

EFFICIENT AUDITING SCHEME FOR SECURE DATA STORAGE IN FOG-TO- CLOUD COMPUTING

A Project Report Phase - II

Submitted in partial fulfilment of the requirements for the award of Bachelor of
Engineering degree in Electronics and Communication Engineering

by

BODDEPALLI HANISH (39130077)
THANISHA VALLI MOHAMMAD (39130292)



DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING
SCHOOL OF ELECTRICAL AND ELECTRONICS ENGINEERING

SATHYABAMA
INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)

Accredited with Grade "A" by NAAC
JEPPIAAR NAGAR, RAJIV GANDHI SALAI, CHENNAI - 600 119

April- 2023



SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY (DEEMED TO BE UNIVERSITY)

Accredited with “A” grade by NAAC I 12B Status by UGC I

Approved by AICTE Jeppiaar Nagar, Rajiv Gandhi Salai,

Chennai – 600 119 www.sathyabama.ac.in

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

BONAFIDE CERTIFICATE

This is to certify that this Project Report is the bonafide work of BODDEPALLI HANISH (39130077) and THANISHA VALLI MOHAMMAD (39130292) who carried out the project entitled “EFFICIENT AUDITING SCHEME FOR SECURE DATA STORAGE IN FOG-TO-CLOUD COMPUTING” under my supervision from November 2022 to April 2023.

Internal Guide

Dr. S. KARTHIKEYAN, M.E., Ph.D.,

Head of the Department

Dr. T. RAVI, M.E., Ph.D.,

Submitted for viva voce Examination held on

Internal Examiner

External Examiner

DECLARATION

We BODDEPALLI HANISH (39130077) and THANISHA VALLI MOHAMMAD (39130292) hereby declare that the Project Report entitled “EFFICIENT AUDITING SCHEME FOR SECURE DATA STORAGE IN FOG-TO-CLOUD COMPUTING” done by us under the guidance of Dr.S.KARTHIKEYAN M.E.,Ph.D., Associate professor, Department of Electronics and Communication Engineering, SATHYABAMA INSTITUTE OF SCIENCEAND TECHNOLOGY, is submitted in partial fulfilment of the requirements for the award of Bachelor of Engineering degree in Electronics and Communication Engineering.

DATE :

PLACE :

SIGNATURE OF THE CANDIDATES

1. 
2. 

ACKNOWLEDGEMENT

We are pleased to acknowledge my sincere thanks to the Board of Management of **SATHYABAMA** for their kind encouragement in doing this project and for completing it successfully. We are grateful to them.

We convey my thanks to **Dr. N. M. NANDHITHA, M.E., PhD., Professor & Dean, School of Electrical and Electronics Engineering** and **Dr. T. RAVI, M.E., Ph.D., Professor & Head, Department of Electronics and Communication Engineering** for providing me necessary support and details at the right time during the progressive reviews.

We would like to express my sincere and deep sense of gratitude to my Project Guide **Dr. S. KARTHIKEYAN, M.E., Ph.D.**, Associate professor, Department of Electronics and Communication Engineering for his valuable guidance, suggestions and constant encouragement paved the way for the successful completion of my project work.

We wish to express my thanks to all Teaching and Non-teaching staff members of the Department of Electronics and Communication Engineering who were helpful in many ways for the completion of the project.

ABSTRACT

Nowadays, large amounts of data are stored with cloud service providers. Third-party auditors (TPAs), with the help of cryptography, are often used to verify this data. Cloud Data Auditing Techniques with a Focus on Privacy and Security. It aims to provide a resource based on-demand. It avoids online usage burden of accessing data through internet. Cloud storage supports to maintain data securely in cloud. Cloud is interconnected with group of computers, which is used to store information and run their applications in cloud platform. Through cloud computing, we can access any file, document of user from anywhere in the world. Mainly, cloud can be used for cost savings, high scalability, and large storage space. But a major issue in cloud computing is security. Most of the schemes introduced by the government go into the dustbin just because the officials who implement the schemes could not make them available to suitable people. So, there is a secured and transparent system needed which enable an arbitrary person to directly apply for a scheme and track the status from time to time and know whether he is entitled to receive the fruit or his application is rejected by officials. In our system admin will add the scheme details to the system. And he can be able to view the registered user details. And he can be able to accept or reject the scheme which is requested by the client. And user can be able to view the status of his scheme request level. Fog-to-cloud computing has now become a new cutting-edge technique along with the rapid popularity of Internet of Things (IoT). Unlike traditional cloud computing, fog-to-cloud computing needs more entities to participate in, including mobile sinks and fog nodes except for cloud service provider (CSP). Hence, the integrity auditing in fog-to-cloud storage will also be different from that of traditional cloud storage. In the recent work of Tian et al., they took the first step to design public auditing system for fog-to-cloud computing. However, their scheme becomes very inefficient since they use intricate public key cryptographic techniques, including bilinear mapping, proof of knowledge

TABLE OF CONTENTS

CHAPTER NO	TITLE	PAGE NO
	ABSTRACT	V
	LIST OF FIGURES	VIII
1	INTRODUCTION	1
2	LITERATURE SURVEY	6
3	REQUIREMENT ANALYSIS	10
	3.1 EXISTING SYSTEM	10
	3.2 DISADVANTAGES OF EXISTING SYSTEM	11
4	DESCRIPTION OF PROPOSED SYSTEM	12
	4.1 PROPOSED SYSTEM	12
	4.2 ADVANTAGES OF PROPOSED SYSTEM	12
	4.3 REQUIREMENT AND ANALYSIS	13
	4.4 ARCHITECTURE	15
	4.5 MODULES	17
	4.6 UMLS	18
	4.7 CLASS DIAGRAM	19
	4.8 USECASE DIAGRAM	20
	4.9 SEQUENCE DIAGRAM	22
5	SOFTWARE ENVIRONMENT	28
	5.1 INTRODUCTION	28
	5.2 APPLICATIONS OF JAVA	28
	5.3 FEATURES OF JAVA	31
	5.4 COLLECTION FRAMEWORK	32
	5.5 TESTING	32
	5.6 TYPES OF TESTS	34
	5.7 TEST STRATEGY AND APPROACH	34

6	RESULT AND DISCUSSION	35
	6.1 RESULT	35
	6.2 DISCUSSION	35
7	CONCLUSION	36
	7.1 CONCLUSION	36
	7.2 FUTURE WORK	36
	REFERENCES	37
	APPENDIX	38
	A. SCREENSHOTS	38
	B. RESEARCH PAPER	53

LIST OF FIGURES

FIGURE NO	FIGURE NAME	PAGE NO
1.1	DATA UPLOAD	5
4.1	ARCHITECTURE DIAGRAM	15
4.2	DATAFLOW DIAGRAM	16
4.3	CLASS DIAGRAM	20
4.4	USER CASE DIAGRAM	22
4.5	SEQUENCE DIAGRAM	23
4.6	COMPONENT DIAGRAM	24
4.7	ACTIVITY DIAGRAM	26
4.8	ER DIAGRAMS	27
5.1	PROGRAMMING PLATFORM	25
5.2	COLLECTION FRAMEWORK	26

CHAPTER 1

INTRODUCTION

Storing large amounts of data with cloud service providers (CSPs) raises concerns about data protection. Data integrity and privacy can be lost because of the physical movement of data from one place to another by the cloud administrator, malware, dishonest cloud providers, or other malicious users who might distort the data.¹ Hence, saved data corrections must be verified at regular intervals. Nowadays, with the help of cryptography, verification of remote (cloud) data is performed by third-party auditors (TPAs). TPAs are also appropriate for public auditing, offering auditing services with more powerful computational and communication abilities than regular users. In public auditing, a TPA is designated to check the correctness of cloud data without retrieving the entire dataset from the CSP. However, most auditing schemes don't protect user data from TPAs; hence, the integrity and privacy of user data are lost. Our research focuses on cryptographic algorithms for cloud data auditing and the integrity and privacy issues that these algorithms face. Many approaches have been proposed in the literature to protect integrity and privacy; they're generally classified according to data's various states: static, dynamic, multi owner, multiuser, and so on.[1]

We provide a systematic guide to the current literature regarding comprehensive methodologies. We not only identify and categorize the different approaches to cloud data integrity and privacy but also compare and analyze their relative merits. For example, our research lists the strengths and weaknesses of earlier work on cloud auditing, which will enable researchers to design new methods. Although related topics such as providing security to the cloud are beyond this article's scope, cloud. As a middleware between IoT devices and clouds, fog computing nodes have their own basic computing, storage as well as resources to achieve the requirements for data preprocessing and transmission. Therefore, the model of fog-to-cloud computing emerges as an attractive solution for data storage in some resource-constraint large-scale industrial applications. However, fog-to-cloud computing has also to face some classical problems appeared in traditional cloud computing. One of the most famous concerns is how to ensure the integrity of stored in cloud service provider (CSP). The reason is as follows. Some CSP may try to conceal the fact that some important data

of IoT devices or fog nodes has been lost or corrupted due to kinds of internal or external attacks. Hence, developing efficient auditing techniques for secure data storage in fog-to-cloud computing are also very necessary and significant just like in traditional cloud computing.[6]

Although, in past years, many auditing schemes are presented for traditional cloud storage including many private and public auditing schemes, all of them are not directly applicable to fog-to-cloud computing for two main reasons. The first one is that the data from IoT is generated by various devices and hence it is inadvisable for those users (or data owners) to first retrieve these data and generate corresponding authenticators before outsourcing. The second one, which is also more important, is that the existing auditing systems do not involve fog computing nodes, which are rather crucial entities for fog-to-cloud computing because those nodes can help to efficiently process and rapidly transmit for large-scale of IoT data. Hence, it is urgent to develop new auditing techniques to ensure data's integrity for fog-to-cloud computing. In recent work of Tian et al. took the first step to this direction and try to fill this gap. In fact, they designed a privacy-preserving public auditing system based on bilinear mapping and the so-called tag-transforming strategy. In addition, they also evaluated the performances of their scheme by theoretical analysis and comprehensive experiments.[5] It is well-known that, in public auditing scheme, the task to verify the integrity of users' data is suitable to be outsourced to another authorized third-party auditor (TPA), which may have more professional knowledge on auditing and more computational resources. However, it should also be noted that, generally speaking, public auditing systems have lower efficiencies than private ones. Just as Zhang et al. illustrated in [4], for the same data file, the time consumptions for proving, verifying and outsourcing in public auditing scheme are hundreds (or even thousands) of times of the corresponding process in their private scheme. Hence, in some pursuing-efficiency scenarios, especially for the resource-constrained mobile sinks in fog-to-cloud computing, we believe the private auditing system may be more popular. While our protocol is used for fog computing there are different type of

Cloud service providers are there in that one is MAC and other HMAC in cloud

necessary and significant to design efficient private auditing schemes for the fog-to-cloud computing.[3]

In this paper, we try to take the step to this direction. More specifically, we propose a new auditing system based on private authentication techniques: message authentication code.

(MAC) and homomorphic MAC (HMAC) schemes, both of which are important primitives in cryptography. The MAC technique is used in the transmission process between mobile sinks and fog nodes while the HMAC scheme is used to verify the integrity of data blocks stored in CSP. Since a common private key is needed for the parties in MAC or HMAC when generating or verifying the tags, this model is not suitable to introduce TPA into it.[5]

Moreover, we give a concrete instantiation of the system by instantiating the hash-based MAC scheme in and the efficient HMAC scheme designed by Agrawal and Boneh in

Finally, we also analyze the performances of our proposed system and compare them with that of Tian et al. as well as two related traditional cloud auditing schemes in The experiment results show that our system outperformed Tian et al.'s system in terms of communication costs and computational efficiency. Moreover, our protocol is suitable for fog-to-cloud computing and hence prior to the two schemes There are many successful applications for IoT based on fog-to-cloud computing. One of the most common situations is users use sensors to collect the required data, such as related environmental data. Of course, users can also set multiple sensors to collect different areas or different types of data and transmit them to the fog node. Each fog node is a small service device provided by a service provider that can simply process and analyze data. Multiple fog nodes form a fog computing center and a cloud management. Fog computing is a decentralized computing infrastructure in which data, compute and storage where applications are located somewhere between the data source and Cloud like edge computing , fog computing brings the advantages and power of the cloud closer to where data is created and acted upon fog computing is used for cloud

There are many successful applications for IoT based on fog-to-cloud computing. One of the most common situations is users use sensors to collect the required data, such as related environmental data. Of course, users can also set multiple sensors to collect different areas or different types of data and transmit them to the fog node. Each fog node is a small service device provided by a service provider that can simply process and analyze data. Multiple fog nodes form a fog computing center and a management node is set up to manage all fog nodes. Finally, all data are outsourced to the cloud for cost-effective storage and other future uses. In order to ensure the integrity of the data, the sensor should create verifiable metadata before sending the collected data to the fog node; for the received data, the fog node must first verify its correctness, and then perform local analysis and processing, and for the processed data, fog nodes should create new verifiable metadata. Finally, all data and its verifiable metadata are transferred to the cloud for long-term storage. The data owner or any other authorized party should be able to verify the integrity of the data anytime, anywhere, that is, remotely audit the correctness of the data. It is the very purpose of this work to design a secure and efficient auditing scheme for data storage based on fog-to-cloud computing for IoT scenarios.[13]

Compared with the existing scheme, the proposed scheme reduces the user's computation overhead through the two-time signature and private key separation method, so that the proposed scheme can be better used for IoT devices with low computing capabilities. At the same time, the proposed scheme will verify the system parameters and the file tag during the signature generation and the proof generation to ensure the security of the scheme. In most applications, the sensor device collects the data and generates verifiable metadata, and then uploads the metadata to the fog node. After receiving the metadata, the fog node will first verify the metadata. If the result is true, the metadata will be further processed, then upload it and the data to the cloud for long-term storage. Data owners can verify at anytime to ensure the correctness and integrity of the data stored in the cloud, that is, the data owner can perform remote integrity auditing of the data. The auditing model is divided into private auditing and public auditing. The verification operation of the private auditing is only carried out between the CSP and the user, without the intervention of a third

party[18] and the approach because it provides more convincing results while significantly reducing the user's computation and communication overhead. At present, data integrity auditing based on IoT devices has received more and more attention. Aazam et al. believed that IoT devices use the cloud to process and store data. There are still some problems that must be solved, because the cloud is not trusted, so users cannot ensure that the cloud correctly stores the data uploaded by IoT. For data stored on the cloud server, the provable data possession (PDP) scheme can effectively verify the integrity of the cloud data and achieve blockless verification, that is, without downloading the original data.

