

Enhancing Data Security and Privacy Through Cloud Computing

Submitted in partial fulfillment of the requirements for
the award of
Bachelor of Engineering degree in Computer Science and Engineering

by

**GANGIREDDY BHARAT (Reg. No.
37110223)**



**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
SCHOOL OF COMPUTING**

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 - 2021



SATHYABAMA



INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)
Accredited with "A" grade by NAAC
Jeppiaar Nagar, Rajiv Gandhi Salai, Chennai - 600 119
www.sathyabama.ac.in

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

BONAFIDE CERTIFICATE

This is to certify that this project report is the bonafide work of **GANGIREDDY BHARAT (Reg. No. 37110223)** who carried out the project "**Enhancing Data Security and Privacy Through Cloud Computing**" under my supervision from **August 2020** to **APRIL 2021**.

Internal Guide

Ms. T. ANANDHI, M.E.,

Head of the Department

Dr.S. VIGNESWARI, M.E., PH.D.,

Dr.L.LAKSHMANAN, M.E., Ph.D.,

Submitted for Viva voce Examination held on _____

Internal Examiner

External Examiner

DECLARATION

I **GANGIREDDY BHARAT** hereby declare that the Project Report entitled **“Enhancing Data Security and Privacy Through Cloud Computing”** is done by me under the guidance of **Ms. T. ANANDHI, M.E.**, Department of Computer Science and Engineering at Sathyabama Institute of Science and Technology is submitted in partial fulfillment of the requirements for the award of Bachelor of Engineering degree in Computer Science and Engineering.

DATE:

PLACE: CHENNAI

SIGNATURE OF THE CANDIDATE

ACKNOWLEDGEMENT

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

I convey my thanks to **Dr. T. Sasikala, M.E., Ph.D., Dean**, School of Computing, **Dr. S. Vigneswari, M.E., Ph.D., and Dr. L. Lakshmanan, M.E., Ph.D., Heads of the Department** of Computer Science and Engineering for providing me necessary support and details at the right time during the progressive reviews.

I would like to express my sincere and deep sense of gratitude to my Project Guide **Ms. T. ANANDHI, M.E., Assistant Professor**, for her valuable guidance, suggestions and constant encouragement paved way for the successful completion of my project work.

I wish to express my thanks to all Teaching and Non-teaching staff members of the **Department of Computer Science and Engineering** who were helpful in many ways for the completion of the project.

ABSTRACT

The development of cloud computing technology with the explosive growth of unstructured data, cloud storage technology gets more attention and better development. The privacy protection schemes are usually based on encryption technology. There are many privacy preserving methods in the side to prevent data in cloud. We propose a three-layer storage framework based on fog computing. The proposed framework can both take full advantage of cloud storage and protect the privacy of data. Here we are using Hash-Solomon code algorithm is designed to divide data into different parts. If the one data part missing we lost the data information. In this framework we are using bucket concept based algorithms and secure the data information and then it can show the security and efficiency in our scheme. Moreover, based on computational intelligence, this algorithm can compute the distribution proportion stored in cloud, fog, and local machine, respectively Software as a Service (SaaS): Client releases their application on a hosting environment which can be accessed through network from various clients by application users. The client does not manage or control the underlying cloud infrastructure with the possible exception of limited user-specific application configuration settings. Google Apps and Microsoft Office 365 are the examples for SaaS.

TABLE OF CONTENTS

CHAP.NO	TITLE	P.NO
----------------	--------------	-------------

	ABSTRACT	v
	LIST OF FIGURES	viii
1	INTRODUCTION	
	1.1 INTRODUCTION	1
	1.2 INTRODUCTION TO .NET	2
	1.3 SQL SERVER MANAGEMENT STUDIO	4
2	LITERATURE SURVEY	8
	2.1 LITERATURE SURVEY	8
3	AIM AND SCOPE	15
	3.1 SCOPE	15
	3.2 OBJECTIVE	15
4	METHODS AND ALGORITHMS	16
	4.1 EXISTING SYSTEM	16
	4.2 PROPOSED SYSTEM	16
	4.3 ALGORITHM	17
	4.4 SYSTEM ARCHITECTURE	18
	4.5 SYSTEM REQUIREMENTS	23
	4.6 MODULE DESCRIPTION	23
5	RESULTS AND DISCUSSION	28
6	CONCLUSION	32
	REFERENCE	33
	APPENDIX	
	A . PAPER ACCEPTANCE	35
	B . PLAGIARISM REPORT	36
	C . JOURNAL PAPER	37

LIST THE FIGURES

FIGURE No.	FIGURE NAME	PAGE No
1.1	SQL GRAPHICAL USER INTERFACE	5
1.2	SQL SERVER MANAGEMENT STUDIO	6
1.3	CREATING DATABASE	7

3.1	SYSTEM ARCHITECTURE	18
3.2	DATA FLOW DIAGRAM	19
3.3	ER DIAGRAM	20
3.4	UML DIAGRAM	21
3.5	ACTIVITY DIAGRAM	22
5.1	REGISTER PAGE	28
5.2	LOGIN PAGE	29
5.3	UPLOAD FORM	29
5.4	SELECT THE UPLOADED FILE	30
5.5	PROCESS OF DECRYPTION	30
5.6	COMBINING DIFFERENT LAYERS DATA	31
5.7	RESULT OF THE ORIGINAL FILE	31

CHAPTER 1

INTRODUCTION

INTRODUCTION

Fog computing can be perceived both in large cloud systems and big data structures, making reference to the growing difficulties in accessing information objectively. This results in a lack of quality of the obtained content. The effects of fog computing on cloud computing and big data systems may vary. However, a common aspect that can be extracted is a limitation in accurate content distribution, an issue that has been tackled with the creation of metrics that attempt to improve accuracy. Fog networking consists of a control plane and a data plane. For example, on the data plane, fog computing enables computing services to reside at the edge of the network as opposed to servers in a data-center. Compared to cloud computing, fog computing emphasizes proximity to end-users and client objectives, dense geographical distribution and local resource pooling, latency reduction and backbone bandwidth savings to achieve better quality of service (QoS) and edge analytics/stream mining, resulting in superior user-experience and redundancy in case of failure while it is also able to be used in AAL scenarios.

In order to protect user's privacy, we propose a TLS framework based on fog computing model. The TSL framework can give user a certain power of management and effectively protect user's privacy. As mentioned, the interior attack is difficult to resist. Traditional approaches work well in solving outside attack, but when CSP itself has problems, traditional ways are all invalid. Different from the traditional approaches, in our scheme, user's data is divided into three different-size parts with encoding technology. Each of them will lack a part of key information for confidentiality. Combining with the fog computing model, the three parts of data will be stored in the cloud server, the fog server and user's local machine according to the order from large to small. By this method, the attacker cannot recover the user's original data even if

he gets all the data from a certain server. As for the CSP, they also cannot get any useful information

without the data stored in the fog server and local machine because both of the fog server and local machine are controlled by users.

INTRODUCTION TO .NET

Microsoft .NET is a set of Microsoft software technologies for rapidly building and integrating XML Web services, Microsoft Windows-based applications, and Web solutions. The .NET Framework is a language-neutral platform for writing programs that can easily and securely interoperate. There's no language barrier with .NET: there are numerous languages available to the developer including Managed C++, C#, Visual Basic and Java Script. The .NET framework provides the foundation for components to interact seamlessly, whether locally or remotely on different platforms. It standardizes common data types and communications protocols so that components created in different languages can easily interoperate.

“.NET” is also the collective name given to various software components built upon the .NET platform. These will be both products (Visual Studio.NET and Windows.NET Server, for instance) and services (like Passport, .NET My Services, and so on).

THE .NET FRAMEWORK

The .NET Framework has two main parts:

1. The Common Language Runtime (CLR).
2. A hierarchical set of class libraries.

The CLR is described as the “execution engine” of .NET. It provides the environment within which programs run. The most important features are

- ◆ Conversion from a low-level assembler-style language, called Intermediate Language (IL), into code native to the platform being executed on.
- ◆ Memory management, notably including garbage collection.
- ◆ Checking and enforcing security restrictions on the running code.
- ◆ Loading and executing programs, with version control and other such features.

THE CLASS LIBRARY

.NET provides a single-rooted hierarchy of classes, containing over 7000 types. The root of the namespace is called System; this contains basic types like Byte, Double, Boolean, and String, as well as Object. All objects derive from System. Object. As well as objects, there are value types. Value types can be allocated on the stack, which can provide useful flexibility. There are also efficient means of converting value types to object types if and when necessary.

The set of classes is pretty comprehensive, providing collections, file, screen, and network I/O, threading, and so on, as well as XML and database connectivity.

The class library is subdivided into a number of sets (or namespaces), each providing distinct areas of functionality, with dependencies between the namespaces kept to a minimum.

LANGUAGES SUPPORTED BY .NET

The multi-language capability of the .NET Framework and Visual Studio .NET enables developers to use their existing programming skills to build all types of applications and XML Web services. The .NET framework supports new versions of Microsoft's old favorites Visual Basic and C++ (as VB.NET and Managed C++), but there are also a number of new additions to the family.

Visual Basic .NET has been updated to include many new and improved language features that make it a powerful object-oriented programming language. These features include inheritance, interfaces, and overloading, among others. Visual Basic also now supports structured exception handling, custom attributes and also supports multi-threading.

Other languages for which .NET compilers are available include

- FORTRAN
- COBOL
- Eiffel

C#.NET is also compliant with CLS (Common Language Specification) and supports structured exception handling. CLS is set of rules and constructs that are supported by the CLR (Common Language Runtime). CLR is the runtime environment provided by the .NET Framework; it manages the execution of the code and also makes the development process easier by providing services C#.NET is a CLS-compliant language. Any objects, classes, or components that created in C#.NET can be used in any other CLS-compliant language. In addition, we can use objects, classes, and

components created in other CLS-compliant languages in C#.NET .The use of CLS ensures complete interoperability among applications, regardless of the languages used to create the application.

OBJECTIVES OF .NET FRAMEWORK

1. To provide a consistent object-oriented programming environment whether object codes is stored and executed locally on Internet-distributed, or executed remotely.
2. To provide a code-execution environment to minimizes software deployment and guarantees safe execution of code.
3. Eliminates the performance problems.

There are different types of application, such as Windows-based applications and Web-based applications.

