ABSTRACT

Your health care provider may be moving from paper records to electronic health records or may be using EHRs already. EHRs allow providers to use information more effectively to improve the quality and efficiency of your care, but EHRs will not change the privacy protections or security safeguards that apply to your health information. This project focuses on developing secure cloud framework for evolving and accessing trusted computing services in all levels of public cloud deployment model. Thus, eliminates both internal and external security threats. These results in achieving data confidentiality, data integrity, authentication and authorization, eliminating both active and passive attacks from cloud network environment. To develop a secure cloud framework for accessing trusted computing and storage services in all levels of public cloud deployment model.

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER -1

INTRODUCTION

1.1 OVERVIEW

With the explosive growth of data, it is a heavy burden for users to store the sheer amount of data locally. Therefore, more and more organizations and individuals would like to store their data in the cloud. However, the data stored in the cloud might be corrupted or lost due to the inevitable software bugs, hardware faults and human errors in the cloud. In order to verify whether the data is stored correctly in the cloud, many remote data integrity auditing schemes have been proposed. In remote data integrity auditing schemes, the data owner firstly needs to generate signatures for data blocks before uploading them to the cloud. These signatures are used to prove the cloud truly possesses these data blocks in the phase of integrity auditing. And then the data owner uploads these data blocks along with their corresponding signatures to the cloud. The data stored in the cloud is often shared across multiple users in manycloud storage applications, such as Google Drive, Dropbox and iCloud. Data sharing as one of the most common features in cloud storage, allows a number of users to share their data with others. However, these shared data stored in the cloud might contain some sensitive information. For instance, the Electronic Health Records stored and shared in the cloud usually contain patients' sensitive information (patient's name, telephone number and ID number, etc.) and the hospital's sensitive information (hospital's name, etc.). If these EHRs are directly uploaded to the cloud to be shared for research purposes, the sensitive information of patient and hospital will be inevitably exposed to the cloud and the researchers. Besides, the integrity of the EHRs needs to be guaranteed due to the existence of human errors and software/hardware failures in the cloud. Therefore, it is important to accomplish remote data integrity auditing on the condition that the sensitive information of shared data is protected. A potential method of solving this problem is to encrypt the whole shared file

beforesending it to the cloud, and then generate the signatures used to verify the integrity of this encrypted file, finally upload this encrypted file and its corresponding signatures to the cloud. This method can realize the sensitive information hiding since only the data owner can decrypt this file. However, it will make the whole shared file unable to be used by others. For example, encrypting the EHRs of infectious disease patients can protect the privacy of patient and hospital, but these encrypted EHRs cannot be effectively utilized by researchers any more. Distributing the decryption key to the researchers seems to be a possible solution to the above problem. However, it is infeasible to adopt this method in real scenarios due to the following reasons. Firstly, distributing decryption key needs secure channels, which is hard to be satisfied in some instances. Furthermore, it seems very difficult for a user to know which researchers will use his/her EHRs in the near future when he/she uploads the EHRs to the cloud. As a result, it is impractical to hide sensitive information by encrypting the whole shared file. Thus, how to realize data sharing with sensitive information hiding in remote data integrity auditing is very important and valuable. Unfortunately, this problem has remained unexplored in previous research.