Integrity verification ensures storage security, but the computational and communication overhead of this scheme is too large to be applied to IoT devices. Xu et al. proposed a distributed fully homomorphic encryption-based Merkle Tree (FHMT) scheme, which effectively solves the cloud credibility problem using blockchain technology, but their scheme does not implement public auditing proposed an identity-based private key generation auditing scheme, which reduces the overhead of certificate management, but the overhead of signature generation and auditing proof verification is still large to the IoT device. Zhu et al. proposed a short signature-based data auditing scheme, which reduced the computational overhead of signature generation. However, their proposed scheme is not based on fog-to-cloud computing.[26]

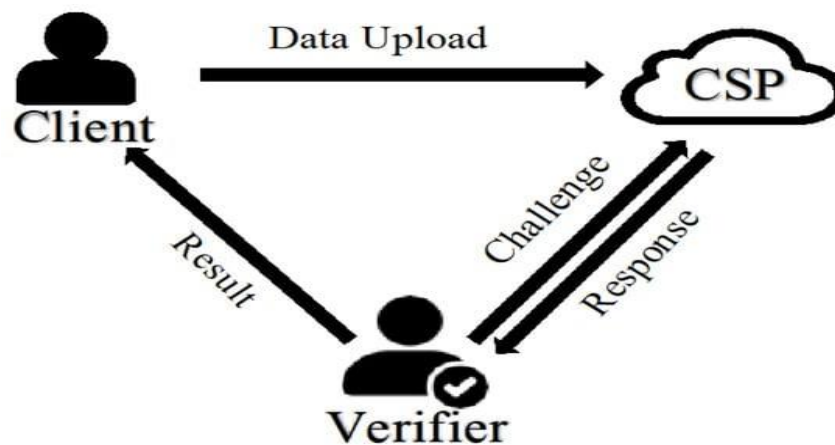


Fig1.1 Diagram of Data Upload

CHAPTER 2

LITERATURE SURVEY

2.1 INFERENCES FROM LITERATURE SURVEY

Armbrust.M (2019) et al. presented work on Cloud Data Auditing Techniques with a Focus on Privacy and Security, large amounts of data are stored with cloud service providers. Third-party auditors (TPAs), with the help of cryptography, are often used to verify this data. However, most auditing schemes don't protect cloud user data from TPAs. A review of the state of the art and research in cloud data auditing techniques highlights integrity and privacy challenges, current solutions, and future research directions. [3]

Wang.C (2018) et al. presented work on A survey on auditing techniques used for preserving privacy of data stored on cloud to the stored data on the cloud is one of the important challenges in cloud computing. Encrypted data which is stored on the cloud may be viewed or modified by the cloud service provider. To overcome this problem many techniques have been developed but, those cannot guarantee accurately about the security of the stored data. These modifications of the data by the service provider or by others should also be known to the data owner. For such purpose, data tagging technique can be used to audit the data. Auditing is done by using Third Party Auditor (TPA). TPA stores data information of the data owner and challenges to the cloud server, depending upon the data owner request. With the help of such mechanism, TPA can convince both, data owner and cloud server[1]

Mell.P (2020) et al. presented work on Auditing in Cloud Computing Solutions with OpenStack will walk through how auditing works in a Cloud environment. We will touch upon things like Cloud Auditing Data standard (CADF), the auditing challenges in a distributed cloud platform like OpenStack and how they are overcome using CADF[2]

Roger pressnma(2021) et al. presented work on Cloud Security Auditing Challenges and Emerging Approaches IT auditors collect information on an organization's information systems, practices, and operations and critically analyze the

information for improvement. One of the primary goals of an IT audit is to determine if the information system and its intainers are meeting both the legal expectations of protecting customer data and the company standards of achieving financial success against various security threats. These goals are still relevant in the newly emerging cloud computing model of business, but they need customization. There are clear differences between cloud and traditional IT security auditing. In this article, the authors explore potential challenges unique to cloud security auditing; examine additional challenges specific to cloud computing domains such as banking, medical, and government sectors; and present emerging cloud-specific security auditing approaches and provide critical analysis[1]

patel moss(2021) et al. presented work on Dynamic-Hash-Table Based Public Auditing for Secure Cloud Storage is an increasingly popular application of cloud computing, which can provide on-demand outsourcing data services for both organizations and individuals. However, users may not fully trust the cloud service providers (CSPs) in that it is difficult to determine whether the CSPs meet their legal expectations for data security. Therefore, it is critical to develop efficient auditing techniques to strengthen data owners' trust and confidence in cloud storage. In this paper, we present a novel public auditing scheme for secure cloud storage based on dynamic hash table (DHT), which is a new two-dimensional data structure located at athird parity auditor (TPA) to record the data property information for dynamic auditing. Differing from the existing works, the proposed scheme migrates the authorized information from the CSP to the TPA, and thereby significantly reduces the computational cost and communication overhead. Meanwhile, exploiting the structural advantages of the DHT, our scheme can also achieve higher updating efficiency than the state-of-the-art schemes. In addition, we extend our scheme to support privacy preservation by combining the homomorphic authenticator based on the public key with the random masking generated by the TPA and achieve batch auditing by employing the aggregate BLS signature technique. We formally prove the security of the proposed scheme and evaluate the auditing performance by detailed experiments and comparisons with the existing ones. The results demonstrate that the proposed scheme can effective[4]

Stoica(2019) et al. presented work on the incentive mechanism for government chiefofficials is the key obstacle to improving interagency government information sharing. This paper considers the political tournament model as suitable to stimulate local governmental “top leaders” at district-level and county-level, and then puts forward some measures for the application of the model[3]

Holzner(2018) et al. presented work on Research on the E-Government Scheme Based on Multi-Technologies and Bi-Directional Authentication The authentication is the key part of the network security. It is also the main problem we should resolve. This scheme, which is bi-directional using multi-mechanism to ensure safety authentication and providing a uniform authentication service to other e-government application system meets the need of current e-government system. But authentication technology and e-government system are continually developing there are still many problems need to be solved[3]

k.Ren (2019) et al. presented work on Analysis of E-government Services Outsourcing and Incentive Scheme Relative theories, operation patterns and trends about e-government out-sourcing are studied. Subsequently, the analyses on the incentive model and system for government and enterprise in the e-government outsourcing project are presented based on the theories of game and principal-agent, emphasizing on motivation and performance evaluation in managing out-sourcing business, in which the importance of incentive game in principal-agent is also derived. The state of incomplete and asymmetric information makes it important for government to implement reward and punishment before enough analyzing. From the aspect of validity analysis, the optimal proposal will have the characteristics of monotone, that is, the awards to the manager which are provided by government should increase with the improvement of output level. It is eventually concluded that the reformation of e-government services outsourcing relationship requires incentive scheme[1]

Patel moss(2019) et al. presented work on A Risk Assessment Model Based-Business-Circle of E-Government Information System With the development of computer network and information technology rapidly, they are serving every walk of life in China. Chinese government is using widely the information and network technology for improving its work. So, Chinese E-Government information system

is developing feetly.However, in fact, E-Government information system has some its characters and some potential hazards in China, which affects E- Government information system's healthy and favorable development. It is insufficient that some secure products and tools are only used for the security system architecture of E-Government information system. To build secure and authentic system architecture of E-Government information system, the risk assessment and management is necessary for secure and reliable E-Government information system. A risk assessment model based-business-circle of E-Government information system is proposed in the article according to the characters of E-Government information system. In the model, some business circles are given according to the importance and features of e-Government information system. Moreover, the risk assessment is done in every business circle. The model introduces the idea of risk assessment, scheme of risk assessment, process of risk assessment and the computational method of risk.[4]

Nick Todd (2020) et al. presented work on secure publishing scheme in e-Government One of the most important functions of e-Government is publication through the Internet. Though digital signatures can be exploited to protect the integrity and authenticity of published information, it cannot effectively resist malicious replacement in scenarios The scheme is able to resist the malicious replacement of published information and its cost is modest.[6]

CHAPTER 3

REQUIRMENT ANALYSIS

3.1 EXISTING SYSTEM OF CLOUD SERVICE PROVIDERS

While Cloud Computing makes these advantages more appealing than ever, it also brings new and challenging security threats towards users' outsourced data. Since cloud service providers (CSP) are separate administrative entities, data outsourcing is relinquishing user's ultimate control over the fate of their data. As a result, the correctness of the data in the cloud is being put at risk due to the following reasons. Although the infrastructures under the cloud are much more powerful and reliable than personal computing devices, they are still facing a broad range of both internal and external threats for data integrity. There do exist various motivations for CSP to behave unfaithfully towards the cloud users regarding their outsourced data status. For example, CSP might reclaim storage for monetary reasons by discarding data that has not been or is rarely accessed, or even hide data loss incidents to maintain a reputation. In short, although outsourcing data to the cloud is economically attractive for long-term large-scale storage, it does not immediately offer any guarantee on data integrity and availability. This problem, if not properly addressed, may impede the success of cloud architecture.

As users no longer physically possess the storage of their data, traditional cryptographic primitives for the purpose of data security protection cannot be directly adopted. Simply downloading all the data for its integrity verification is not a practical solution due to the expensiveness in I/O and transmission cost across the network. Besides, it is often insufficient to detect the data corruption only when accessing the data, as it does not give users correctness assurance for those un accessed data and might be too late to recover the data loss or damage. Considering the large size of the outsourced data and the user's constrained resource capability, the tasks of auditing the data correctness in a cloud environment can be formidable and expensive for the cloud users. Moreover, the overhead of using cloud storage should be minimized as much as possible, such that a user does not need to perform too many operations to

use the data (in addition to retrieving the data). In particular, users may not want to go through the complexity in verifying the data integrity. Besides, there may be more than one user accesses the same cloud storage, say in an enterprise setting. For easier management, it is desirable that cloud only entertains verification request from a single designated party.

3.2 DISADVANTAGES OF EXISTING SYSTEM

IaaS providers offer their customers the illusion of unlimited compute, network, and storage capacity often coupled with a 'frictionless' registration process where anyone with a valid credit card can register and immediately begin using cloud services. Some providers even offer free limited trial periods. By abusing the relative anonymity behind these registration and usage models, spammers, malicious code authors, and other criminals have been able to conduct their activities with relative impunity. PaaS providers have traditionally suffered most from these kinds of attacks; however, recent evidence shows that hackers have begun to target IaaS vendors as well. Future areas of concern include password and key cracking, DDOS, launching dynamic attack points, hosting malicious data, botnet command and control, building rainbow tables, and CAPTCHA solving farms.

3.2.1 Insecure Interfaces and APIs

Cloud computing providers expose a set of software interfaces or APIs that customers use to manage and interact with cloud services. Provisioning, management, orchestration, and monitoring are all performed using these interfaces. The security and availability of general cloud services is dependent upon the security of these basic APIs. This introduces the complexity of the new layered API; it also increases risk, as organizations may be required to relinquish their credentials to third parties to enable their agency.

3.2.2 Malicious Insiders

The threat of a malicious insider is well-known to most organizations. This threat is amplified for consumers of cloud services by the convergence of IT services.

CHAPTER 4

DESCRIPTION OF PROPOSED SYSTEM

4.1 PROPOSED SYSTEM OF THIRD PARTY AUDITOR

The proposed system can be summarized as the following three aspects:

- We motivate the public auditing system of data storage security in Cloud Computing and provide a privacy-preserving auditing protocol, i.e., our scheme supports an external auditor to audit user's outsourced data in the cloud without learning knowledge on the data content.
- To the best of our knowledge, our scheme is the first to support scalable and efficient public auditing in Cloud Computing. Our scheme achieves batch auditing where multiple delegated auditing tasks from different users can be performed simultaneously by the TPA.
- We prove the security and justify the performance of our proposed schemes through concrete experiments and comparisons with the state-of-the-art.

4.2 ADVANTAGES OF PROPOSED SYSTEM

- Novel automatic and enforceable logging mechanism in the cloud.
- proposed architecture is platform independent and highly decentralized, in that it does not require any dedicated authentication or storage system in place.
- Provide a certain degree of usage control for the protected data after these are delivered to the receiver.
- The results demonstrate the efficiency, scalability, and granularity of our approach

4.3 REQUIREMENT & ANALYSIS OF SOFTWARE REQUIREMENT

The software requirement specification gives the system specification in which process requirements are presented in an easily understandable way. Thus, it contains all the inputs required, processes in the system and outputs produced by the system.

Software Requirements Specification plays an important role in creating quality software solutions. Specification is basically a representation process. Requirements are represented in a manner that ultimately leads to successful software implementation.

Requirements may be specified in a variety of ways. However, there are some guidelines worth following.

- Representation format and content should be relevant to the problem.
- Information contained within the specification should be nested.

Requirement analysis enables the system engineer to specify software function and perform, indicate software's interface with the other system elements, and establish constraints that software must meet. Requirement analysis allows the analyst to refine the software allocation and build models of the data, functional and behavioral domains that will be treated by software.

The first step is to understand the user's requirement within the framework of the organization's objectives and the environment in which the system is installed. Considerations are given to the user to carry on with the work within the organization's specified objectives.

Using swings in java we will develop the proposed system. The proposed application can be implemented by taking a minimum of three systems into consideration. The server is implemented in one system TPA is implemented in another system and client can be implemented from n no of systems it can be implemented on any operating

system like windows or linux. The client system will store data like files images on to server through TPA. The TPA will store the metadata information of file on TPA whereas server will store files as well as metadata data information about the files. Whenever the client asks for the verification of files on cloud the TPA will check for the data integrity on the server. This application demands minimum three systems should be connected within a network.

HARDWARE AND SOFTWARE REQUIREMENTS

- Database : MySQL
- Operating System : Windows95/98/2000/XP
- Processor : Pentium 4 processor
- RAM : 1 GB RAM
- Hard Disk : 80 GB Hard Disk Space

4.4 ARCHITECTURE OF CLOUD SERVICE PROVIDER

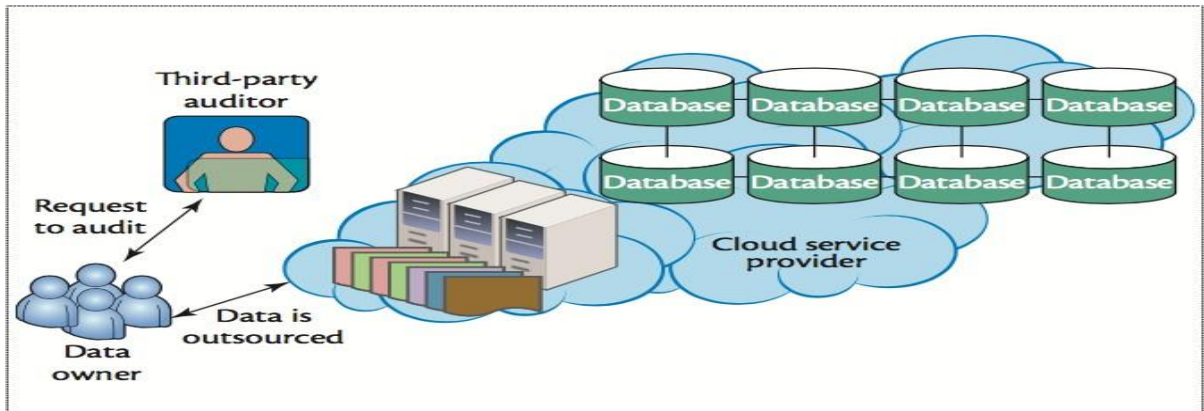


Fig 4.1 Architecture of cloud service provider

The architecture of TPA typically includes the following components:

- Auditor Client: The Auditor Client is the entity that outsources its data to the CSP for storage or processing and seeks the services of the TPA to audit the security and integrity of its data.
- Third-Party Auditor: The TPA is responsible for auditing the security and integrity of the data stored or processed by the CSP. The TPA performs audits by accessing the data stored at the CSP and verifying that it meets the security and integrity requirements.
- CSP: The CSP provides the storage or processing services to the Auditor Client. The CSP is responsible for maintaining the security and integrity of the data stored or processed on its infrastructure.
- Secure Channel: The Secure Channel is the communication channel established between the TPA and the CSP to ensure that the data being audited is not tampered with or compromised.
- Audit Logs: Audit Logs are the records of all activities performed on the data stored or processed by the CSP. The TPA uses the Audit Logs to verify the integrity and security.