SQL SERVER MANAGEMENT STUDIO

Microsoft is the vendor of SQL Server. We have different editions of SQL Server, where SQL Server Express is free to download and use. SQL Server uses T-SQL (Transact-SQL). T-SQL is Microsoft's proprietary extension to SQL. TSQL is very similar to standard SQL, but in addition it supports some extra functionality, built in functions, etc.

SQL Server Management Studio can also be used to create a new database, alter any existing database schema by adding or modifying tables and indexes, or analyze performance. It includes the query windows which provide a GUI based interface to write and execute queries.

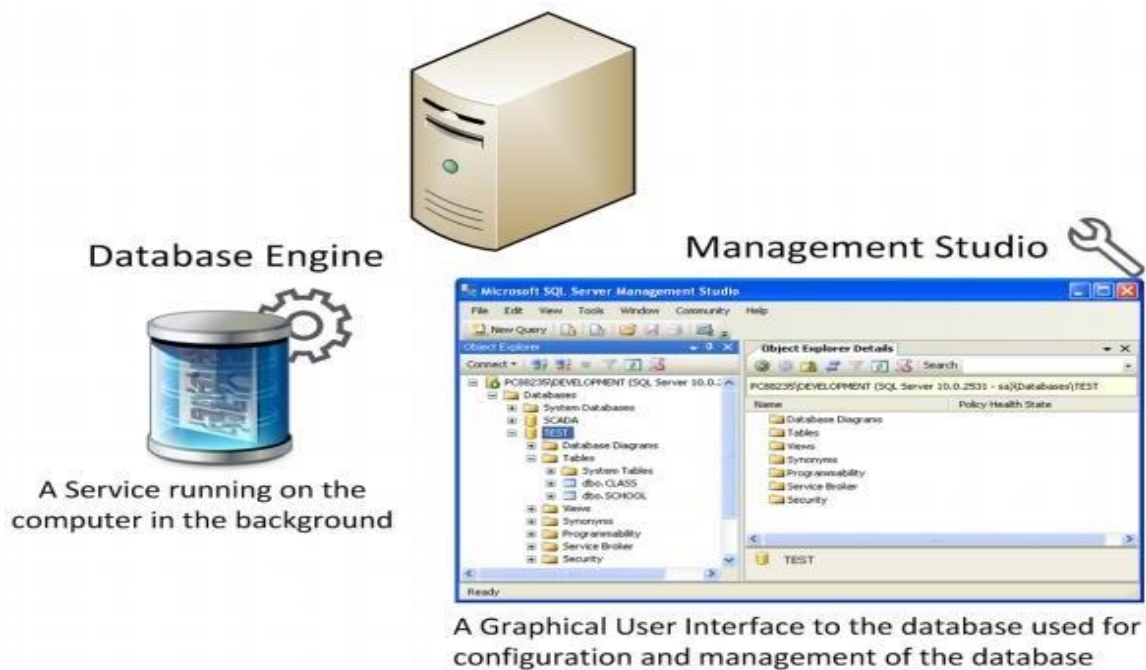


Fig 1. 1:Sql Graphical User Interface

SQL Server Management Studio is a GUI tool included with SQL Server for configuring, managing, and administering all components within Microsoft SQL Server. The tool includes both script editors and graphical tools that work with objects and features of the server. As mentioned earlier, version of SQL Server Management Studio is also available for SQL Server Express Edition, for which it is known as SQL Server Management Studio Express.

A central feature of SQL Server Management Studio is the Object Explorer, which allows the user to browse, select, and act upon any of the objects within the server. It can be used to visually observe and analyze query plans and optimize the database performance, among others. SQL Server Management Studio can also be used to create a new database, alter any existing database schema by adding or modifying tables and indexes, or analyze performance. It includes the query windows which provide a GUI based interface to write and execute queries.

When creating SQL commands and queries, the “Query Editor” (select “New Query” from the Toolbar) is used (shown in the figure above). With SQL and the “Query Editor” we can do almost everything with code, but sometimes it is also a good idea to

use the different Designer tools in SQL to help us do the work without coding (so much).

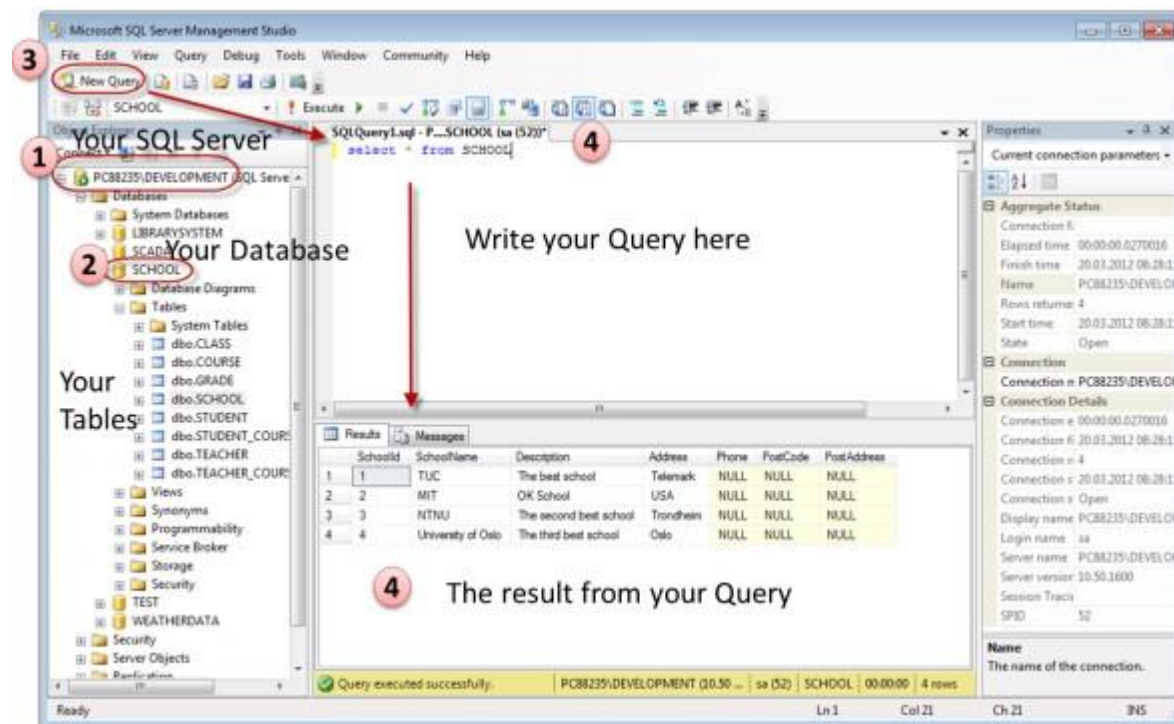


Fig 1. 2: SQL SERVER MANAGEMENT STUDIO

CREATE A NEW DATABASE

It is quite simple to create a new database in Microsoft SQL Server. Just right-click on the “Databases” node and select “New Database...”

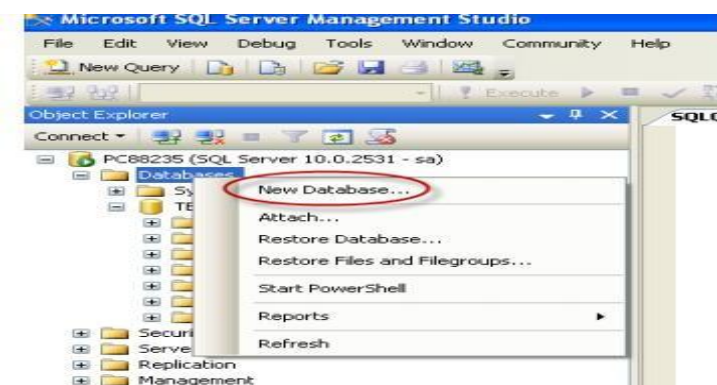


Fig 1. 3: Creating Database

The OLAP Services feature available in SQL Server version 7.0 is now called SQL Server 2000 Analysis Services. The term OLAP Services has been replaced with the term Analysis Services. Analysis Services also includes a new data mining component. The Repository component available in SQL Server version 7.0 is now called Microsoft SQL Server 2000 Meta Data Services. References to the component now use the term Meta Data Services. The term repository is used only in reference to the repository engine within Meta Data Services

CHAPTER 2

LITERATURE SURVEY

2.1 LITRATURE SURVEY

Title 1: Privacy-preserving security solution for cloud services

Author: L. Malina*, J. Hajny, P. Dzurenda and V. Zeman

A novel privacy-preserving security solution for cloud services. Our solution is based on an efficient nonbilinear group signature scheme providing the anonymous access to cloud services and shared storage servers. The novel solution offers anonymous authentication for registered users. Thus, users' personal attributes (age, valid registration, successful payment) can be proven without revealing users' identity, and users can use cloud services without any threat of profiling their behaviour. However, if a user breaks provider's rules, his access right is revoked. Our solution provides anonymous access, unlinkability and the confidentiality of transmitted data. We implement our solution as a proof of concept application and present the experimental results. Further, we analyse current privacy preserving solutions for cloud services and group signature schemes as basic parts of privacy enhancing solutions in cloud services. We compare the performance of our solution with the related solutions and schemes.

Title 2: A secure data privacy preservation for on-demand cloud service

Author: Chandramohan Dhasarathan *, Vengattaraman Thirumal, Dhavachelvan Ponnurangam

This paper spotlights privacy and its obfuscation issues of intellectual, confidential information owned by insurance and finance sectors. Privacy risk in business era if authoritarians misuse secret information. Software interruptions in steeling digital data in the name of third party services. Liability in digital secrecy for the business continuity isolation, mishandling causing privacy breaching the vicinity and its preventive phenomenon is scrupulous in the cloud, where a huge amount of data is stored and maintained enormously. In this developing IT-world toward cloud, users privacy protection is becoming a big question , albeit cloud computing made changes in the computing field by increasing its effectiveness, efficiency and optimization of the service environment etc., cloud users data and their identity, reliability, maintainability and privacy may vary for different CPs

(cloud providers). CP ensures that the user's proprietary information is maintained more secretly with current technologies. More remarkable occurrence is even the cloud provider does not have suggestions regarding the information and the digital data stored and maintained globally anywhere in the cloud. The proposed system is one of the obligatory research issues in cloud computing. We came forward by proposing the Privacy Preserving Model to Prevent Digital Data Loss in the Cloud (PPM-DDLC). This proposal helps the CR (cloud requester/users) to trust their proprietary information and data stored in the cloud.

