environment. The paper has proposed trust models for owners and roles in RBAC systems which are using cryptographic RBAC schemes to secure stored data. These trust models assist owners and roles to create flexible access policies, and cryptographic RBAC schemes ensure that these policies are enforced in the cloud. The trust models enable the owners and roles to determine the trustworthiness of individual roles and users in the RBAC system respectively. They allow the data owners to use the trust evaluation to decide whether or not to store their encrypted data in the cloud for a particular role. The models also enable the role managers to use the trust evaluation in their decision to grant the membership to a particular user. Another significant contribution of this paper is that the proposed trust models take into account role inheritance and hierarchy in the evaluation of trustworthiness of roles. As far as we are aware, this is the first time such a trust model for role-based access control system taking into account role inheritance has been proposed. We designed the architecture of a trust-based cloud storage system which has shown how the trust models can be integrated into a system that uses cryptographic RBAC schemes. We have also described the application of the trust models by considering a practical scenario and illustrating how the trust evaluations can be used to reduce the risks and enhance the quality of decision making by data owners and role managers of the cloud storage service.

References:

- *Greg Black ZRK, "ASP.NET Developer Guide", Fifth Edition, Addition Welsay Publication.*
- *Stephen Walher, "ASP.NET Unreleased", Galgotia Publications, Second Edition.*
- *Janathan Gordyear, "Debugging in ASP.NET", First Edition, BPB Publications.*
- *Roger S.Pressman,"Software Engineering", Tata Mc Graw-Hill, 2000, Fifth Edition.*
- *Ellias M. Award, "System Analysis and Design", Galgotia Publications PVT Ltd 1997, Second Edition.*

- *NITT's Education Research and Development Group, "Structured System Analysis and Design", Pace Education PVT Ltd 1993 Edition.*
- *Davin Reader, "Master SQL Server 2000", Third Edition BPB Publications.*
- www.aspdotnettutorials.com
- www.dotnetheaven.com
- www.sqlserver.com