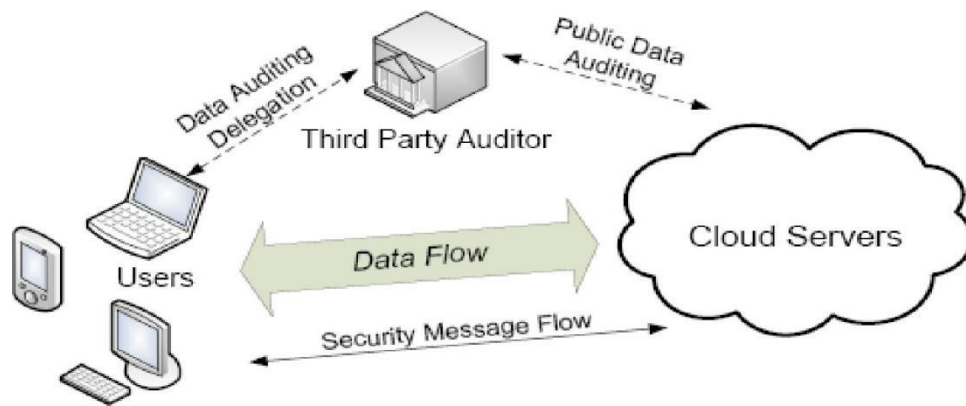


Fig 4.2 Data flow diagram of Third party auditor

- **Data Auditing Delegation:** Data auditing delegation refers to the process of delegating the task of auditing the data stored on cloud servers to a third-party auditor (TPA) by the data owner or data user. This delegation is done to ensure that the data stored on the cloud is secure, confidential, and free from any unauthorized access or tampering. The TPA verifies the data integrity and security by performing various auditing operations on the data, such as verification of the data hash, comparison of the data copies, and analysis of the data logs. By delegating the auditing task to a TPA, the data owner or user can focus on their core business or personal activities, while the TPA takes care of the data security and integrity.
- **Public Data Auditing:** Public data auditing is a type of data auditing that allows anyone to audit the data stored on cloud servers. In public data auditing, the data owner or user publishes the data along with its audit information (such as hash values, digital signatures, or encryption keys) on a public auditing platform, which can be accessed by anyone. The public can then verify the data integrity and security by performing their own auditing operations on the data and comparing the results with the audit information published by the data owner or user. Public data auditing provides transparency and accountability to the cloud computing services and enhances the trust and confidence of the public in the cloud providers.

4.5 MODULES

The system is proposed to have the following modules:

4.5.1 ADMIN MODULE

Admin is allowed to check which user registered and which data is stored in the cloudspace area

4.5.2 TPA MODULE

TPA check that data is modified or not if modified that information send to user

4.5.3 USER MODULE

User can register and he can login with his user id and password and he can uploadthe data to cloud space area

4.5.4 BLOCK VERIFICATION MODULE

User can check that the uploaded file is modified by any one or not (like server area)

4.5.5 BLOCK INSERTION MODULE

In the block insertion module user can insert the new block

4.5.6 BLOCK DELETION MODULE

In the Block Deletion Module user can delete the Block.

4.6 UMLS

UNIFIED MODELING LANGUAGE

The Unified Modelling Language allows the software engineer to express an analysis model using the modelling notation that is governed by a set of syntactic semantic and pragmatic rules.

A UML system is represented using five different views that describe the system from distinctly different perspectives. Each view is defined by a set of diagrams, which is as follows.

4.6.1 User Model View

- This view represents the system from the user's perspective.
- The analysis representation describes a usage scenario from the end-user's perspective.

4.6.2 Structural model view

- In this model the data and functionality are arrived from inside the system.
- This model view models the static structures.

4.6.3 Behavioral Model View

It represents the dynamic of behavioral as parts of the system, depicting the interactions of collection between various structural elements described in the user model and structural model view.

4.6.4 Implementation Model View

In this the structural and behavioral as parts of the system are represented as they are to be built.

4.6.5 Environmental Model View

In these the structural and behavioral aspects of the environment in which the system is to be implemented are represented.

UML is specifically constructed through two different domains they are:

- UML Analysis modeling, this focuses on the user model and structural model views of the system.
- UML design modeling, which focuses on the behavioral modeling, implementation modeling and environmental model views.

Use case Diagrams represent the functionality of the system from a user's point of view. Use cases are used during requirements elicitation and analysis to represent the functionality of the system. Use cases focus on the behavior of the system from an external point of view.

Actors are external entities that interact with the system. Examples of actors include users like administrator, bank customer ...etc., or another system like central database.

4.7 CLASS DIAGRAM AUDITING FOR SECURE DATA STORAGE IN CLOUD

This class diagram contains four classes that are Server, TPA, Client and Database. Server will perform operations like it maintains client details & session information, stores details & files and generate graphs. Client will perform operations like registration, login, upload files, download files, verify documents, add blocks, delete blocks. TPA will perform operations like taking file size, divide file into blocks, maintain metadata information, send response and verification message. And this diagram shows the relationship between these classes.

- User: This class represents the user of the cloud computing service, who stores and accesses data on the cloud server.
- Cloud Server: This class represents the cloud server that stores the data uploaded by the user.
- Third-Party Auditor (TPA): This class represents the TPA that is responsible for auditing the data stored on the cloud server to ensure its security and integrity.

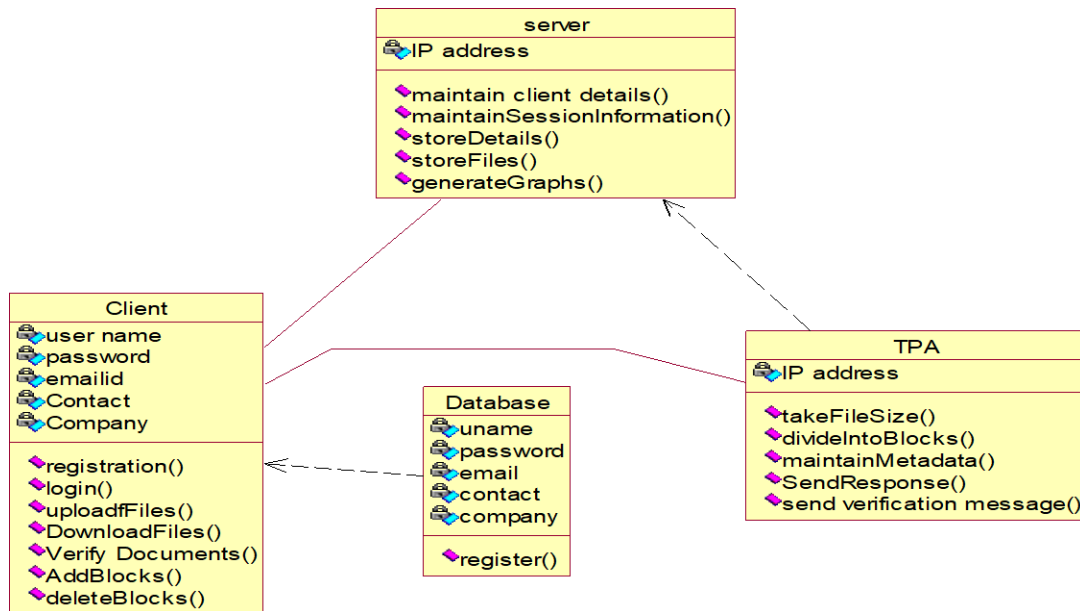


Fig 4.3 Class diagram for secure data storage in cloud

4.8 USERCASE DIAGRAM OF CLIENT AND SERVER

This use case diagram contains three actors that are Server, TPA, Client and. Server will perform operations like it maintains client details & session information, stores details & files and generate graphs. Client will perform operations like registration, login, upload files, download files, verify documents, add blocks, delete blocks. TPA will perform operations like take file size, divide file into blocks, maintain metadata information, send response and verification message. And this diagram shows the use cases of each actor and relationship between this actors and useFig:4.9 Fog-to-cloud computing has now become a new cutting-edge technique along with the rapid popularity of Internet of Things (IoT). Unlike traditional cloud computing, fog-to-cloud computing needs more entities to participate in, including mobile sinks and fog nodes except for cloud service provider (CSP). Hence, the integrity auditing in fog-to-cloud storage will also be different from that of traditional cloud storage. In the recent work of

Tian et al., they took the first step to design public auditing system for fog-to-cloud computing. However, their scheme becomes very inefficient since they use intricate public key cryptography techniques, including bilinear mapping, proof

- Upload Data: The client can upload data to the cloud server by sending a request to the server. This use case involves interactions between the client, server, and TPA for auditing and verification of the data.
- Download Data: The client can download data from the cloud server by sending a request to the server. This use case involves interactions between the client and server.
- Delete Data: The client can delete data from the cloud server by sending a request to the server. This use case involves interactions between the client and server.
- View Audit Report: The client can view the audit report generated by the TPA for a particular data file on the cloud server. This use case involves interactions between the client and TPA.
- Modify Data Access Control: The client can modify the access control policies for their data stored on the cloud server. This use case involves interactions between the client and server.
- Register/Log in: The client can register an account on the cloud server or log in to their existing account to access their data. This use case involves interactions between the client and server.
- Modify Account Details: The client can modify their account details such as email address or password. This use case involves interactions between the client and server.

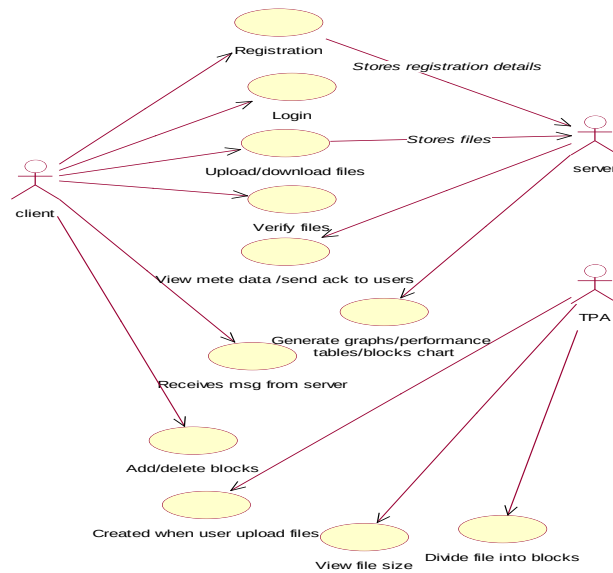


FIG 4.4 Usecase diagram of client and server

4.9 SEQUENCE DIAGRAM OF SERVER , TPA AND CLIENT

This sequence diagram contains three objects that are Server, TPA, Client and. Server will perform operations like it maintains client details & session information stores details & files and generate graphs. Client will perform operations like registration, login, upload files, download files, verify documents, add blocks, delete blocks. TPA will perform operations like take file size, divide file into blocks, maintain metadata information, send response and verification message. And this diagram shows the sequence of actions performed between these objects.

- The client sends a request to upload data to the cloud server.
- The cloud server receives the request and sends a confirmation message back to the client.
- The client encrypts the data and sends it to the cloud server.
- The cloud server stores the encrypted data and generates a data hash using a hash function.
- The cloud server sends the data hash and other audit information to TPA

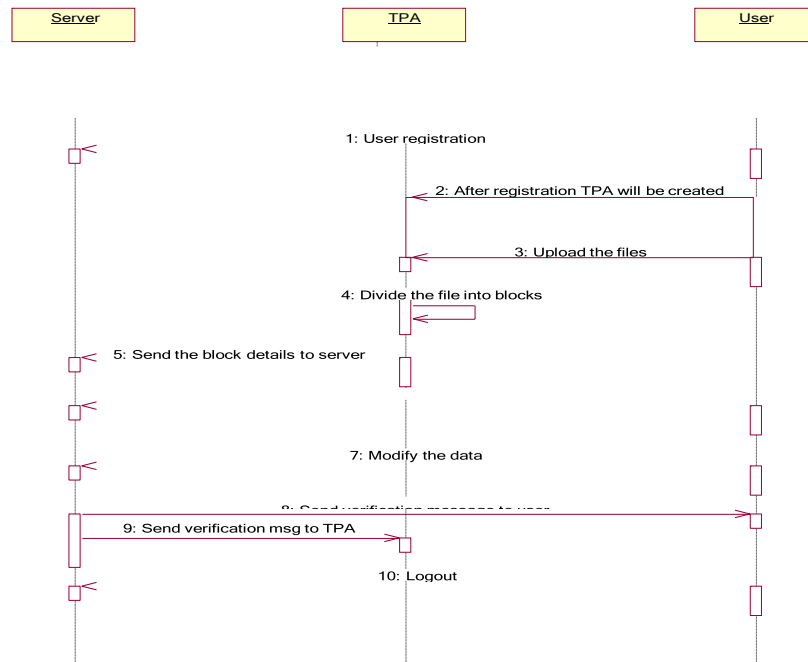


Fig 4.5 Sequence diagram of server ,TPA and client

4.9.1 COMPONENT DIAGRAM OF CLIENT AND SERVER

This component diagram contains three components that are Server, TPA, Client and. Server will perform operations like it maintains client details & session information stores details & files and generate graphs. Client will perform operations like registration, login, upload files, download files, verify documents, add blocks, delete blocks. TPA will perform operations like take file size, divide file into blocks, maintain metadata information, send response and verification message. And this diagram shows the actions performed by these components.

- **Client Interface:** This component represents the user interface through which the client interacts with the system. It may include features such as a file browser, login screen, and upload/download buttons.
- **Client Application:** This component represents the application that runs on the client side and manages the interactions between the client interface and the cloud server.

It may include features such as encryption/decryption modules, communication protocols, and access control modules.

- **Server Application:** This component represents the application that runs on the server side and manages the interactions between the cloud server and the client. It may include features such as storage management, audit management, and access control management.
- **Database:** This component represents the database system that stores the data and metadata related to the client's files on the cloud server. It may include features such as backup and recovery, data access control, and scalability.
- **Third-Party Auditor (TPA):** This component represents the TPA that performs the auditing of the client's data stored on the cloud server. It may include features such as auditing algorithms, signature verification, and logging.