Title 3: A Survey on Secure Storage Services in Cloud Computing

Author: Ms. B.Tejaswi, Dr. L.V.Reddy & Ms. M.Leelavathi

Cloud computing is an emerging technology and it is purely based on internet and its environment. It provides different services to users such as Software-as-a-Service (SaaS), PaaS, IaaS, Storage-as-a-service (SaaS). Using Storage-as-a-Service, users and organizations can store their data remotely which poses new security risks towards the correctness of data in cloud. In order to achieve secure cloud storage, there exists different techniques such as flexible distributed storage integrity auditing mechanism, distributed erasure-coded data, Merkle Hash Tree(MHT) construction etc. These techniques support secure and efficient dynamic data storage in the cloud. This paper also deals with architectures for security and privacy management in the cloud storage environment.

Title 4: On a Relation Between Verifiable Secret Sharing Schemes and a Class of Error-Correcting Codes

Author: Ventzislav Nikov and Svetla Nikova

We try to shed a new insight on Verifiable Secret Sharing Schemes (VSS). We first define a new "metric" (with slightly different properties than the standard Hamming metric). Using this metric we define a very particular class of codes that we call error-set correcting codes, based on a set of forbidden distances which is a monotone decreasing set. Next we redefine the packing problem for the new settings and generalize the notion of error correcting capability of the error-set correcting codes

accordingly (taking into account the new metric and the new packing). Then we consider burst-error interleaving codes proposing an efficient burst-error correcting technique, which is in fact the well-known VSS and Distributed Commitments (DC) pair-wise checking protocol and we prove the error-correcting capability of the error-set correcting interleaving codes.

Title 5: A Secure Cloud-assisted Urban Data Sharing Framework for Ubiquitous-cities

Author: Jian Shena,b,c,_, Dengzhi Liuc, Jun Shenc, Qi Liua,c, Xingming Suna,c

With the accelerated process of urbanization, more and more people tend to live in cities. In order to deal with the big data that are generated by citizens and public city departments, new information and communication technologies are utilized to process the urban data, which makes it more easier to manage. Cloud computing is a novel computation technology. After cloud computing was commercialized, there have been lot of cloud-based applications. Since the cloud service is provided by the third party, the cloud is semi-trusted. Due to the features of cloud computing, there are many security issues in cloud computing. Attribute-based encryption (ABE) is a promising cryptography technique which can be used in the cloud to solve many security issues. In this paper, we propose a framework for urban data sharing by exploiting the attribute-based cryptography. In order to fit the real world ubiquitous-cities utilization, we extend our scheme to support dynamic operations. In particular, from the part of performance analysis, it can be concluded that our scheme is secure and can resist possible attacks. Moreover, experimental results and comparisons show that our scheme is more efficient in terms of computation.

Title 6: Security and Privacy Preservation Scheme of Face Identification and Resolution Framework Using Fog Computing in Internet of Things

Author: P. Hu, H. Ning, Y. Wang, X.

Face identification and resolution technology is crucial to ensure the identity consistency of humans in physical space and cyber space. In current Internet of Things (IoT) and big data situation, the increase of applications based on face identification

and resolution raises the demands of computation, communication and storage capabilities. Therefore, we have proposed the fog computing based face identification and resolution framework to improve processing capacity and save the bandwidth. However, there are some security and privacy issues brought by the properties of fog computing based framework. In this paper, we propose a security and privacy preservation scheme to solve above issues. We give an outline of the fog computing based face identification and resolution framework, and summarize the security and privacy issues. Then the authentication and session key agreement scheme, data encryption scheme, and data integrity checking scheme are proposed to solve the issues of confidentiality, integrity, and availability in the processes of face identification and face resolution. Finally, we implement a prototype system to evaluate the influence of security scheme on system performance. Meanwhile, we also evaluate and analyze the security properties of proposed scheme from the viewpoint of logical formal proof and the CIA (confidentiality, integrity, availability) properties of information security. The results indicate that the proposed scheme can effectively meet the requirements for security and privacy preservation.

Title 7: Survey on Privacy-Preserving Methods for Storage in Cloud Computing

Author: Neethu Mariam Joseph, Esther Daniel, N. A. Vasanthi, Ph.D

At present the mankind are progressively relying more on a number of online storage stores to back up our data or for using it in real time which gives an anywhere, anytime access. All these services bring with it, concerns of security and privacy weaknesses for all the services provided by them since the user's data are stored and maintained out of user's premises. This paper portrays the various issues associated to privacy while storing the user's data on third party service providers, which is more commonly termed as cloud service. Cloud computing refers to the fundamental infrastructure for an up-coming model of service provision that has the benefit of dropping cost by sharing computing and storage resources, united with an on-demand provisioning mechanism depending on a pay-per-use business model. Without appropriate security and privacy solutions designed for clouds this computing paradigm could become a huge failure. There is a lot of research being made to spot

out the issues with these cloud service providers and cloud security in general. This paper is on regard of one of the key issue -privacy that occur in the context of cloud computing and analyze the various works being done to solve the issues in privacy and thus to ensure privacy to outsourced data on cloud storage.

TITLE 8: Survey on Secure Storage in Cloud Computing

AUTHOR: A. Rajathi^{1*} and N. Saravanan²

Cloud Computing is an environment for providing information and resources that are delivered as a service to end-users over the Internet on demand. Thus cloud enables users to access their data from any geographical locations at any time and also has brought benefits in the form of online storage services. Cloud storage service avoids the cost expensive on software, personnel maintenance and provides better performance, less storage cost and scalability. But the maintenance of stored data in a secure manner is not an easy task in cloud environment and especially that stored data may not be completely trustworthy. Cloud delivers services through internet which increases their exposure to storage security vulnerabilities. However security is one of the major drawbacks that preventing several large organizations to enter into cloud computing environment. This work surveyed on several existing cloud storage frameworks, techniques and their advantages, drawbacks and also discusses the challenges that are required to implement secure cloud data storage. This survey results help to identify the future research areas and methods for improving the existing drawbacks.

TITLE 9: Security and Privacy Preservation Scheme of Face Identification and Resolution Framework Using Fog Computing in Internet of Things

AUTHOR : Yanna Wang, and Xuanxia Yao

Face identification and resolution technology is crucial to ensure the identity consistency of humans in physical space and cyber space. In current Internet of Things (IoT) and big data situation, the increase of applications based on face identification and resolution raises the demands of computation, communication and storage capabilities. Therefore, we have proposed the fog computing based face identification

and resolution framework to improve processing capacity and save the bandwidth. However, there are some security and privacy issues brought by the properties of fog computing based framework. In this paper, we propose a security and privacy preservation scheme to solve above issues. We give an outline of the fog computing based face identification and resolution framework, and summarize the security and privacy issues. Then the authentication and session key agreement scheme, data encryption scheme, and data integrity checking scheme are proposed to solve the issues of confidentiality, integrity, and availability in the processes of face identification and face resolution. Finally, we implement a prototype system to evaluate the influence of security scheme on system performance. Meanwhile, we also evaluate and analyze the security properties of proposed scheme from the viewpoint of logical formal proof and the CIA (confidentiality, integrity, availability) properties of information security. The results indicate that the proposed scheme can effectively meet the requirements for security and privacy preservation.

TITLE 10: A Secure Cloud-assisted Urban Data Sharing Framework for Ubiquitous-cities

AUTHOR: Jian Shena,b,c,_, Dengzhi Liuc, Jun Shenc, Qi Liua,c, Xingming Suna,c

With the accelerated process of urbanization, more and more people tend to live in cities. In order to deal with the big data that are generated by citizens and public city departments, new information and communication technologies are utilized to process the urban data, which makes it more easier to manage. Cloud computing is a novel computation technology. After cloud computing was commercialized, there have been lot of cloud-based applications. Since the cloud service is provided by the third party, the cloud is semi-trusted. Due to the features of cloud computing, there are many security issues in cloud computing. Attribute-based encryption (ABE) is a promising cryptography technique which can be used in the cloud to solve many security issues. In this paper, we propose a framework for urban data sharing by exploiting the attribute-based cryptography. In order to fit the real world ubiquitous-cities utilization, we extend our scheme to support dynamic operations. In particular, from the part of performance analysis, it can be concluded that our scheme is secure and can resist possible attacks. Moreover, experimental results and comparisons show that our scheme is more efficient in terms of computation

CHAPTER 3

AIM AND SCOPE

SCOPE

A Three-Layer Privacy Preserving Cloud Storage Scheme Based on Computational Intelligence in Fog Computing. The privacy preservation is our focus, some active attacks are beyond the scope of this work. The three layer cloud storage stores in to the three different parts of data parts .If the one data part missing we lost the data information. In this proposed framework using the bucket concept based algorithms. We are using a BCH code algorithm. It's High flexible.

OBJECTIVE

Cloud storage also causes a series of secure problems. When using cloud storage, users do not actually control the physical storage of their data and it results in the separation of ownership and management of data. In order to solve the problem of privacy protection in cloud storage, we propose a TLS framework based on fog computing model and design a Hash-Solomon algorithm. Through the theoretical safety analysis, the scheme is proved to be feasible. By allocating the ratio of data blocks stored in different servers reasonably, we can ensure the privacy of data in

each server. On another hand, cracking the encoding matrix is impossible theoretically. Besides, using hash transformation can protect the fragmentary information. Through the experiment test, this scheme can efficiently complete encoding and decoding without influence of the cloud storage efficiency. The three layer cloud storage stores in to the three different parts of data parts .If the one data part missing we lost the data information. In this proposed framework using the bucket concept based algorithms

CHAPTER 4

Methods & Algorithms

EXISTING SYSTEM

- Data has been partitioned and stored in three storage servers by using hash-Solomon code algorithm in the existing system: cloud server, fog server, and local server.
- The reality that the third party is clueless of our data partitioning is key. The Cloud server has 80% of the valuable information, the Fog server has 15% among the most important information, and also the Local server will have 5% of the valuable information.
- If a scammer address the potential in any of these layers, he or she will either alter or delete information. As a result, the user will end up losing that data. It's the most massive disadvantage.