CHAPTER -2
LITERATURE SURVEY

2.1 ANALYSISOFTHELITERATURE

Literature survey is the main advance in programming improvement measure. Priorto building up the instrument it is important to decide the time factor, economy andfriends strength. When these things are fulfilled, at that point the subsequent stageis to figure out which working framework and language can be utilized for buildingup the device. When the developers begin assembling the apparatus the softwareengineersneedparcelofouterhelp.Thishelpcanbegottenfromseniordevelop ers, from book or from sites. The major part of the project developmentsector considers and fully survey all the required needs for developing the project.Beforedevelopingthetoolsandtheassociateddesigningitisnecessarytodeter mine and survey the time factor, resource requirement, man power, economy,and company strength. Prior to building the framework the above thought areconsidered for building up the proposed framework. The significant piece of theundertaking advancement area considers and completely survey all the necessaryrequirements for building up the venture. For each undertaking Literature survey isthe main area in programming improvement measure. Prior to building up theinstruments and the related planning it is important to decide and survey the timefactor, asset prerequisite, labor, economy, and friends strength. When these thingsare fulfilled and completely surveyed, at that point the following stage is to decideabout the product details in the separate framework, for example, what kind ofworking framework the venture would require and what are largely the importantprogramming are expected to continue with the subsequent stage like building uptheapparatuses,andtherelatedactivities.Herewehavetakenthegeneralsurveys of different creators and noted down the fundamental central issues withrespect to their work. In this venture literature survey assumes a prevailing part inget assets from different areas and all the connected points that are exceptionallyvaluable

under this segment. The most awesome aspect if this is the manner inwhich things get all together and encourages us to suite our work according to thecurrentinformation.

2.2 LITERARYREVIEWS

TITLE 1:

Securely Outsourcing Attribute-Based Encryption with Checkability.

AUTHOR: Jin Li, Xinyi Huang, Jingwei Li, Xiaofeng Chen, and Yang Xiang

Attribute-Based Encryption (ABE) is a promising cryptographic primitive which significantly enhances the versatility of access control mechanisms. Due to the high expressiveness of ABE policies, the computational complexities of ABE key-issuing and decryption are getting prohibitively high. Despite that the existing Outsourced ABE solutions are able to offload some intensive computing tasks to a third party, the verifiability of results returned from the third party has yet to be addressed. Aiming at tackling the challenge above, we propose a new Secure Outsourced ABE system, which supports both secure outsourced key-issuing and decryption. Our new method offloads all access policy and attribute related operations in the key-issuing process or decryption to a Key Generation Service Provider (KGSP) and a Decryption Service Provider (DSP), respectively, leaving only a constant number of simple operations for the attribute authority and eligible users to perform locally. In addition, for the first time, we propose an outsourced ABE construction which provides checkability of the outsourced computation results in an efficient way. Extensive security and performance analysis show that the proposed schemes are proven secure and practical.

TITLE: 2 Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records

AUTHOR: Josh Benaloh, Melissa Chase, Eric Horvitz, and Kristin Lauter

patient-centric framework and a suite of mechanisms for data access control to PHRs stored in semitrusted servers. To achieve fine-grained and scalable data access control for PHRs, we leverage attribute-based encryption (ABE) techniques to encrypt each patient's PHR file. Different from previous works in secure data outsourcing, we focus on the multiple data owner scenario, and divide the users in the PHR system into multiple security domains that greatly reduces the key management complexity for owners and users. A high degree of patient privacy is guaranteed simultaneously by exploiting multiauthority ABE. Our scheme also enables dynamic modification of access policies or file attributes, supports efficient on-demand user/attribute revocation and break-glass access under emergency scenarios. Extensive analytical and experimental results are presented which show the security, scalability, and efficiency of our proposed scheme.

TITLE 9:A cloud-based approach for interoperable electronic health records (EHRs)

AUTHOR: A. Bahga, V. Madisetti,

We present a cloud-based approach for the design of interoperable electronic health record (EHR) systems. Cloud computing environments provide several benefits to all the stakeholders in the healthcare ecosystem (patients, providers, payers, etc.). Lack of data interoperability standards and solutions has been a major obstacle in the exchange of healthcare data between different stakeholders. We propose an EHR system - cloud health information systems technology architecture (CHISTAR) that achieves semantic interoperability

-grained and scalable data access control for PHRs, we leverage attribute-based encryption (ABE) techniques to encrypt each patient's PHR file. Different from previous works in secure data outsourcing, we focus on the multiple data owner scenario, and divide the users in the PHR system into multiple security domains that greatly reduces the key management complexity for owners and users. A high degree of patient privacy is guaranteed simultaneously by exploiting multiauthority ABE. Our scheme also enables dynamic modification of access policies or file attributes, supports efficient on-demand user/attribute revocation and break-glass access under