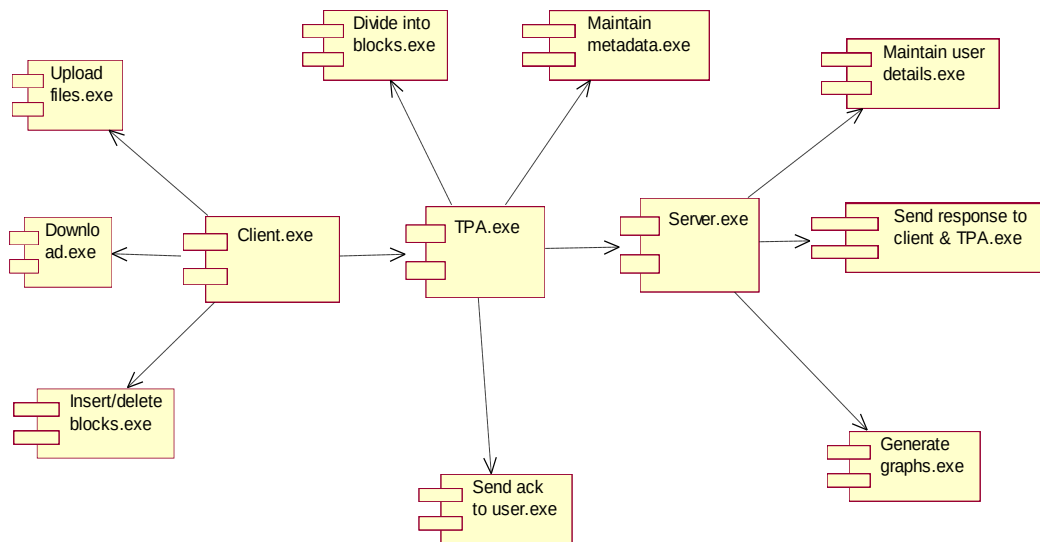


Fig 4.6 Component diagram of client and server

4.9.2 ACTIVITY DIAGRAM OF SERVER AND CLIENT

This activity diagram contains three activities that are Server, TPA, Client and. This diagram shows the flow of control between these activities.

- Uploading Data:
 - The client selects a file to upload.
 - The client encrypts the file and sends it to the server.
 - The server receives the file, stores it, and updates the database with the file's metadata.
 - The server sends an acknowledgement to the client.
- Downloading Data:
 - The client selects a file to download.
 - The client sends a request to the server for the file.
 - The server retrieves the file from storage, decrypts it, and sends it to the client.
 - The client receives the file and stores it locally.
- Deleting Data:
 - The client selects a file to delete.
 - The client sends a request to the server to delete the file.
 - The server removes the file from storage and updates the database accordingly.
 - The server sends an acknowledgement to the client.

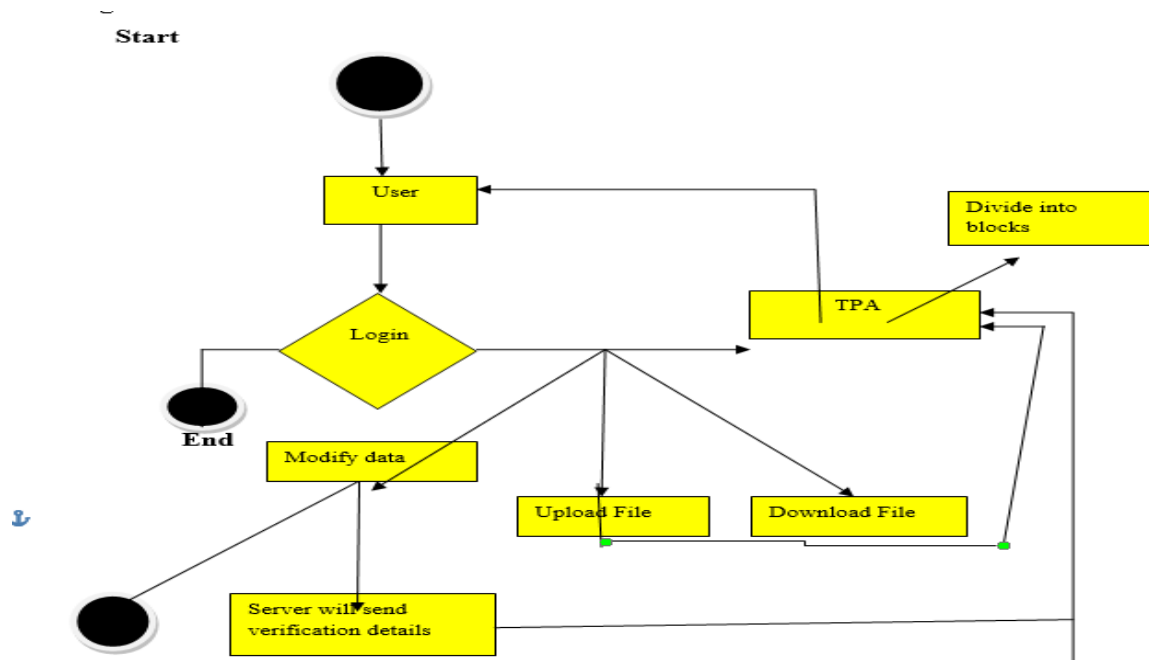


Fig 4.7 Activity diagram of server and client

4.9.3 ER-DIAGRAMS OF CLIENT , TPA AND SERVER

This ER-Diagram contains three entities that are Server, TPA, Client and. Server will perform operations like it maintains client details & session information stores details & files and generate graphs. Client will perform operations like registration, login upload files, download files, verify documents, add blocks, delete blocks. TPA will perform operations like take file size, divide file into blocks, maintain metadata information, send response and verification message. And this diagram shows the relationship between these entities.

- Client:
 - The client entity represents the user who wants to store their data on the server.
 - The client entity may have attributes such as client ID, username, password, email, and phone number.

- Server:
 - The server entity represents the cloud server where the client's data is stored.
 - The server entity may have attributes such as server ID, server name, IP address, and storage capacity.
- TPA:
 - The TPA entity represents the third-party auditor who provides auditing and access control services to the client.
 - The TPA entity may have attributes such as TPA ID, TPA name, and TPA public key.
- File:
 - The file entity represents the client's data stored on the server.
 - The file entity may have attributes such as file ID, file name, file size, and file type.

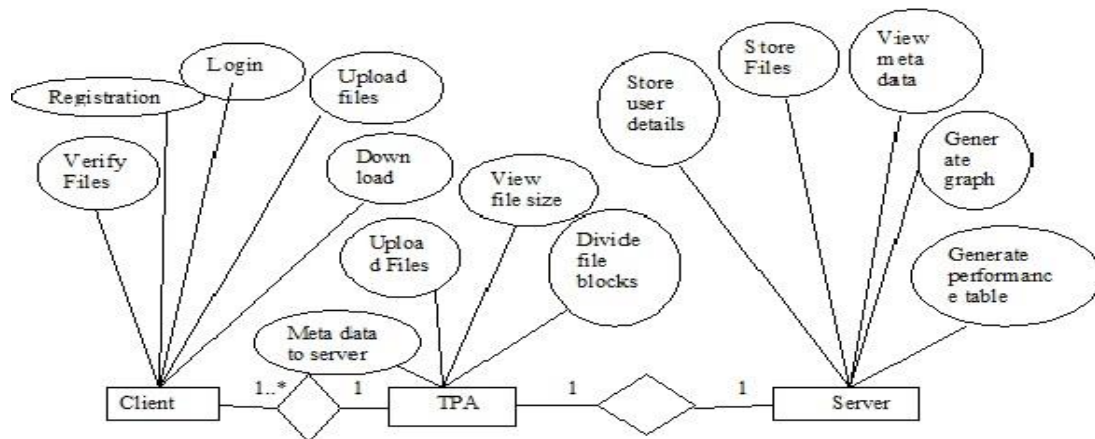


FIG 4.8 ER DIAGRAM OF CLIENT, TPA AND SERVER

CHAPTER 5

SOFTWARE ENVIRONMENT OF JAVA

INTRODUCTION

Java is one of the world's most important and widely used computer languages, and it has held this distinction for many years. Unlike some other computer languages whose influence has waned with passage of time, while Java's has grown.

5.1 APPLICATION OF JAVA

Java is widely used in every corner of world and of human life. Java is not only used in software but is also widely used in designing hardware controlling software components. There are more than 930 million JRE downloads each year and 3 billion mobile phones run java.

Following are some other usage of Java:

1. Developing Desktop Applications
2. Web Applications like LinkedIn.com, Snapdeal.com etc
3. Mobile Operating System like Android
4. Embedded Systems
5. Robotics and games etc.

5.2 FEATURES OF JAVA

The prime reason behind creation of Java was to bring portability and security feature into a computer language. Beside these two major features, there were many other features that played an important role in moulding out the final form of this outstanding language. Those features are;

5.2.1 Simple

Java is easy to learn and its syntax is quite simple, clean and easy to understand.

The confusing and ambiguous concepts of C++ are either left out in Java or they have been re-implemented in a cleaner way.

Eg: Pointers and Operator Overloading are not there in Java but were an important part of C++.

5.2.2 Object Oriented

In Java everything is Object which has some data and behaviour. Java can be easily extended as it is based on Object Model.

5.2.3 Robust

Java makes an effort to eliminate error prone codes by emphasizing mainly on compile time error checking and runtime checking. But the main areas which Java improved were Memory Management and mishandled Exceptions by introducing automatic Garbage Collector and Exception Handling.

5.2.4 Platform Independent

Unlike other programming languages such as C, C++ etc. which are compiled into platform specific machines. Java is guaranteed to be write-once, run-anywhere language.

On compilation Java program is compiled into byte code. This byte code is platform independent and can be run on any machine, plus this byte code format also provides security. Any machine with Java Runtime Environment can run Java Programs.

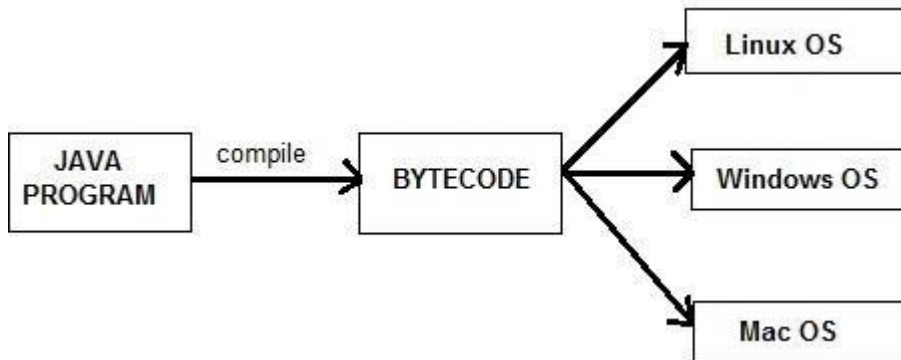


Fig 5.1 Diagram of Java program

5.2.5 Secure

When it comes to security, Java is always the first choice. With java secure features it enable us to develop virus free, temper free system. Java program always runs in Java runtime environment with almost null interaction with system OS, hence itis more secure.

5.2.6 Multi-Threading

Java multithreading feature makes it possible to write program that can do manytasks simultaneously. Benefit of multithreading is that it utilizes same memory and other resources to execute multiple threads at the same time, like While typing, grammatical errors are checked along.

5.2.7 Architectural Neutral

Compiler generates byte codes, which have nothing to do with a particular computer architecture, hence a Java program is easy to interpret on any machine.

5.2.8 Portable

Java Byte code can be carried to any platform. No implementation dependent features. Everything related to storage is predefined, ex : Data type

5.2.9 High Performance

Java is an interpreted language, so it will never be as fast as a compiled language like C or C++. But, Java enables high performance with the use of just-in-time compiler.

5.3 COLLECTION FRAMEWORK

Collection framework was not part of original Java release. Collections was added to J2SE 1.2. Prior to Java 2, Java provided adhoc classes such as Dictionary, Vector, Stack and Properties to store and manipulate groups of objects. Collection framework provides many important classes and interfaces to collect and organize group of alike objects.

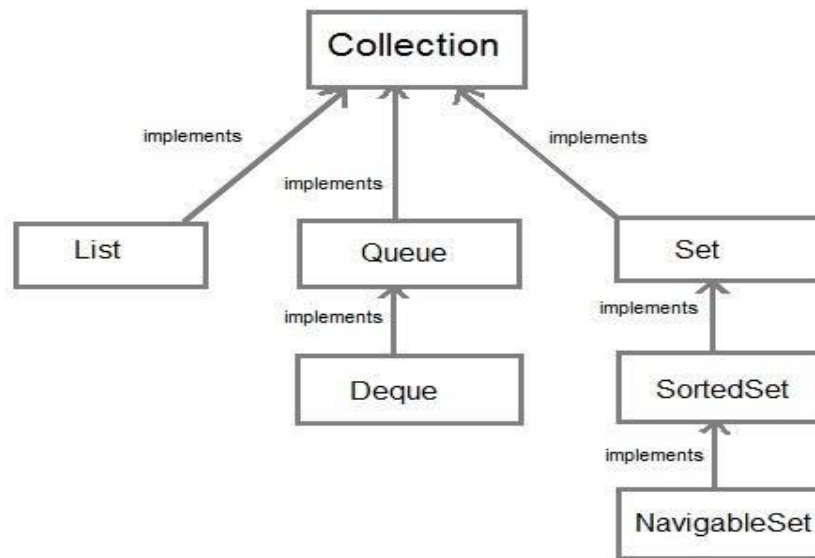


Fig 5.2 Collection Table of List, Queue and set

5.4 TESTING PROCESS

The purpose of testing is to discover errors. Testing is the process of trying to discover every conceivable fault or weakness in a work product. It provides a way to check the functionality of components, sub-assemblies, assemblies and/or a finished product it is the process of exercising software with the intent of ensuring that the Software system meets its requirements and user expectations and does not fail in an unacceptable manner. There are various types of test. 0Each test type addresses a specific testing requirement.

5.5 TYPES OF TESTS

5.5.1 Unit Testing

Unit testing involves the design of test cases that validate that the internal Program logic is functioning properly, and that program input produces valid Outputs. All decision branches and internal code flow should be validated. It is the testing of individual software units of the application .It is done after the Completion of an individual unit before integration. This is a structural testing, that relies on knowledge of its construction and is invasive. Unit tests perform basic tests at component level and test a specific business process, application, and/or system configuration. Unit tests ensure that each unique path of business process performs accurately to the documented specifications and contains clearly defined inputs and expected results.

5.5.2 Integration Testing

Integration tests are designed to test integrated software components to determine if they actually run as one program. Testing is event driven and is more concerned with the basic outcome of screens or fields. Integration tests demonstrate that although the components were individually satisfaction, as shown by successfully unit testing, the combination of components is correct and consistent. Integration testing is specifically aimed at exposing the problems that arise from the combination of components.

5.5.3 Functional Testing

Functional tests provide systematic demonstrations that functions tested are available as specified by the business and technical requirements, system documentation and user manuals. Systems/Procedures is used to interfacing systems or procedures must be invoked. Organization and preparation of functional tests is focused on requirements, key functions, or special test cases. In addition, systematic coverage pertaining to identify Business process flows; data fields, predefined processes, and successive. Processes must be considered for testing. Before functional testing is complete, additional tests are identified and the effective value of current tests is determined.

5.5.4 System Testing

System testing ensures that the entire integrated software system meets requirements. It tests a configuration to ensure known and predictable results. An example of system testing is the configuration-oriented system integration test. System testing is based on process descriptions and flows, emphasizing pre-Driven process links and integration points.

5.5.5 White Box Testing

White Box Testing is a testing in which the software tester has knowledge of the inner workings, structure and language of the software, or at least it's purpose. It is used to test areas that cannot be reached from a black box level.