EXISTING SYSTEM DISADVANTAGES:

- Changes in the understanding of risk as a result of extending the datacentre into the cloud.
- Low latency and location awareness

PROPOSED SYSTEM

- To protect and preserve the missing data, we will use bucket system.
- Bucket is similar to a mirror within this any data the user enters is saved automatically in the bucket system.
- We introduced a multi BCH code algorithm for data comparison, with synchronized data preserved in a bucket.

ADVANTAGES:

- In our system we are using a bucket concept in order to reduce the data wastages and reduce the process timings.
- We are using a BCH (Bose–Chaudhuri–Hocquenghem) code algorithm. It's High flexible.
- BCH code are used in many communications application and low amount of redundancy.

ALGORITHM

Bucket

- The Bucket Access Controls resource represents the Access Control Lists (ACL) for buckets within Google Cloud Storage. ACL let you specify who has access to your data and to what extent.
- This mechanism is explicitly designed to allow the user to recover deleted data or manipulated by a 3rd person. Bucket serves as a reflection; whichever data the user enters is automatically saved in it.

BCH code algorithm

- The BCH codes, or Bose–Chaudhuri–Hocquenghem codes, are a type of cyclic error correcting codes that are developed using polynomials over a finite field in coding theory. One of the major benefits of BCH codes is that the amount of symbol errors that the code will correct could be accurately monitored during validation phase.
- It is possible to build binary BCH codes that can resolve several bit errors in particular.
- One attribute of BCH codes is its ease of decoding, which is accomplished using an arithmetic procedure known as syndrome decryption. It optimises

the decoder process for these codes, enabling over the use of compact, reduced embedded software.

4.3.3 Hash Solomon

- The Hash-Solomon code algorithm is primarily used to separate data into parts. The information is divided into three sections and stored in this location. Information is divided into groups based on the value of the knowledge found within.

SYSTEM ARCHITECTURE

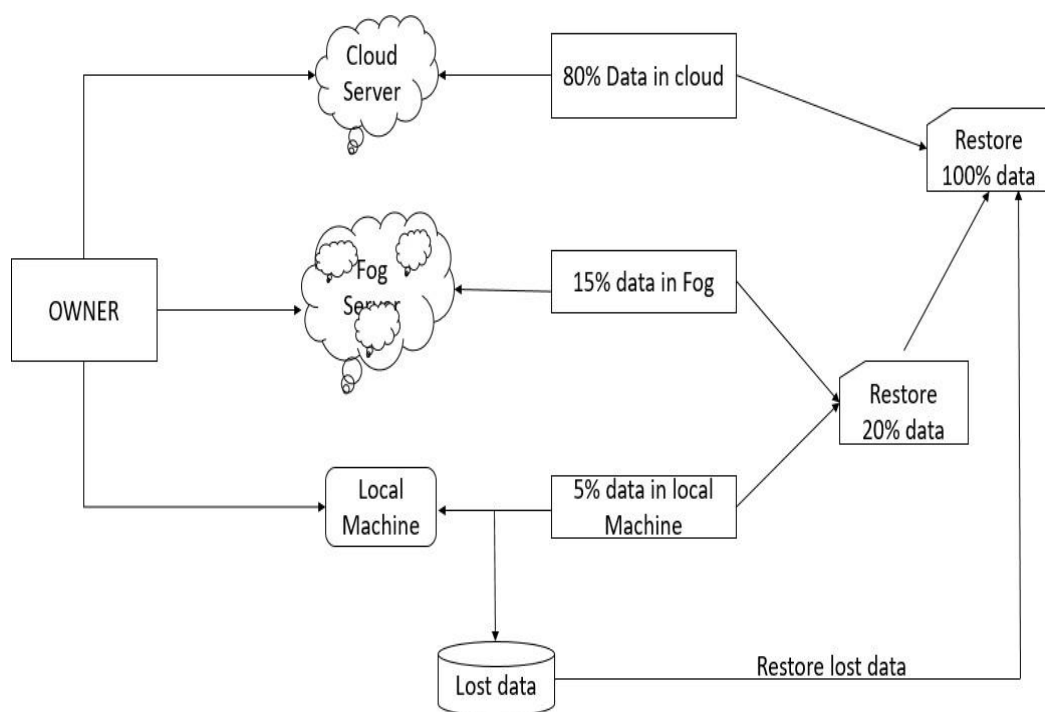


Fig 3. 1: SYSTEM ARCHITECTURE

DATA FLOW DIAGRAM

Data Flow Diagram (DFD) is a two-dimensional diagram that describes how data is processed and transmitted in a system. The graphical depiction recognizes each

source of data and how it interacts with other data sources to reach a mutual output.

In order to draft a data flow diagram one must

- Identify external inputs and outputs
- Determine how the inputs and outputs relate to each other
- Explain with graphics how these connections relate and what they result in.

Role of DFD :

- It is a documentation support which is understood by both programmers and non programmers. As DFD postulates only what processes are accomplished not how they are performed.
- A physical DFD postulates where the data flows and who processes the data.
- It permits analyst to isolate areas of interest in the organization and study them by examining the data that enter the process and viewing how they are altered when they leave.

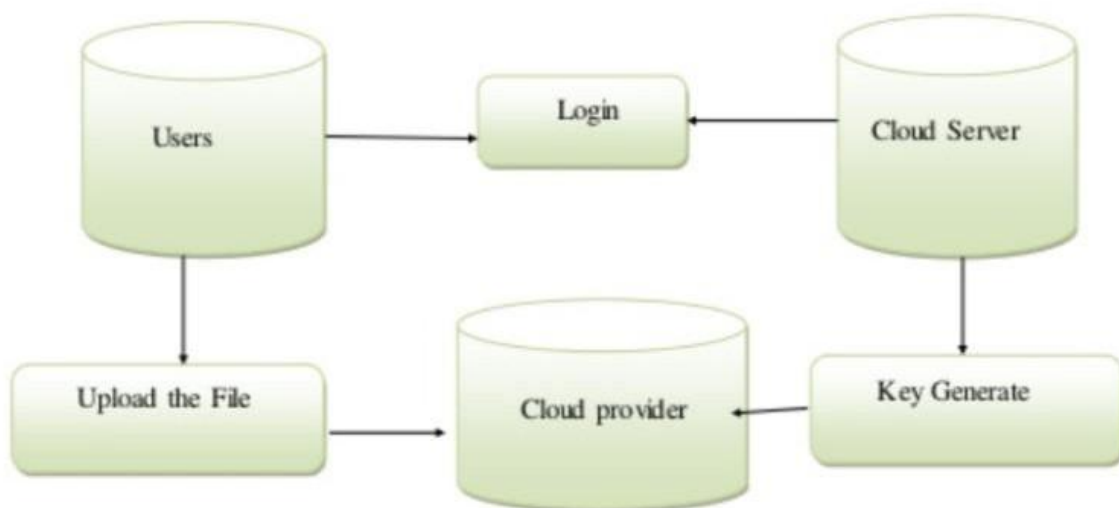


Fig 3. 2: DATA FLOW DIAGRAM

ERDiagram:

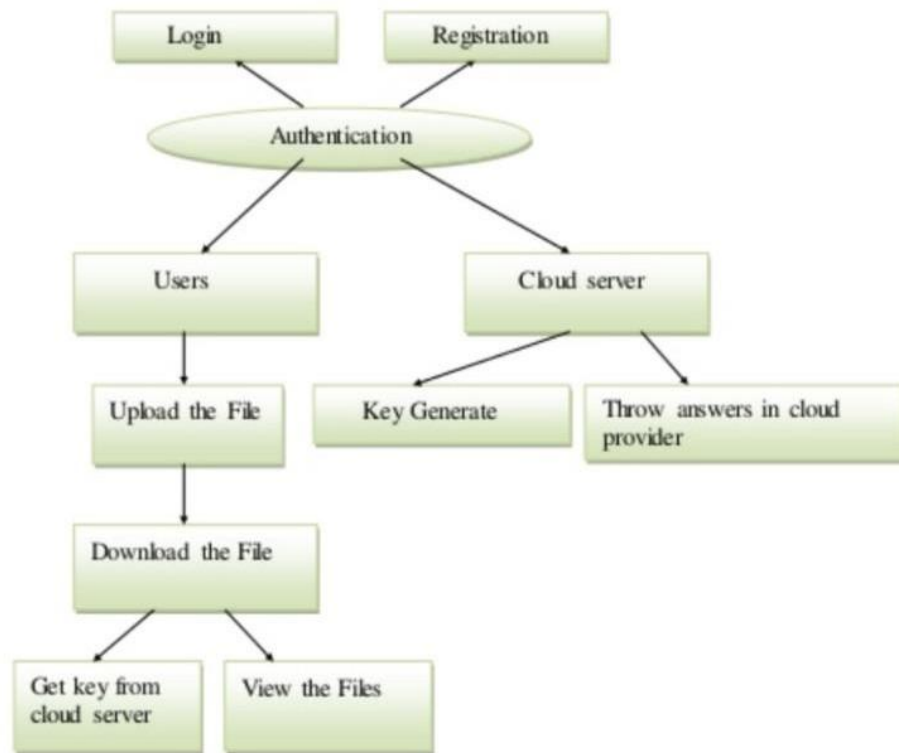


Fig 3. 3: ER Diagram

UML Diagram:

Use case diagram

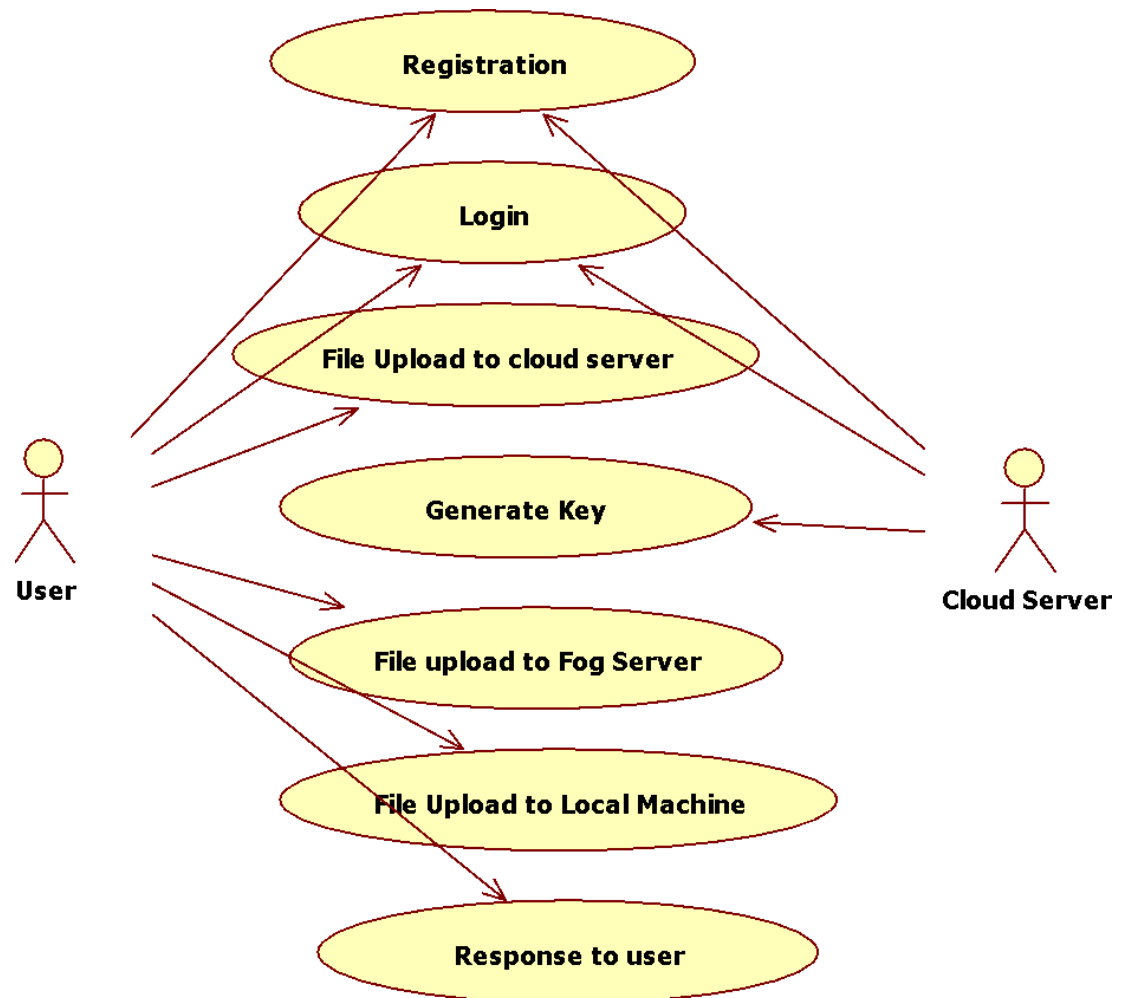


FIG 3.4 : UML DIAGRAM

Activity Diagram:

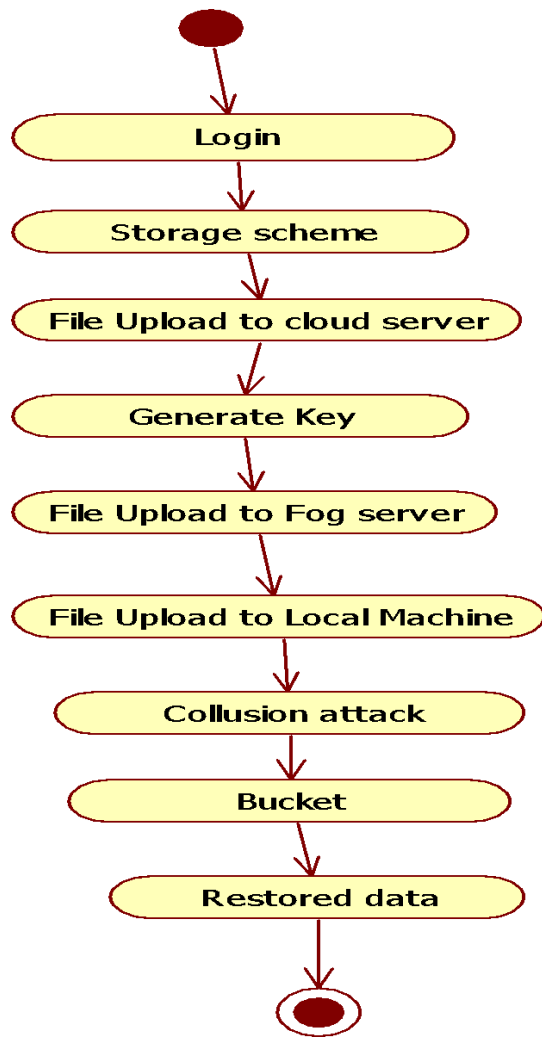


FIG 3.4 : ACTIVITY DIAGRAM

SYSTEM REQUIREMENTS

HARDWARE REQUIREMENTS:

- System - Pentium-IV
- Speed - 2.4GHZ
- Hard disk - 40GB

- Monitor - 15VGA color
- RAM - 512MB

SOFTWARE REQUIREMENTS:

- Operating System - Windows XP
- Coding language - .Net
- IDE - Microsoft Visual Studio
- Database - MYSQL

MODULE DESCRIPTION

MODULES

- Login
- Registration
- Storage Scheme
- Recovery Scheme

Login Module

This module enables users to access the website via their authorized account and a valid pin. He or she would not be permitted to log in if he or she is not a legitimate user. The website can only be accessed and is used by authorized individuals.

Registration Module

The user registers their account identification using this module by giving the absolute necessities of details.

Users must only include minimum necessary of details, such as their email address, title, contact details, and pin, that would be used for subsequent logins. In order for them to be able to access the website.

Storage Module

Users can store their files in three separate cloud server using this module. Cloud server, fog server, and local server are the storage centers. We place 80% of our information on a central server. We store 15% of crucial information on the fog server. We hold 5% of the details on the local computer.

Recovery Module

Users can retrieve documents from three separate cloud server using this module. If data fits these three volumes of information, it is preserved in the bucket by using BCH method. The person can simply recover data from bin if its been hacked in any of the levels.

SOFTWARE TESTING

Software testing is the process of evaluation a software item to detect differences between given input and expected output. Also to assess the feature of a software item. Testing assesses the quality of the product. Software testing is a process that should be done during the development process. In other words software testing is a verification and validation process.

Verification

Verification is the process to make sure the product satisfies the conditions imposed at the start of the development phase. In other words, to make sure the product behaves the way we want it to.

Validation

Validation is the process to make sure the product satisfies the specified requirements at the end of the development phase. In other words, to make sure the product is built as per customer requirements.

Basics of software testing

There are two basics of software testing: black box testing and white box testing.

Black box Testing

Black box testing is a testing technique that ignores the internal mechanism of the system and focuses on the output generated against any input and execution of the system. It is also called functional testing.

White box Testing

White box testing is a testing technique that takes into account the internal mechanism of a system. It is also called structural testing and glass box testing. Black box testing is often used for validation and white box testing is often used for verification.

Types of testing

There are many types of testing like

- Unit Testing
- Integration Testing
- Functional Testing
- System Testing
- Stress Testing
- Performance Testing
- Usability Testing
- Acceptance Testing
- Regression Testing
- Beta Testing

Unit Testing

Unit testing is the testing of an individual unit or group of related units. It falls under the class of white box testing. It is often done by the programmer to test that the unit he/she has implemented is producing expected output against given input.

Integration Testing

Integration testing is testing in which a group of components are combined to produce output. Also, the interaction between software and hardware is tested in integration testing if software and hardware components have any relation. It may fall under both white box testing and black box testing.

Functional Testing

Functional testing is the testing to ensure that the specified functionality required in the system requirements works. It falls under the class of black box testing.

System Testing

System testing is the testing to ensure that by putting the software in different environments (e.g., Operating Systems) it still works. System testing is done with full system implementation and environment. It falls under the class of black box testing.

Stress Testing

Stress testing is the testing to evaluate how system behaves under unfavorable conditions. Testing is conducted at beyond limits of the specifications. It falls under the class of black box testing.

Performance Testing

Performance testing is the testing to assess the speed and effectiveness of the system and to make sure it is generating results within a specified time as in performance requirements. It falls under the class of black box testing.

Usability Testing

Usability testing is performed to the perspective of the client, to evaluate how the GUI is user-friendly? How easily can the client learn? After learning how to use, how proficiently can the client perform? How pleasing is it to use its design? This falls under the class of black box testing.

Acceptance Testing

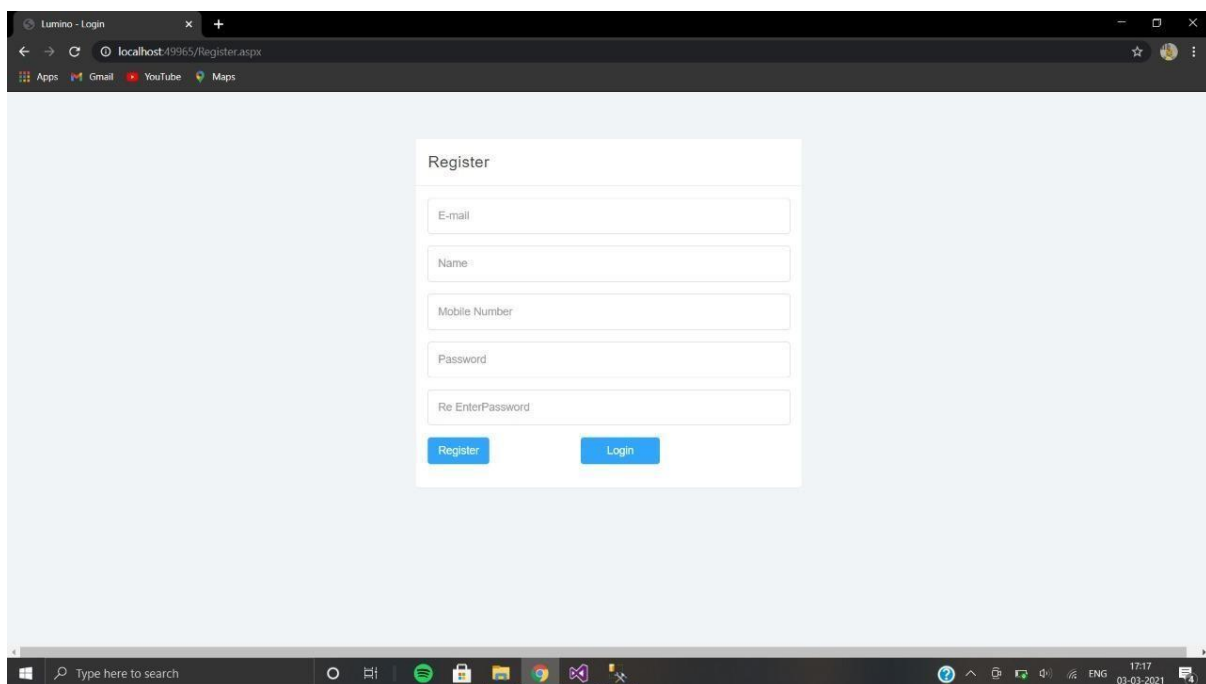
Acceptance testing is often done by the customer to ensure that the delivered product meets the requirements and works as the customer expected. It falls under the class of black box testing.