5.5.6 Black Box Testing

Black Box Testing is testing the software without any knowledge of the inner workings, structure or language of the module being tested. Black box tests, as most other kinds of tests, must be written from a definitive source document, such as specification or requirements document, such as specification or requirement document. It is a testing in which the software under test is treated, as a black box .you cannot “see” into it. The test provides inputs and responds to outputs without considering how the software works.

5.6 TEST STRATEGY AND APPROACH

Field testing will be performed manually and functional tests will be written in detail.

Test Objectives

- All field entries must work properly.
- Pages must be activated from the identified link.
- The entry screen, messages and responses must not be delayed
- Features to be tested
- Verify that the entries are of the correct format
- No duplicate entries should be allowed
- All links should take the user to the correct page.

5.7 Integration Testing

Software integration testing is the incremental integration testing of two or more integrated software components on a single platform to produce failures caused by interface defects.

The task of the integration test is to check that components or software applications.

5.8 Acceptance Testing

User Acceptance Testing is a critical phase of any project and requires significant participation by the end user. It also ensures that the system meets the functional requirements.

5.8.3 ALPHA TESTING

In software development, alpha test will be a test among the teams to confirm that your product works. Originally, the term alpha test meant the first phase of testing in a software development process. The first phase includes unit testing, component testing, and system testing. It also enables us to test the product on the lowest common denominator machines to make sure download times are acceptable and preloads work.

5.8.4 BETA TESTING

In software development, a beta test is the second phase of software testing in which a sampling of the intended audience tries the product out. Beta testing can be considered “pre-release testing.” Beta test versions of software done

CHAPTER 6

RESULT AND DISCUSSION

6.1 RESULT

In this project, we propose a cloud auditing system for data storage security in Cloud Computing. We utilize the homomorphic linear authenticator and random masking to guarantee that the TPA would not learn any knowledge about the data content stored on the cloud server during the efficient auditing process, which not only eliminates the burden of cloud user from the tedious and possibly expensive auditing task, but also alleviates the users' fear of their outsourced data leakage. Considering TPA may concurrently handle multiple audit sessions from different users for their outsourced data files, we further extend our privacy preserving public auditing protocol into a multi-user setting, where the TPA can perform multiple auditing tasks in a batch manner for better efficiency. Extensive analysis shows that our schemes are provably secure and highly efficient.

6.2 DISCUSSION

In this section, we evaluate the performance of the proposed scheme by several experiments. The experiment was implemented using the Ubuntu 16.04 operating system with an Intel Core i5 3.0 GHz processor and an 8 GB memory. The programmer is written in C program, and it uses the library functions in the pairing based cryptography (PBC) library to simulate the cryptographic operations, where the benchmark threshold is 512 bits, the size of the element is $jjp = 160$ bits in Z_p , the size of the file is 20 MB, and the length of user identity to be 160 bits. the performance of signature generation and signature verification, we generate the signatures for different numbers of blocks from 0 to 1000 increased by an interval of 10 in our experiment. As shown in Figure 5, the time cost of the original signature generation, the final signature generation, and the signature generation with DAFCI all linearly increases with the number of the data blocks. The time of original signature generation

CHAPTER 7

7.1 CONCLUSION

This article proposed an efficient and secure public cloud data auditing scheme based on IoT scenarios. Through the encryption of sensitive information, the separation of private key method, and the two-time signature method, data sharing under privacy protection is realized, which reduce the computation and communication overhead of IoT devices, while ensured security. The security analysis shows that the scheme is safe under the random oracle model. Performance analysis shows that compared with traditional cloud data auditing schemes and other schemes using fog-to-cloud computing, the scheme is more efficient and has certain advantages, which can be better applied to low power IoT devices. However, considering the rapid development and widespread application of IoT technology, further reducing the overhead of computation and communication under the condition of ensuring the security of the solution will still be the focus of work in the future for a long time We utilize the homomorphic linear authenticator and random masking to guarantee that the TPA would not learn any knowledge about the data content stored on the cloud server during the efficient auditing process, which not only eliminates the burden of cloud user from the tedious and possibly expensive auditing task, but also alleviates the users' fear of their outsourced data leakage. Considering TPA may concurrently handle multiple audit sessions from different users for their outsourced data files, we further extend our privacy preserving public auditing protocol into a multi-user setting, where the TPA can perform multiple auditing tasks in a batch manner for better efficiency. Extensive analysis shows that our schemes are provably secure and highly efficient.

7.2 FUTURE WORK

Cloud computing is the future now a days because it will store in a cloud and it will sent to the third party auditor and third party auditor checks whether the cloud Data we entered is correct or not if the entered data is correct then it will sent to server so whatever data we are entering in our cloud is automatically storing

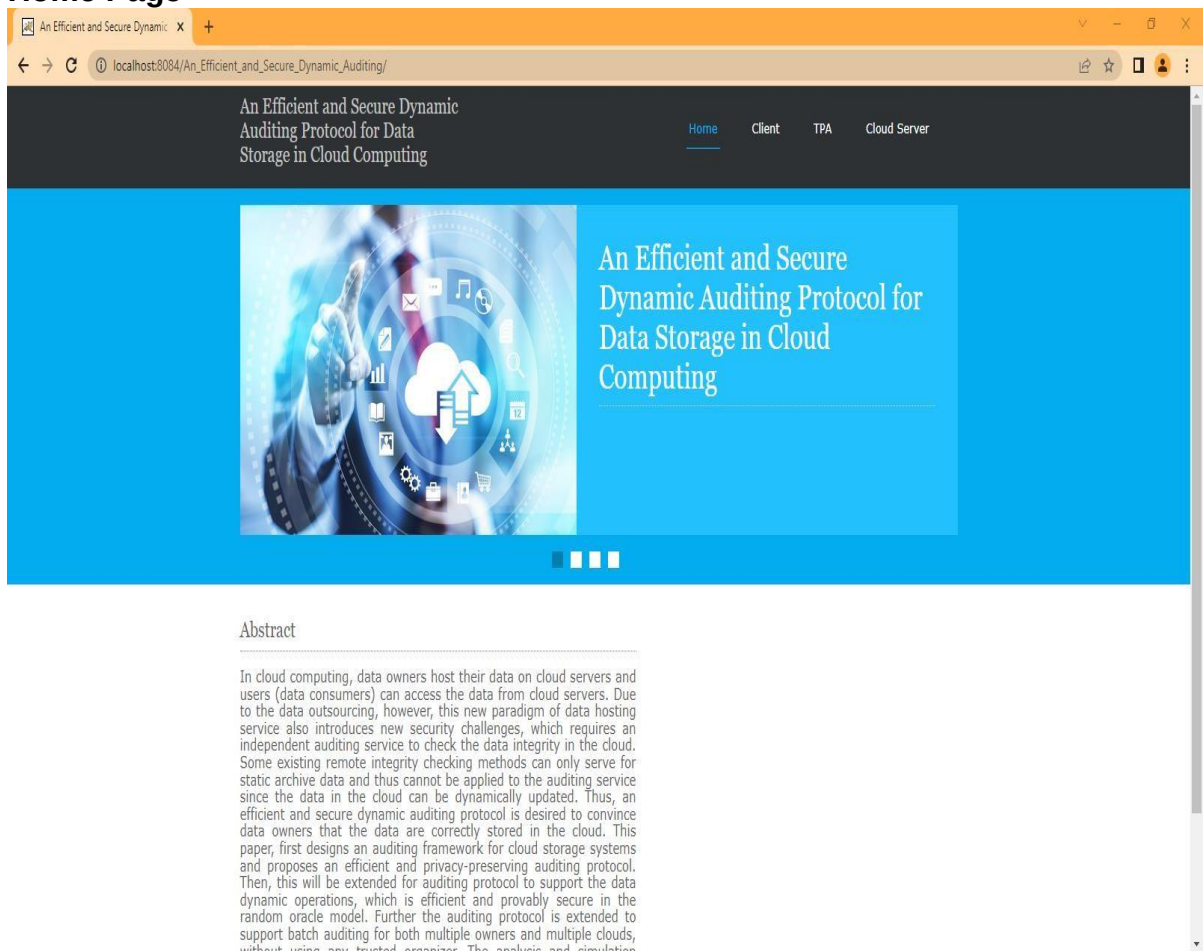
REFERENCE:

- [1.] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Storage Security in Cloud Computing," Proc. IEEE INFOCOM '10, Mar. 2010.
- [2.] P. Mell and T. Grance, "Draft NIST Working Definition of Cloud Computing," <http://csrc.nist.gov/groups/SNS/cloudcomputing/index.html>, June 2009.
- [3.] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "Above the Clouds: A Berkeley View of Cloud Computing," Technical Report UCB-EECS-2009-28, Univ. of California, Berkeley, Feb. 2009.
- [4.] Cloud Security Alliance, "Top Threats to Cloud Computing," <http://www.cloudsecurityalliance.org>, 2010.
- [5.] M. Arrington, "Gmail Disaster: Reports of Mass Email Deletions," <http://www.techcrunch.com/2006/12/28/gmail-disasterreportsof-mass-email-deletions/>, 2006.
- [6.] Roger Pressnma, "SOFTWARE ENGINEERING", 7 th edition
- [7.] YehudaShiran:Java Script Programming,2008.
- [8.] Holzner: HTML Black Book (HTML4)
- [9.] Patel moss:Java Database Programming with JDBC
- [10.] J2EE Professional by c
- [11.] Nick Todd: JAVA server pages

APPENDIX

A. SCREENSHOTS

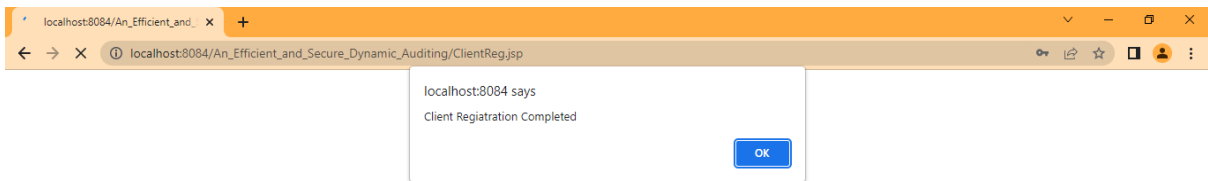
Home Page



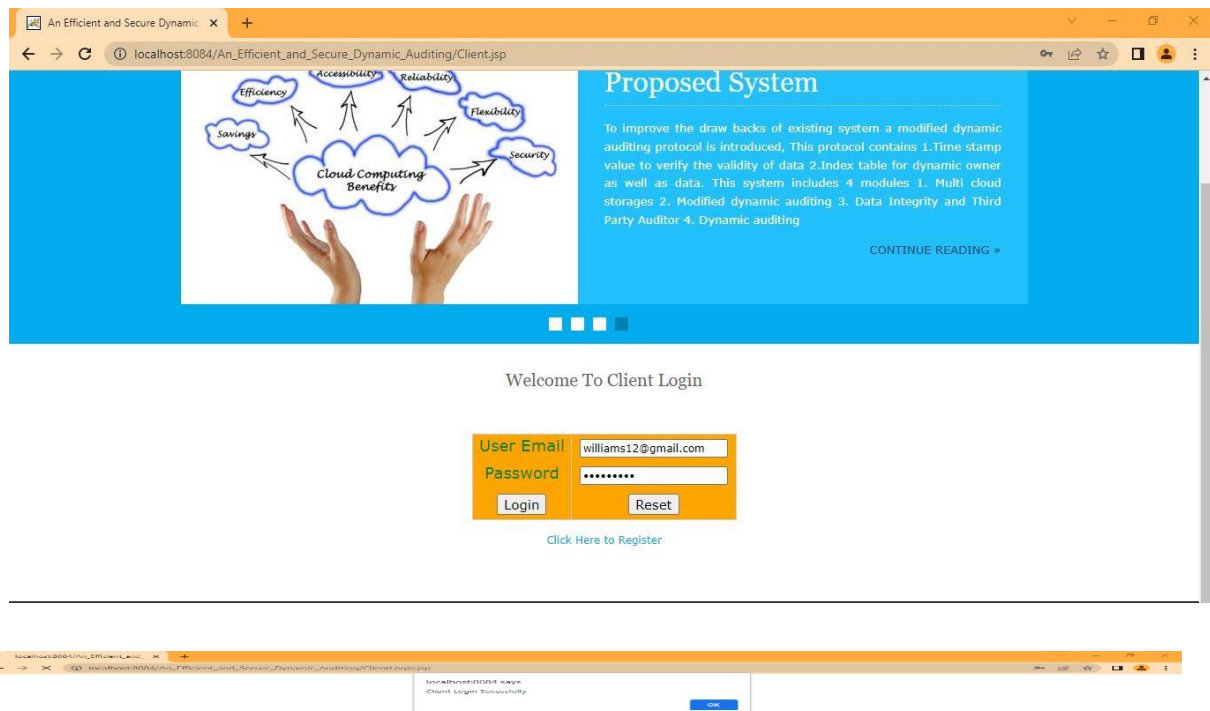
Client Registration Page

Welcome To Client Register

First Name	williams
Last Name	raj
Email ID	williams12@gmail.com
Mobile Number	9876543210
Location	chennai
Complete Address	Chennai
User Name	williams
Password	*****
Register	Reset



Client Login Page



An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing

Home
Logout

```

graph LR
    Clients -- Key Update Request --> TPA
    Clients -- Audit Delegation --> TPA
    TPA -- Audit Challenge --> Cloud
    Cloud -- Result --> TPA
    Clients <--> |Data Flow| Cloud
  
```

Abstract

In cloud computing, data owners host their data on cloud servers and users (data consumers) can access the data from cloud servers. Due to the data outsourcing, however, this new paradigm of data hosting service also introduces new security challenges, which requires an independent auditing service to check the data integrity in the cloud. Some existing remote integrity

[CONTINUE READING >](#)

Client Login

Click Here to send Key

Secret Key

SQLyog Enterprise - MySQL GUI - [New Connection - root@localhost]

File Edit Favorites DB Table Objects Tools Powertools Window Help

dynamic_auditing

Tables

block1
block2
block3
block4
block5
client
cloud
dhistory
files
otp
tpa
tpareq

Views
Stored Procs
Functions
Triggers

Query
QueryBuilder
SchemaDesigner

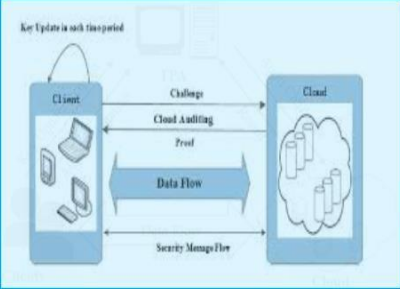
Autocomplete: [Tab]->Next Tag, [Ctrl+Space]->List Matching Tags, [Ctrl+Enter]->List All Tags.

```

1 /*
2 SQLyog Enterprise - MySQL GUI v6.56
3 MySQL - 5.0.67-community-nt : Database - dynamic_auditing
4 *****
5 */
6
7
8 /*140101 SET NAMES utf8 */;
9
10 /*140101 SET SQL_MODE='*/;
11
12
13 /*140014 SET @OLD_FOREIGN_KEY_CHECKS=@@FOREIGN_KEY_CHECKS, FOREIGN_KEY_CHECKS=0 */;
14 /*140101 SET @OLD_SQL_MODE=@@SQL_MODE, SQL_MODE='NO_AUTO_VALUE_ON_ZERO' */;
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1090
1091
1092
1093
1094
1095
1096
1097
1098
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1190
1191
1192
1193
1194
1195
1196
1197
1198
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1289
1290
1291
1292
1293
1294
1295
1296
1297
1298
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1389
1390
1391
1392
1393
1394
1395
1396
1397
1398
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1489
1490
1491
1492
1493
1494
1495
1496
1497
1498
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1689
1690
1691
1692
1693
1694
1695
1696
1697
1698
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1789
1790
1791
1792
1793
1794
1795
1796
1797
1798
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1889
1890
1891
1892
1893
1894
1895
1896
1897
1898
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
2031
2032
2033
2034
2035
2036
2037
2038
2039
2040
2041
2042
2043
2044
2045
2046
2047
2048
2049
2050
2051
2052
2053
2054
2055
2056
2057
2058
2059
2060
2061
2062
2063
2064
2065
2066
2067
2068
2069
2070
2071
2072
2073
2074
2075
2076
2077
2078
2079
2080
2081
2082
2083
2084
2085
2086
2087
2088
2089
2090
2091
2092
2093
2094
2095
2096
2097
2098
2099
2100
2101
2102
2103
2104
2105
2106
2107
2108
2109
2110
2111
2112
2113
2114
2115
2116
2117
2118
2119
2120
2121
2122
2123
2124
2125
2126
2127
2128
2129
2130
2131
2132
2133
2134
2135
2136
2137
2138
2139
2140
2141
2142
2143
2144
2145
2146
2147
2148
2149
2150
2151
2152
2153
2154
2155
2156
2157
2158
2159
2160
2161
2162
2163
2164
2165
2166
2167
2168
2169
2170
2171
2172
2173
2174
2175
2176
2177
2178
2179
2180
2181
2182
2183
2184
2185
2186
2187
2188
2189
2190
2191
2192
2193
2194
2195
2196
2197
2198
2199
2200
2201
2202
2203
2204
2205
2206
2207
2208
2209
2210
2211
2212
2213
2214
2215
2216
2217
2218
2219
2220
2221
2222
2223
2224
2225
2226
2227
2228
2229
2230
2231
2232
2233
2234
2235
2236
2237
2238
2239
2240
2241
2242
2243
2244
2245
2246
2247
2248
2249
2250
2251
2252
2253
2254
2255
2256
2257
2258
2259
2260
2261
2262
2263
2264
2265
2266
2267
2268
2269
2270
2271
2272
2273
2274
2275
2276
2277
2278
2279
2280
2281
2282
2283
2284
2285
2286
2287
2288
2289
2290
2291
2292
2293
2294
2295
2296
2297
2298
2299
2300
2301
2302
2303
2304
2305
2306
2307
2308
2309
2310
2311
2312
2313
2314
2315
2316
2317
2318
2319
2320
2321
2322
2323
2324
2325
2326
2327
2328
2329
2330
2331
2332
2333
2334
2335
2336
2337
2338
2339
2340
2341
2342
2343
2344
2345
2346
2347
2348
2349
2350
2351
2352
2353
2354
2355
2356
2357
2358
2359
2360
2361
2362
2363
2364
2365
2366
2367
2368
2369
2370
2371
2372
2373
2374
2375
2376
2377
2378
2379
2380
2381
2382
2383
2384
2385
2386
2387
2388
2389
2390
2391
2392
2393
2394
2395
2396
2397
2398
2399
2400
2401
2402
2403
2404
2405
2406
2407
2408
2409
2410
2411
2412
2413
2414
2415
2416
2417
2418
2419
2420
2421
2422
2423
2424
2425
2426
2427
2428
2429
2430
2431
2432
2433
2434
2435
2436
2437
2438
2439
2440
2441
2442
2443
2444
2445
2446
2447
2448
2449
2450
2451
2452
2453
2454
2455
2456
2457
2458
2459
2460
2461
2462
2463
2464
2465
2466
2467
2468
2469
2470
2471
2472
2473
2474
2475
2476
2477
2478
2479
2480
2481
2482
2483
2484
2485
2486
2487
2488
2489
2490
2491
2492
2493
2494
2495
2496
2497
2498
2499
2500
2501
2502
2503
2504
2505
2506
2507
2508
2509
2510
2511
2512
2513
2514
2515
2516
2517
2518
2519
2520
2521
2522
2523
2524
2525
2526
2527
2528
2529
2530
2531
2532
2533
2534
2535
2536
2537
2538
2539
2540
2541
2542
2543
2544
2545
2546
2547
2548
2549
2550
2551
2552
2553
2554
2555

```

An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing
HomeLogout



Existing System

To solve the data privacy problem, existing method is to generate an encrypted proof with the challenge stamp by using the Bilinearity property of the bilinear pairing, such that the auditor cannot decrypt it but can verify the correctness of the proof. Without using the mask technique, this method does not require any trusted organizer during the batch auditing for multiple clouds. Therefore, existing method can greatly reduce the computing loads of the auditor by moving it to the cloud server

CONTINUE READING >

key verify

Enter Key

63305

Verify

Reset

Upload File

An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing
HomeUpload FilePacket SendingDownloadHistoryLogout



An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing

Welcome to Client Home : williams12@gmail.com

An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing

Home
Upload File
Packet Sending
Download
History
Logout

```

graph TD
    Clients -- Key Update Request --> TPA
    TPA -- Audit Delegation --> Cloud
    Cloud -- Audit Challenge --> TPA
    TPA -- Result --> Cloud
    Clients <--> |Data Flow| Cloud
  
```

Abstract

In cloud computing, data owners host their data on cloud servers and users (data consumers) can access the data from cloud servers. Due to the data outsourcing, however, this new paradigm of data hosting service also introduces new security challenges, which requires an independent auditing service to check the data integrity in the cloud. Some existing remote integrity

[CONTINUE READING »](#)

Upload File Here

File ID

9

Subject

demo

Choose File

Choose File

demo.txt

Upload

Packet Sending Page

An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing

File Sending With Meta Key

Blocks	Secrete Key	Metadata Key	Status	Send
Block1	a	610621	Block1 Sent	☐
Block2	b	858042	Block2 Sent	☐
Block3	c	110746	Block3 Sent	☐
Block4	d	790667	Block4 Sent	☐
Block5	e			☒

Each Block Size

9.0 Bytes

Total Size

45.0 Bytes

Back

localhost:8084/An_Efficient_and_Secure_Dynamic_Auditing/Block5.jsp

localhost:8084 says
File sent to SERVER with metadata key &Alert sent to TPA.

OK

An Efficient and Secure Dynamic
+
localhost:8084/An_Efficient_and_Secure_Dynamic_Auditing/PacketSendin.jsp



Data Storage in Cloud Computing

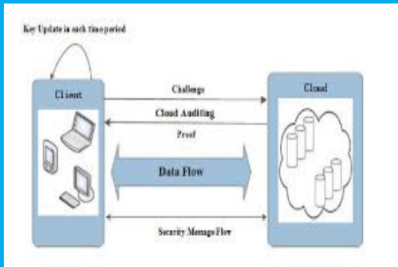
File Sending With Meta Key

Blocks	Secrete Key	Metadata Key	Status
Block1	a	610621	Block1 Sent
Block2	b	858042	Block2 Sent
Block3	c	110746	Block3 Sent
Block4	d	790667	Block4 Sent
Block5	e	933006	Block5 Sent

Back

TPA Login Page

An Efficient and Secure Dynamic
+
localhost:8084/An_Efficient_and_Secure_Dynamic_Auditing/TPALogin.jsp



Existing System

To solve the data privacy problem, existing method is to generate an encrypted proof with the challenge stamp by using the Bilinearity property of the bilinear pairing, such that the auditor cannot decrypt it but can verify the correctness of the proof. Without using the mask technique, this method does not require any trusted organizer during the batch auditing for multiple clouds. Therefore, existing method can greatly reduce the computing loads of the auditor by moving it to the cloud server.

[CONTINUE READING >](#)

Welcome To TPA Page

TPA Login

User Name

Password

localhost:8084 says
TPA login succesfully

OK

An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing
HomeAlert MessageKey ResponseLogout



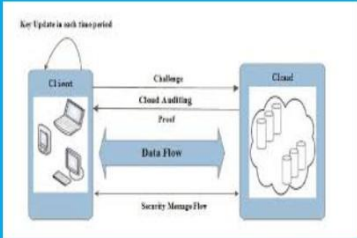
Welcome
TPA

Abstract

In cloud computing, data owners host their data on cloud servers and users (data consumers) can access the data from cloud servers. Due to the data outsourcing, however, this new paradigm of data hosting service also introduces new security challenges, which requires an independent auditing service to check the data integrity in the cloud. Some existing remote integrity checking methods can only serve for static archive data and thus cannot be applied to the auditing service.

TPA Alert Message Page

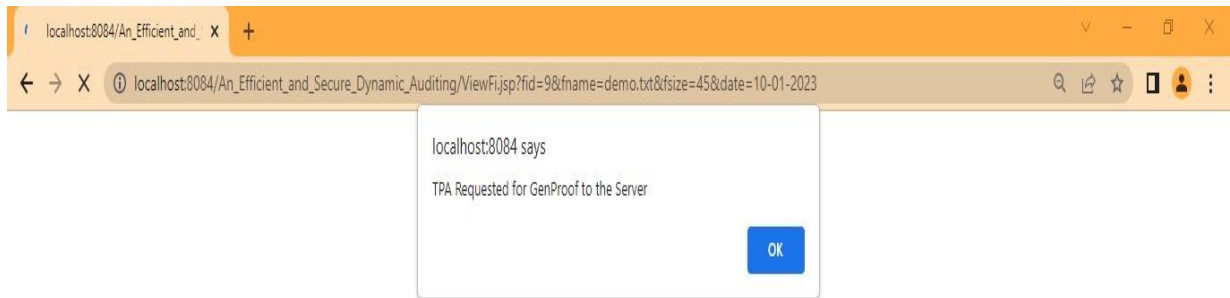
An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing
HomeAlert MessageKey ResponseLogout



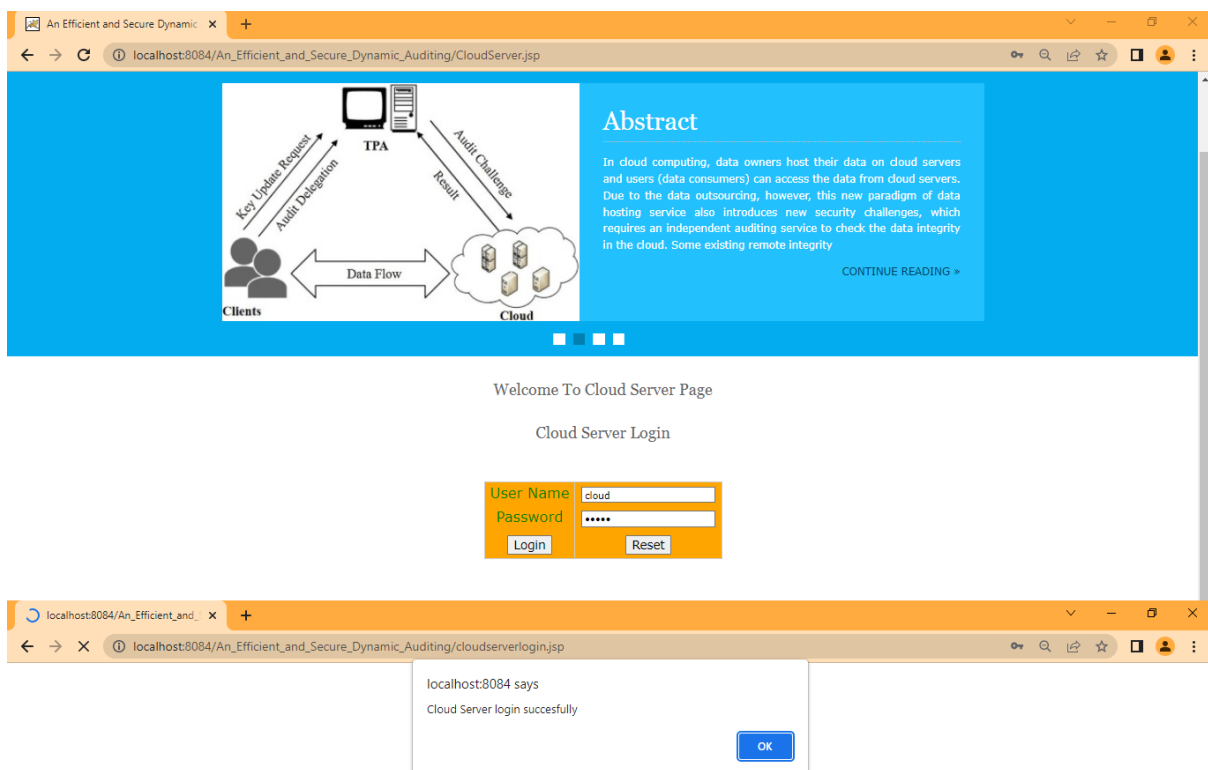
Existing System

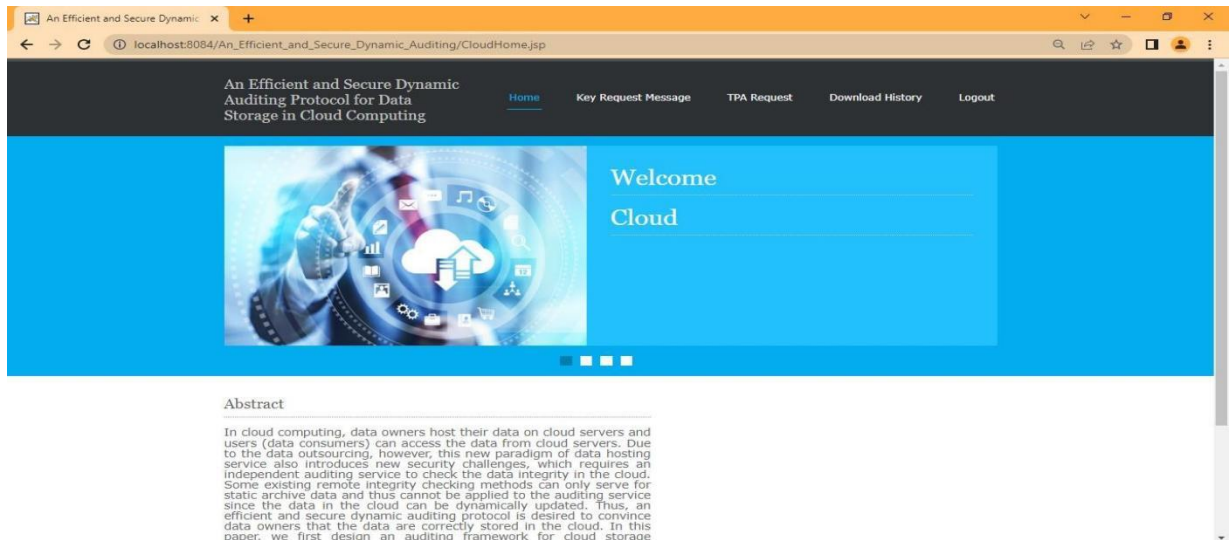
To solve the data privacy problem, existing method is to generate an encrypted proof with the challenge stamp by using the bilinearity property of the bilinear pairing, such that the auditor cannot decrypt it but can verify the correctness of the proof. Without using the mask technique, this method does not require any trusted organizer during the batch auditing for multiple clouds. Therefore, existing method can greatly reduce the computing loads of the auditor by moving it to the cloud server.