Regression Testing

Regression testing is the testing after modification of a system, component, or a group of related units to ensure that the modification is working correctly and is not damaging or imposing other modules to produce unexpected results. It falls under the class of black box testing.

CHAPTER 5

RESULTS AND DISCUSSION



The screenshot displays a web browser window with the title 'Lumino - Login'. The address bar shows the URL 'localhost:49365/Register.aspx'. The browser's toolbar includes icons for back, forward, and refresh. Below the browser window, the Windows taskbar is visible, showing the search bar and several application icons. The main content of the browser is a registration form titled 'Register'. The form is centered on a light blue background and contains the following elements:

- A title 'Register' at the top of the form.
- Five input fields stacked vertically: 'E-mail', 'Name', 'Mobile Number', 'Password', and 'Re EnterPassword'.
- Two blue buttons at the bottom of the form: 'Register' and 'Login'.

Fig 5. 1: Register Page

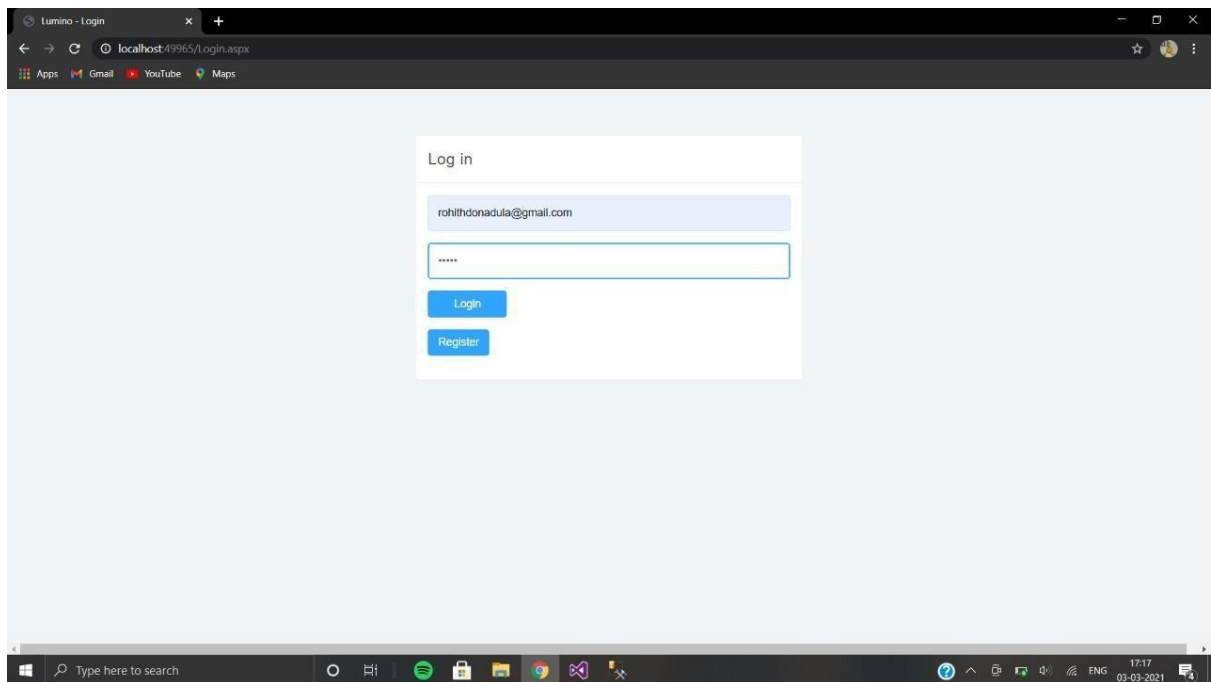


Fig 5. 2: Login Page

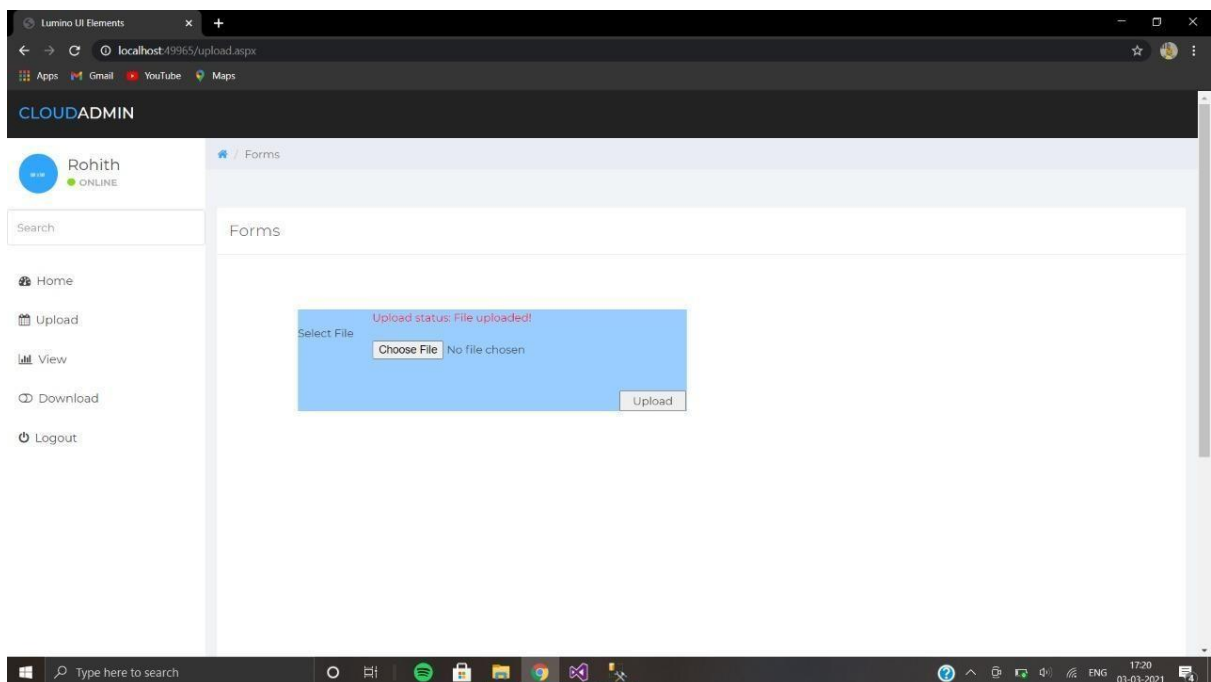


Fig 5. 3: Upload Form

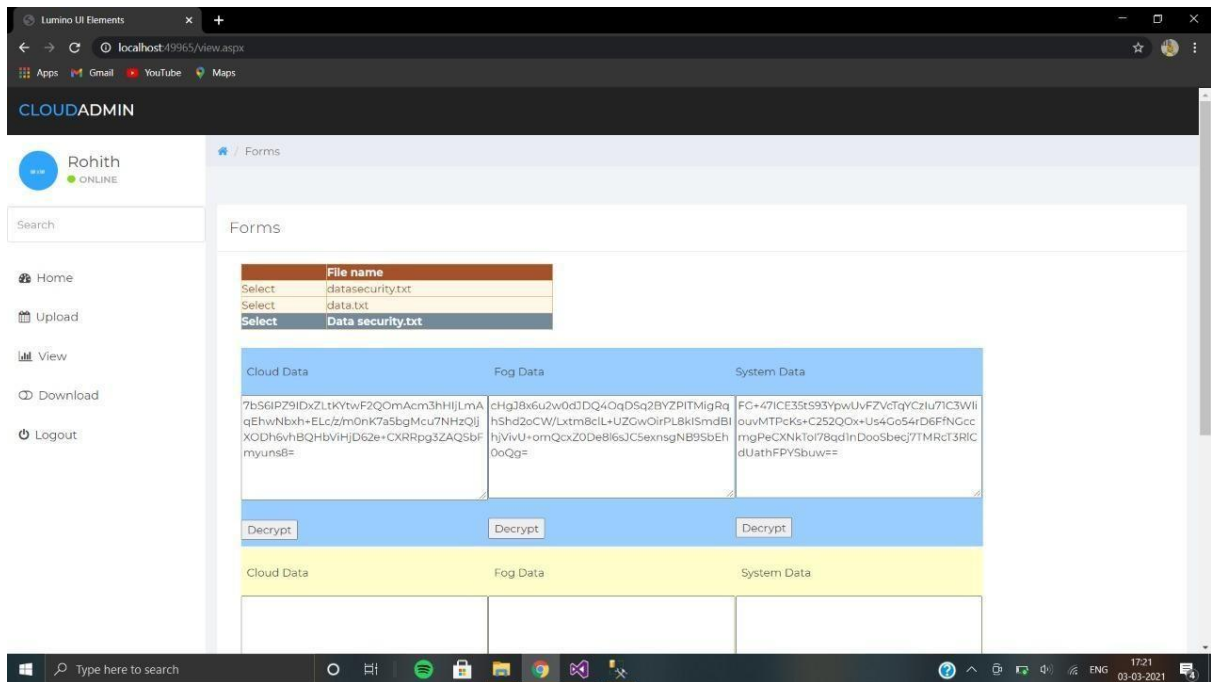


Fig 5. 4: Select The uploaded File

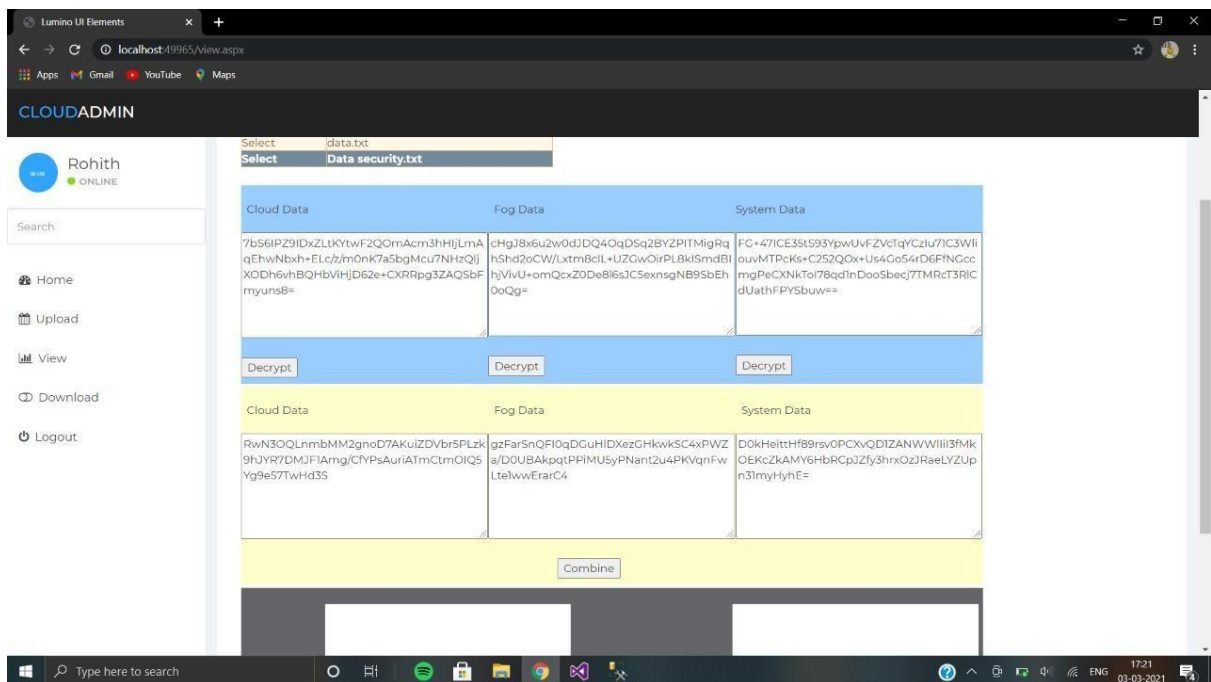


Fig 5. 5: Process of Decryption

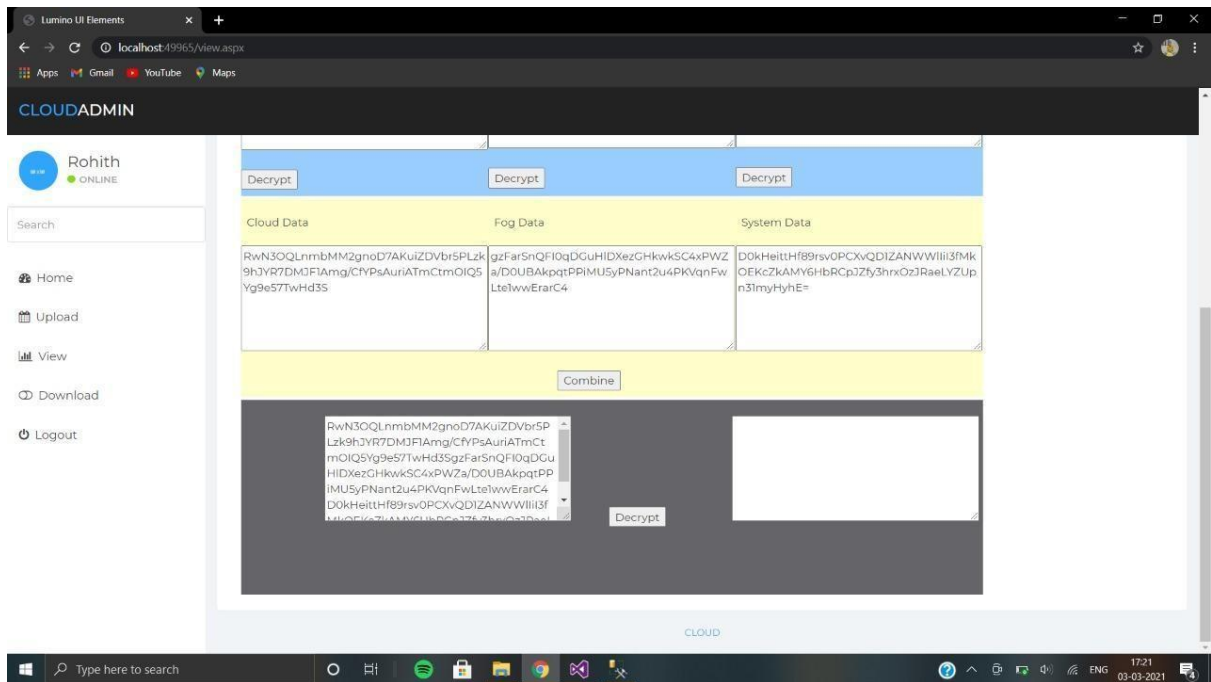


Fig 5. 6: Combining Three Different Layers Data

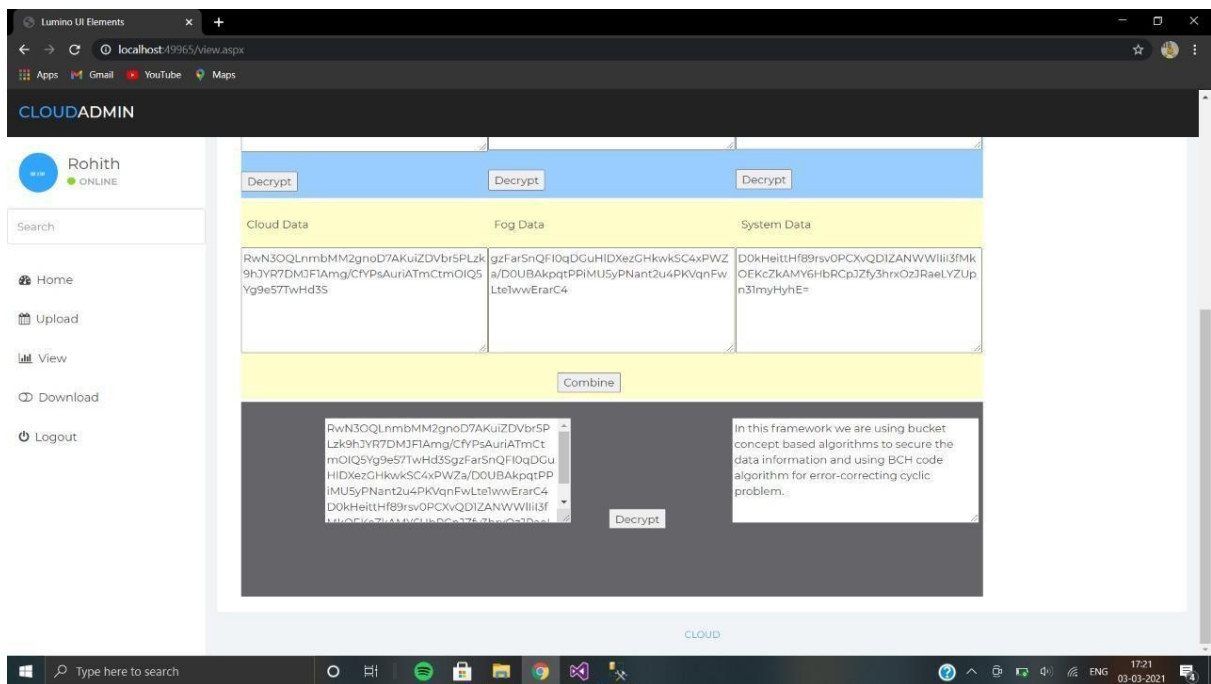


Fig 5. 7: Result Of The Original File

CHAPTER 6

CONCLUSION

The development of cloud computing brings us a lot of benefits. Cloud storage is a convenient technology which helps users to expand their storage capacity. However, cloud storage also causes a series of secure problems. When using cloud storage, users do not actually control the physical storage of their data and it results in the separation of ownership and management of data. In order to solve the problem of privacy protection in cloud storage, we propose a TLS framework based on fog computing model and design a BCH Code algorithm. Through the theoretical safety analysis, the scheme is proved to be feasible. By allocating the ratio of data blocks stored in different servers reasonably, we can ensure the privacy of data in each