File ID	File Name	Total Bytes	Date	Send
1	aboutjava.txt	32	28-02-2019	send To Server
4	hello.txt	11	12-03-2019	send To Server
5	New Text Document.txt	14	13-03-2019	send To Server
6	New Text Document (2).txt	13	13-03-2019	send To Server
8	fgg.txt	10	13-03-2019	send To Server
9	demo.txt	45	10-01-2023	send To Server



Cloud Server Login Page





Key Request Message Page

An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing

Home Key Request Message TPA Request Download History Logout

Proposed System

To improve the draw backs of existing system a modified dynamic auditing protocol is introduced, This protocol contains 1. Time stamp value to verify the validity of data 2. Index table for dynamic owner as well as data. This system includes 4 modules 1. Multi cloud storages 2. Modified dynamic auditing 3. Data Integrity and Third Party Auditor 4. Dynamic auditing.

[CONTINUE READING »](#)

File ID	File Name	Total Bytes	Date
1	aboutjava.txt	32	28-02-2019
4	hello.txt	11	12-03-2019
5	New Text Document.txt	14	13-03-2019
6	New Text Document (2).txt	13	13-03-2019
8	fgg.txt	10	13-03-2019
9	demo.txt	45	10-01-2022

TPA Request Page

An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing

HomeKey Request MessageTPA RequestDownload HistoryLogout

```
graph TD
    Clients -- Key Update Request --> TPA
    TPA -- Audit Delegation --> Cloud
    Cloud -- Audit Challenge --> TPA
    TPA -- Result --> Cloud
    Clients <--> |Data Flow| Cloud
```

Abstract

In cloud computing, data owners host their data on cloud servers and users (data consumers) can access the data from cloud servers. Due to the data outsourcing, however, this new paradigm of data hosting service also introduces new security challenges, which requires an independent auditing service to check the data integrity in the cloud. Some existing remote integrity

CONTINUE READING >

File ID	File Name	Total Bytes	Date	Generate Proof
6	New Text Document (2).txt	13	13-03-2019	<button>Generate GenProof of this file</button>
9	demo.txt	45	10-01-2023	<button>Generate GenProof of this file</button>

An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing

HomeKey Request MessageTPA RequestDownload HistoryLogout

```
graph TD
    Clients -- Key Update Request --> TPA
    TPA -- Audit Delegation --> Cloud
    Cloud -- Audit Challenge --> TPA
    TPA -- Result --> Cloud
    Clients <--> |Data Flow| Cloud
```

Abstract

In cloud computing, data owners host their data on cloud servers and users (data consumers) can access the data from cloud servers. Due to the data outsourcing, however, this new paradigm of data hosting service also introduces new security challenges, which requires an independent auditing service to check the data integrity in the cloud. Some existing remote integrity

CONTINUE READING >

File ID	File Name	Total Bytes	Date	Generate Proof
6	New Text Document (2).txt	13	13-03-2019	<button>Generate GenProof of this file</button>

SQLyog Enterprise - MySQL GUI - [New Connection - root@localhost]

File Edit Favorites DB Table Objects Tools Powertools Window Help

root@localhost
 information_schema
 carproject
 carrental
 cars
 dynamic_auditing
 Tables
 block1
 block2
 block3
 block4
 block5
 client
 cloud
 dhistory
 files
 otp
 tpa
 tpareq
 Views
 Stored Procs
 Functions
 Triggers

QueryBuilder SchemaDesigner

Autocomplete: [Tab]->Next Tag. [Ctrl+Space]->List Matching Tags. [Ctrl+Enter]->List All Tags.

```

1  /*
2  SQLyog Enterprise - MySQL GUI v6.56
3  MySQL - 5.0.67-community-nt : Database - dynamic_auditing
4  *****
5  */
6
7
8  /*140101 SET NAMES utf8 */;
9
10 /*140101 SET SQL_MODE='';*/
11
12 /*140014 SET @OLD_FOREIGN_KEY_CHECKS=@@FOREIGN_KEY_CHECKS, FOREIGN_KEY_CHECKS=0 */;
13 /*140101 SET @OLD_SQL_MODE=@@SQL_MODE, SQL_MODE='NO_AUTO_VALUE_ON_ZERO' */;
14
15

```

1 Messages 2 Table Data 3 Objects 4 History

Show All Or Limit 0 50 Refresh

fid	fname	fsize	fdate	proof	tpaperm
1	aboutjava.txt	32	28-02-2019	384CD856E6	Granted
4	hello.txt	11	12-03-2019	R22D816DCa	Granted
5	New Text Document.txt	14	13-03-2019	1sa5k3baak	Granted
6	New Text Document (2).txt	13	13-03-2019	waiting	waiting
8	fgg.txt	10	13-03-2019	DG1D65E3C4	Granted
9	demo.txt	45	10-01-2023	k131jR2D5b	waiting
*	(NULL)	(NULL)	(NULL)	(NULL)	(NULL)

Key Response From Cloud Page

An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing

Home Alert Message Key Response Logout

Abstract

In cloud computing, data owners host their data on cloud servers and users (data consumers) can access the data from cloud servers. Due to the data outsourcing, however, this new paradigm of data hosting service also introduces new security challenges, which requires an independent auditing service to check the data integrity in the cloud. Some existing remote integrity

[CONTINUE READING »](#)

File ID	File Name	Total Bytes	Date	GenProof Key	Send To Client
1	aboutjava.txt	32	28-02-2019	384CD856E6	Send To Client
4	hello.txt	11	12-03-2019	R22D816DCa	Send To Client
5	New Text Document.txt	14	13-03-2019	1sa5k3baak	Send To Client
8	fgg.txt	10	13-03-2019	DG1D65E3C4	Send To Client
9	demo.txt	45	10-01-2023	k131jR2D5b	Send To Client

SQLyog Enterprise - MySQL GUI - [New Connection - root@localhost]

File Edit Favorites DB Table Objects Tools Powertools Window Help

dynamic_auditing

root@localhost

- information_schema
- carproject
- carrental
- cars
- dynamic_auditing
 - Tables
 - block1
 - block2
 - block3
 - block4
 - block5
 - client
 - cloud
 - dhistory
 - files
 - otp
 - tps
 - tpareq
 - Views
 - Stored Procs
 - Functions
 - Triggers

Query

QueryBuilder SchemaDesigner

Autocomplete: [Tab]->Next Tag. [Ctrl+Space]->List Matching Tags. [Ctrl+Enter]->List All Tags.

```

1 /*
2 SQLyog Enterprise - MySQL GUI v6.56
3 MySQL - 5.0.67-community-nt : Database - dynamic_auditing
4
5 */
6
7
8 /*140101 SET NAMES utf8 */;
9
10 /*140101 SET SQL_MODE='*/;
11
12 /*140014 SET @OLD_FOREIGN_KEY_CHECKS=@@FOREIGN_KEY_CHECKS, FOREIGN_KEY_CHECKS=0 */;
13 /*140101 SET @OLD_SQL_MODE=@@SQL_MODE, SQL_MODE='NO_AUTO_VALUE_ON_ZERO' */;

```

1 Messages 2 Table Data 3 Objects 4 History

Show All Or Limit 50 Refresh

fid	fname	fsize	fdate	proof	tpaperm
1	aboutjava.txt	32	28-02-2019	384CD856E6	Granted
4	hello.txt	11	12-03-2019	R22D81EDCa	Granted
5	New Text Document.txt	14	13-03-2019	1aa5k3baak	Granted
6	New Text Document (2).txt	13	13-03-2019	waiting	waiting
8	fgg.txt	10	13-03-2019	D01D6E3C4	Granted
9	demo.txt	45	10-01-2023	kl3ljR2DSb	Granted
(NULL)	(NULL)	(NULL)	(NULL)	(NULL)	(NULL)

File Download Page

An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing

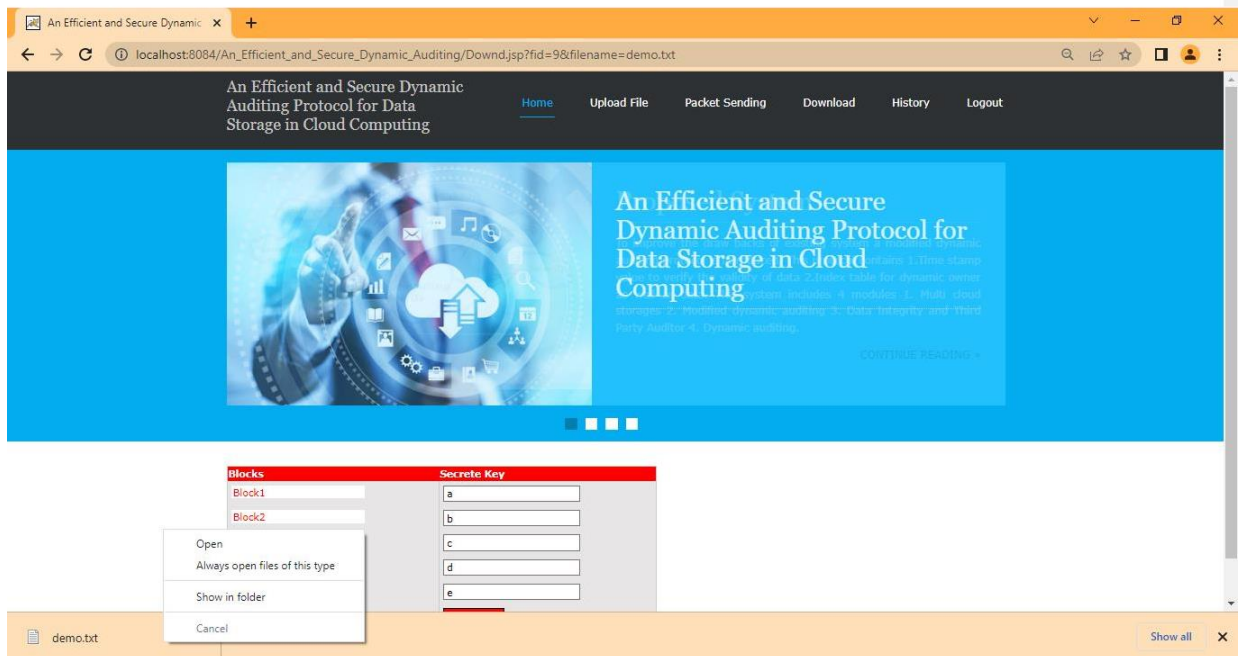
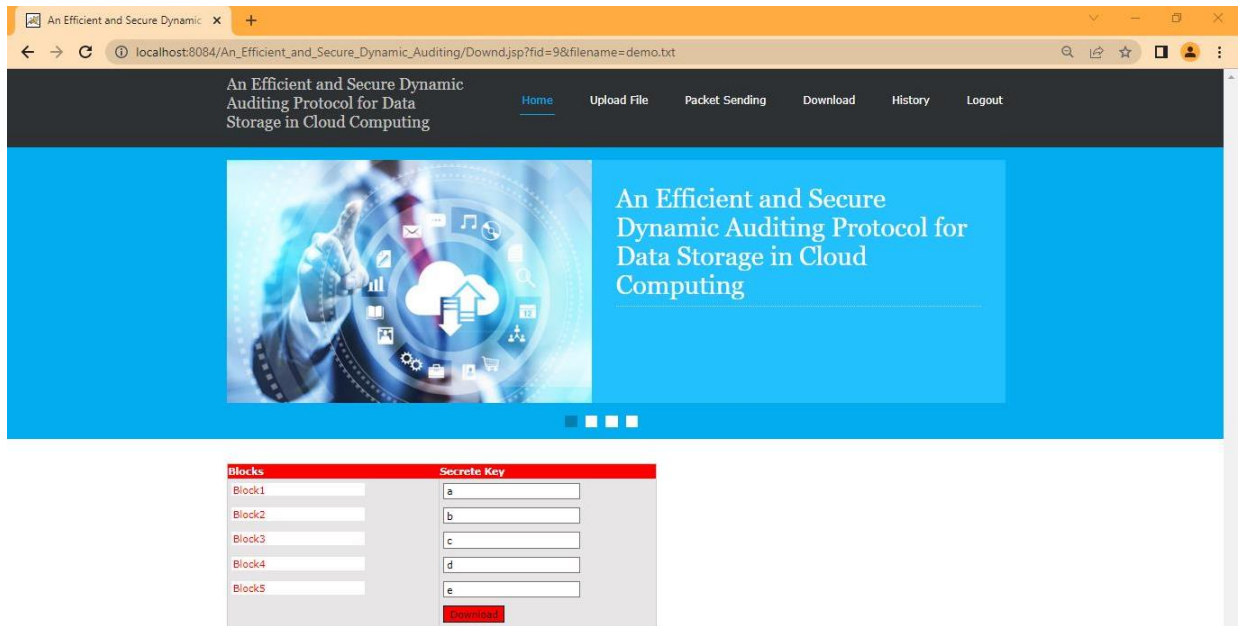
Home Upload File Packet Sending Download History Logout

Abstract

In cloud computing, data owners host their data on cloud servers and users (data consumers) can access the data from cloud servers. Due to the data outsourcing, however, this new paradigm of data hosting service also introduces new security challenges, which requires an independent auditing service to check the data integrity in the cloud. Some existing remote integrity

CONTINUE READING »

File ID	File Name	Total Bytes	Date	Download
1	aboutjava.txt	32	28-02-2019	Download
4	hello.txt	11	12-03-2019	Download
5	New Text Document.txt	14	13-03-2019	Download
8	fgg.txt	10	13-03-2019	Download
9	demo.txt	45	10-01-2023	Download



Download History in Client Page

An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing

Home Upload File Packet Sending Download History Logout

Welcome to Client Home :williams12@gmail.com

DOWNLOAD HISTORY

FileName	Downloaded Date
demo.txt	2023-01-10 12:21:04

demo.txt Show all

Download History in Cloud Page

An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing

Home Key Request Message TPA Request Download History Logout

Welcome to Cloud Downloads History

DOWNLOAD HISTORY

Email address	FileName	Downloaded Date
yashwanth12boinpally@gmail.com	aboutjava.txt	2019-02-28 16:28:08
williams12@gmail.com	demo.txt	2023-01-10 12:21:04

EFFICIENT AUDITING SCHEME FOR SECURE DATA STORAGE IN FOG-TO-CLOUD COMPUTING

Thanisha Valli Mohammad
Student
Sathyabama Institute Of Science & Technology
Chennai, India
md.thanishavalli786@gmail.com

S.Karthikeyan
Associate Professor
Sathyabama Institute Of Science & Technology
Chennai, India
karthijoy1@gmail.com

Boddepalli Hanish
Student
Sathyabama Institute of Science & Technology
Chennai, India
hanish.cpwd@gmail.com

Vijaybaskar
Associate Professor
Sathyabama Institute of Science & Technology
Chennai, India
vvijaybaskar@yahoo.co.in

Abstract

Most effective regulations arise as in the garbage since the cops who implement them aren't to be had to the correct individuals. Thus, a reliable and evident gadget is needed to enable a random man or woman to apply quickly for the reason and to music the state of the time and to identify whether he's qualified for the foetus or if his software has been refused using the help of the government. With our system, the administrator will add the details of the scheme to the account. And the individual may examine the user statistics. And he may go or reject the advice requested by the consumer. And the individual may examine the renown of the request aircraft

INTRODUCTION:

The purpose of Government Scheme Alerts is to make them less complicated and to save time while enrolling for and utilising programme offers..The Public Alerts System is aimed to give a clear and appealing device. Government Programme Alerts assist the person to apply without delay for the scheme and reveal their status now and again. Because of this, the web

page assists to discover if the customer is eligible to acquire the advantages, or whether his application has been declined by means of the authorities. This website is beneficial for everyone and anyone to review the present kingdom call for degree system. permits customers to carry out diverse operations. It is recognised that under a public audit system, the duty of validating the integrity of person statistics can be outsourced to a 3rd celebration auditor (TPA) who might also have more auditing expertise and greater computing skills. . But it have to additionally be cited that public accounting structures are much less green than non-public ones. As Zhang et al., as proven in fig. , for the equal record marking, the time to test, affirm, and pass in the public accounting scheme, is hundreds (or even heaps) of times more than the time required for the due system in its private design. Therefore, in some performance-looking for situations, particularly for useful resource-restricted cellular receivers of cloud computing, we consider that personal

Lastly, We also explore and compare the features of our proposed device with those of Tian et al. He also hears two popular cloud technologies. The testing results indicate that Tian et al. modified our device. Communication costs and computational performance

SCOPE OF THE PROJECT

Making it simpler to sign up for Government Scheme Alerts and making the most of them are the two main goals of Government Scheme Alerts. scheme services.. The Public Alerts System is meant to deliver a clear and attractive gadget.. Government Scheme Alerts help the individual to apply without delay for the scheme and show their status now and again. Because of this, the web website helps to realise whether the client is entitled to acquire the benefits, or if his application has been refused by means of the authorities. This website is handy for everyone and everybody to examine the current kingdom call for degree system.

LITERATURE SURVEY

The most crucial stage of the software development process is literature analysis. When building the device, examine the time constraint, the financial system, and the employer's power. If these standards are fulfilled, the next step is to choose which operating system and language will be used to improve the item. As programmers start building a tool, they seek a range of outside help. This assistance may be obtained via older software, books, or the internet. Such problems are taken into account before expanding a system when the device is being expanded. Consideration and completeness are critical components of job enhancement.

Learning all of the qualifications required for employment advancement. For any reason, literature research is the most important aspect of the software development procedure. Before extending the key gear and tactics, it is much more important to identify the time problem and the interest, the desire for sources, the hard work force, the financial system, and the organization's strength. With this information finished and properly understood, the following stage is to pick the software specification within the specific device, as to what kind of working machine is required for the purpose, and what is intended to carry in all of the major software programmes. About the subsequent efforts to increase required equipment and operations

Investigation on a Government Program Based on Multi-Technology and Bi-Directional Authentication

Authentication is a critical a component of network safety. This is also the fundamental difficulty to be overcome. This bi-directional design, uses a multi-mechanism to deliver pleasant authentication and an unmarried authentication service for various e- authority utility structures, meets the necessities of the prevailing e-government device. However, authentication era and e-authorities structures are continuously evolving and many troubles continue to be to be solved. [Author: Li Liangzhi (2017)]

Analysis of E-government Services Outsourcing and Incentive Scheme

Related theories, work mechanisms and traits in e-governance are investigated. Then, an evaluation of the version and motivation of the governance machine and the initiative within the e-government of the rising promise in the sport and the most important agent theories with a focus at the

motivation and overall performance assessment inside the rising enterprise management is supplied, in which it's miles important. The game stimulus is alsoderived from the predominant-agent. The presence of incomplete and uneven recordsis vital for making use of rewards and punishments before enough analysis has been completed. From the factor of view of a certain evaluation, the ideal deliver can have the characteristics of monotonicity, this is, the praise supplied to the supervisorby means of the nation have to growth with an boom within the degree of output. Finally, it's far concluded that e-governance reform proposals require an incentive machine. [Or: Jiang Hong (2018)]

A Risk Assessment Model for E-Government Information Systems Based on the Business Circle

With a quick expansion of laptop networks and statistical technology, they serve many walks of the life in China. The Chinese government makes extensive use of information and network technologies to boost its job. Hence, China's e-authorities statistics gadget is expanding swiftly. But, in reality, the e-authorities statistics machine has certain features and some competence threats in China, which influences the wholesome and favorable improvement of the e- government records system. It isn't sufficient that some at ease products and gear are used simplest for the safety of the digital data system structure. In orderto make sure a dependable and accurate structure of the electronic facts machine architecture, risk assessment and control are vital for a reliable and dependable e- authorities information gadget. The article proposes a hazard evaluation model primarily based on the business of the "Electronic Government"

totally at the records of the "Electronic Government" machine. The model shows some enterprise circles in keeping with the importance and functions of the information gadget "Electronic Government". Also, in every enterprise, chance evaluation is completed. The model introduces the concept of chance evaluation, danger assessment approach, chance evaluation procedure and threat calculation technique.

A secure publishing scheme in e-Government

One of the maximum vital capabilities of e-mail over the Internet is dissemination. Although a digital signature may be used to protect the integrity and authenticity of public facts, it can't efficaciously resist malicious spoofing in situations where the public statistics is composed of various documents. A relaxed hashing schemebased totally on a Merkle hash tree is proposed. The design can face up to malicious spoofing of public facts, and its value is low.

EXISTING SYSTEM

In this state of affairs, various authorities schemes are posted within the print media and promulgated with the aid of the relevant authorities. It is regularly hard for humans to get the applicable records and turn to the police services. Because of the shortage of proper communique among the numerous departments and officials, frequently the technical intention become no longer performed. Individuals do now not learn out about the tactics and did not profit from them.

PROPOSED SYSTEM

This recommended device was an internet service that keeps a consolidated repository of all information related with the schism.

easier it's miles to locate the information you need. Users and the public can access the account to acquire facts as well as go online to apply targeted tricks. The gadget entails coordination between all departments and officers. The gadget additionally allows everyday monitoring and amendment of records.

ADVANTAGES OF PROPOSED SYSTEM

- Provides all policies issued with the help of the government.
- Announcement of each new event.
- Display notifications on most critical pages.
- User registration method.
- Login authentication.
- Enables customers to test their renowned facts.

ARCHITECTURE DIAGRAM

SYSTEM REQUIREMENTS

HARDWARE REQUIREMENTS:

- | | |
|-------------|--------------------|
| • System | - Windows 7/10 \s• |
| • Speed | - 2.4GHZ \s• |
| • Hard disk | - 40GB \s• |
| • Monitor | - 15VGA colour \s• |
| • RAM | - 4GB |

SOFTWARE REQUIREMENTS:

- Operating System - Windows 10. \s•
- Coding language - Java \s•
- **IDE** - NetBeans
- Backend - Mysql

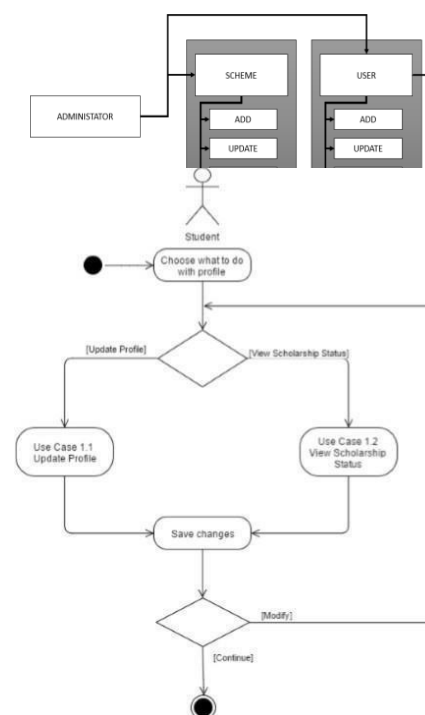
UML DIAGRAM

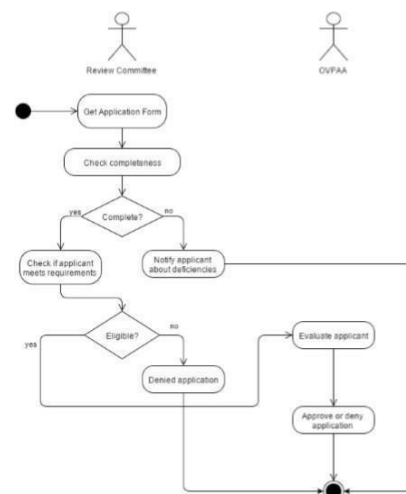
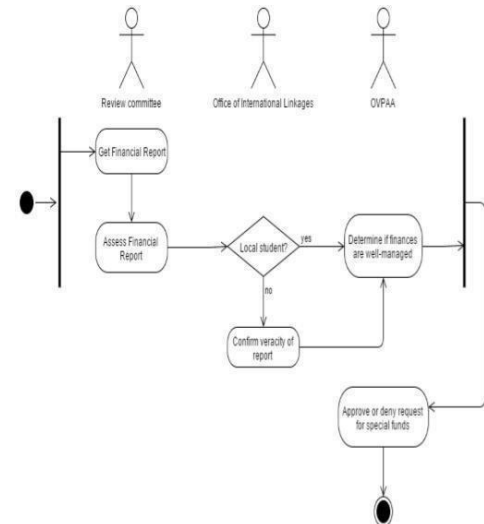
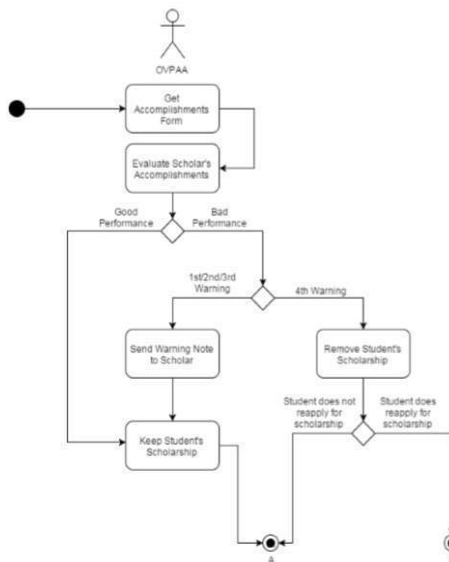
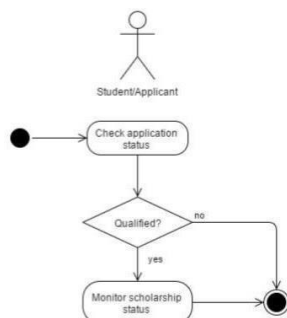
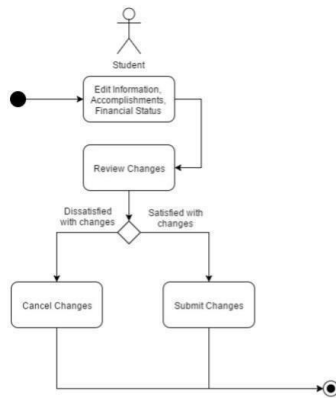
UML is a way of defining the architecture of a device using a specific diagram. UML Sets engineering great

approaches which have proved to be beneficial in modelling vast and sophisticated structures. UML is a vital a part of item-focused software programme improvement and the software programme development method. UML specifically makes use of graphical notation to organise software operations. UML aids design teams in communicating, exploring capacity designs, and evaluating software architecture design.

ACTIVITY DIAGRAM

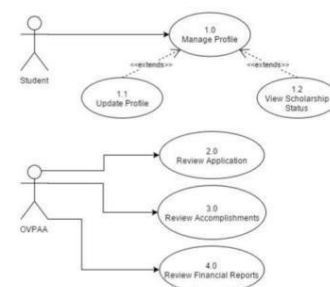
Actions describe conduct in a machine's workflow. Action diagrams are just like country diagrams because movements are states of doing something. Diagrams describe the kingdom of sports with the aid of displaying the collection of sports that take location. Action diagrams can represent actions which are conditional or parallel.





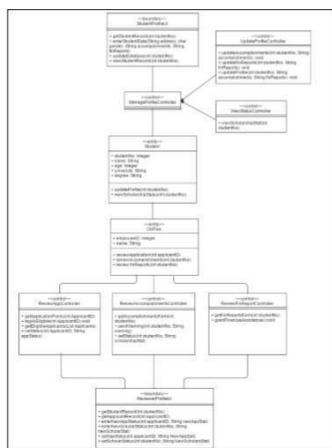
USECASE DIAGRAM

A use case diagram in the Unified Modeling Language (UML) is a kind of behavioural diagram that has been described and created by use-case research. Its goal is to offer a graphical representation of a system's operation in terms of actors, objectives (expressed as use cases), and any interactions between those use cases.



CLASS DIAGRAM

The many kinds of components in a system and their relationships are often described using class diagrams. Class diagrams are used to explain Design components like as classes, packages, and objects are used to create class structure and content. When developing a system, class diagrams allow for three distinct views: conceptual, specification, and implementation. Various points of view become obvious as the diagram is constructed and assist to reinforce the concept. The most typical UML diagram is probably a class diagram. It is a crucial component of any object-oriented system. It displays the classes in a system, their properties and behavior, and the connections between them. The name is at the top, the characteristics are in the middle, and the operations or methods are at the bottom of a class in the majority of modelling tools. Comparable classes are grouped together to create class diagrams in complex systems with numerous classes. Several types of Arrows depict various links between diagrams. Below is a class diagram illustration. More class diagram examples may be found by following the link.



CONCLUSION

An RFID-based system's viability and practicability as a mobile phone anti-loss and anti-theft solution are discussed. A body-worn passive tag is questioned by a smart phone with a low-power RFID scanner to locate a private area that is 10 feet or less from the owner of the tag. The cell phone may also function as a cheap mobile RFID terminal. Aside from that, the positive results of our present design indicate that our system may be used to academic study and upcoming communications-based research.

REFERENCES

- [1]. Roger Pressman, "SOFTWARE ENGINEERING", 7th edition
- [2]. Yehuda Shiran: Java Script Programming, 2008.
- [3]. Holznner: HTML Black Book (HTML4)
- [4]. Patel moss: Java Database Programming with JDBC
- [5]. J2EE Professional by Shadab Siddiqui
- [6]. Nick Todd: JAVA server pages
- [7]. Larne Pekowsley: JAVA server pages
- [8]. Tamilselvi, M. and S. Karthikeyan. "An ingenious face recognition system based on HRPSM_CNN under unrestrained environmental condition." Alexandria Engineering Journal (2021): n. pag.
- [9]. Jacintha, V., Karthikeyan, S., & Sivaprakasam, P. (2022). Surface Flaw Detection of Plug Valve Material Using Infrared Thermography and Weighted Local Variation Pixel-Based Fuzzy Clustering Technique. Advances in Materials Science and Engineering.