server. On another hand, cracking the encoding matrix is impossible theoretically. Besides, using hash transformation can protect the fragmentary information. Through the experiment test, this scheme can efficiently complete encoding and decoding without influence of the cloud storage efficiency. Furthermore, we design a reasonable comprehensive efficiency index, in order to achieve the maximum efficiency, and we also find that the Cauchy matrix is more efficient in coding process.

REFERENCE

- [1] P. Mell and T. Grance, "The NIST definition of cloud computing," Nat. Inst. Stand. Technol., vol. 53, no. 6, pp. 50–50, 2009.

- [2] H. T. Dinh, C. Lee, D. Niyato, and P. Wang, "A survey of mobile cloud computing: Architecture, applications, and approaches," *Wireless Commun. Mobile Comput.*, vol. 13, no. 18, pp. 1587–1611, 2013.
- [3] J. Chase, R. Kaewpuang, W. Yonggang, and D. Niyato, "Joint virtual machine and bandwidth allocation in software defined network (sdn) and cloud computing environments," in *Proc. IEEE Int. Conf. Commun.*, 2014, pp. 2969–2974.
- [4] H. Li, W. Sun, F. Li, and B. Wang, "Secure and privacy-preserving data storage service in public cloud," *J. Comput. Res. Develop.*, vol. 51, no. 7, pp. 1397–1409, 2014.
- [5] Y. Li, T. Wang, G. Wang, J. Liang, and H. Chen, "Efficient data collection in sensor-cloud system with multiple mobile sinks," in *Proc. Adv. Serv. Comput., 10th Asia-Pac. Serv. Comput. Conf.*, 2016, pp. 130–143.
- [6] L. Xiao, Q. Li, and J. Liu, "Survey on secure cloud storage," *J. Data Acquis. Process.*, vol. 31, no. 3, pp. 464–472, 2016.
- [7] R. J. McEliece and D. V. Sarwate, "On sharing secrets and reed-solomon codes," *Commun. ACM*, vol. 24, no. 9, pp. 583–584, 1981.
- [8] J. S. Plank, "T1: Erasure codes for storage applications," in *Proc. 4th USENIX Conf. File Storage Technol.*, 2005, pp. 1–74.
- [9] R. Kulkarni, A. Forster, and G. Venayagamoorthy, "Computational intelligence in wireless sensor networks: A survey," *IEEE Commun. Surv. Tuts.*, vol. 13, no. 1, pp. 68–96, First Quarter 2011.
- [10] Z. Xia, X. Wang, L. Zhang, Z. Qin, X. Sun, and K. Ren, "A privacy-preserving and copy-deterrence content-based image retrieval scheme in cloud computing," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 11, pp. 2594–2608, Nov. 2016.

APPENDIX

A. Paper Acceptance Mail



5th International Conference on
Trends in Electronics and Informatics
(ICOEI 2021)

3-5, June 2021 | icoei.com/2021 | icoei.conf@gmail.com

Letter of Acceptance

To

T.Anandhi, Assistant Professor, D.Rohit, G.Bharat,
E.Brumania, Assistant Professor, R.M.Gomathi, Assistant Professor, P.Ajitha,
Associate Professor, School of Computing,
Sathyabama Institute Of Science And Technology, Chennai, India.

Greetings!!

On behalf of the SCAD College of Engineering and Technology Tirunelveli, we take great pleasure in inviting you to attend the "5th International Conference on Trends in Electronics and Informatics (ICOEI 2021)" which is going to be held during 3-5, June 2021 at Tirunelveli, India.

We are glad to inform you that your submitted article entitled "Enhancing Data Security and Privacy Through Cloud Computing" [Paper id:ICOEI-082] has been accepted for publication at ICOEI 2021. We welcome you to join us and share your research and views. This conference will offer you an unforgettable experience in exploring new opportunities.

We look forward to seeing you at Tirunelveli, India.

With Thanks,

Yours' Sincerely

Dr.P. Ebby Darney,
Principal, SCAD College of Engineering
and Technology, Tirunelveli,
TamilNadu, India.

Proceedings by

ICOEI Previous Publications
[2020](#) [2019](#) [2018](#) [2017](#)

B. Plagiarism Report

Data security and privacy through cloud computing(modified).docx

ORIGINALITY REPORT

10%

SIMILARITY INDEX

8%

INTERNET SOURCES

6%

PUBLICATIONS

2%

STUDENT PAPERS

PRIMARY SOURCES

1

[docplayer.net](#)

Internet Source

2%

2

[worldwidescience.org](#)

Internet Source

2%

3

L. Malina, J. Hajny, P. Dzurenda, V. Zeman.
"Privacy-preserving security solution for cloud services", Journal of Applied Research and Technology, 2015

Publication

1%

C. Journal Paper

Enhancing Data Security and Privacy Through Cloud Computing

Abstract:

Cloud computing technology's progression Cloud storage technology is experiencing exponential growth and advancement as the volume of procedural code rises at an incredible rate. The cloud provider seems to have no recommendations for the knowledge and cloud data that is collected and processed internationally in the cloud. The bulk of confidentiality security systems rely on secure communications. Cloud computing is used to construct a three-layer storage approach. The designed system can enjoy the benefits of cloud services while also seeking to protect data security. The hash-solomon code methodology is used to segregate information into data sections in this case. This algorithm, that is premised on cognitive computing, can measure the allocation stored on cloud, fog, and local machine, respectively.

Keywords - Hash-solomon code, Fog computing, cloud computing, bucket framework

INTRODUCTION

In IT, cloud computing describes a type of IT outsourcing service, similar to how the supply of electricity is to be outsourced. Users can use only. You don't need to say, where the anxiety caused by electricity, how it occurred, or to transfer. For each day of the month, give it back. After cloud computing, the idea is similar to: The user can only use storage, computing power, is, or has been called upon with the development of the profession, for them is a work of the anguish of a freedom of those on the outside. Cloud computing is generally internet-based computing. The cloud is the Internet computer network diagram metaphor for how the Internet is depicted; how the removal of everything is hiding in the Internet infrastructure. There is a way in which the related count developer are provided as a service, "allowing users of Internet access technology (" cloud ") services is not

knowledge or power technologies after servers.

And that the clouds with a great mist can be perceived and the means to count it and to give itself to the works, which is increased by the flow for an example of the difficulty of the thing. This results in a lack of quality of the content obtained. The effects of fog on a large computer and computer system vary. However, a common method that can be extracted is a limitation in the distribution of accurate content, and the problem is that creating and examining metrics that attempt to improve accuracy. Networking of fog by plane and data control plan. For example, in the data plane, cloud computing allows metering to reside at the edge of network information services, as opposed to central servers. Compared to cloud computing, cloud computing emphasizes proximity to end users and a customer for some, dense geographic distribution and the pooling of local

resources, latency for people and savings in bandwidth for achieve better Quality of Service (QoS) and mining edge analytics / flow; so that it becomes the top redundancy and user experience, it can only be, even if they did not use the AAL to pass, that the lack of missions. To protect user privacy, we offer a framework according to the TLS cloud computing model. TSL is a power user management framework that can effectively protect user privacy. With which the interiors were barely able to attack. Traditional approaches to work without, and so on, in the attacks, but with the CSP is proportional to the difficulties, all the traditional ways of being null. In several traditional ways in our program, Customer information is divided into 3 areas with a different size encryption technology. The computer model fog is collected, and the different parts of the information are stored on cloud server, the user fog server and the machine room, from short to long. And recovered via an old-age opponent, if knowledge is not certain knowledge in this way, it adorns the User as a whole. CSP and that this will not be useful information Without a cloud server and the name of the stored data on the local system, the name of the local server and of any machine at the time of the world, and most certainly only the cloud of users.

LITERATURE SURVEY

Title 1: Privacy-preserving security solution for cloud services

Author: L. Malina*, J. Hajny, P. Dzurenda and V. Zeman

A current top reliability analysis for cloud computing safety. Our approach is focused on the essence of the identity for some anonymity in obtaining cloud data storage to a community of semi and distributed databases. Introduces a better data encryption solution for active users. As a result, users' individual

characteristics (date of birth, valid enrollment, and accurate fee) can be illustrated despite revealing their identifications, and cloud providers can use their resources without threat behavioral profiling. If the user's supplier breaches the appropriate access, it'll be terminated. Our solution gives access to anonymous, and is transmitted to the knowledge of the secret of the possibility of dissociating. We have a proof of concept application to implement our solution and the results of this experiment. In addition, privacy solutions for cloud services execute a foolproof rule, and group signing of core skills to the role of privacy enhancing results for cloud services. From there, we compare our performance with associated solutions and diagrams.

Title 2: A secure data privacy preservation for on-demand cloud service

Author: Chandramohan Dhasarathan*, Vengattaraman Thirumal, Dhavachelvan Ponnuramam

This paper brings to light the problems of the disciples, and of the intellectual obfuscation, the finance and insurance industries are confidential information belonging to the name of the. The secret of authoritarian times information that is hidden, so the danger of misuse of the thing. To be cut out and given to us in the name of the third part of the Software by the services of digital steel its heart. Responsibility for business continuity in the digital secrecy project and in widely dispersed regions of the world, and close to its mismanagement causing a preventive breach of confidentiality of the service from the cloud, where a huge amount of data is stored and maintained tremendously. In this

developing world of computing to cloud, protecting user privacy is a big issue, even with changes in the field of cloud computing to improve its efficiency, efficiency and optimization among developers. Office, etc., information reliability and cloud user identification and maintainability privacy may vary for different CPs (Cloud providers). CP is done as stated in the user owns information and today's technology is more related to my heart, do they work. No, but they have the cloud provider issue that is most important when it comes to data suggestions for cloud and digital data storage that you do, this way and that, and keep it. , worldwide. The reason for the need for the issues proposed in cloud computing research. We arrived at the Privacy offering of Prevent Loss Model the digital data recorded in the cloud (ppm, dDLC). This proposal helps the CR (Requester cloud / users) to have confidence in proprietary data and data stored in the cloud.

Title 3: A Survey on Secure Storage Services in Cloud Computing

Author: Ms. B.Tejaswi, Dr. L.V.Reddy & Ms. M.Leelavathi

Cloud computing is an emerging technology that is simple and its Internet environment. It provides users, such as various offices, Software-in-a-Service (SaaS), PaaS, IaaS, Order-at-a-Service (SaaS). For-use-to-a-service, the security of data with which users interact and organizations cannot store their data in the cloud, the new commander, the risk of changes in the accuracy of the order of. It represents a consumer technology divided between various arts like Porta integrity of the audit mechanism, gave plaster encoded data, Merkle hash tree, construction (MHT), etc. These techniques help secure data storage and an efficient dynamic cloud.

This article discusses privacy and security architectures in day-to-day management in cloud storage.

Title 4: On a Relation Between Verifiable Secret Sharing Schemes and a Class of Error-Correcting Codes

Author: Ventzislav Nikov and Svetla Nikova

We are trying to kill the participation of new information on verifiable secret plans (vss). Define a new one for us, "metric" (the properties look slightly different from a standard Hamming meter). This is the most widely used type of metric definition codes, that is, an error correction code defining a forbidden space by prescription, increasing or decreasing the monotonic set. Then redefine what we went to a new problem package, and the settings fix these errors is usually an opportunity to fix the error, but some code (taking into account this fresh metric and new package). Error correction technique, of which it is well known that the VSS and distributed commitments (600) in pairs by holding the test protocol and the error correction capability of the error correction codes establish interleaving.

Existing System:

Three database centers were used to divide and access information by using hash-Solomon code algorithm in the existing system namely cloud , fog , and local PC. The reality that the third party is clueless of our info splitting is key.The Web server holds 80percent of total of the critical data, the Fog layer processes 15% of the most necessary info, and the Base station will comprise 5percent of the overall of the useful data.If a scammer address potential in anyone of these

servers, he or she will either alter or delete information. As a result, the user will end up losing that data. It's the most massive disadvantage.

Proposed system:

To protect and preserve the missing data, we will use bucket system. Bucket is similar to a mirror within this any data the user enters is saved automatically in the bucket system. We introduced a multi BCH code algorithm for data comparison, with synchronized data preserved in a bucket.

Algorithm:

Hash soloman:

The Hash-Solomon code algorithm is primarily used to separate data into parts. The information is divided into three sections and stored in this location. Information is divided into groups based on the value of the knowledge found within it.

bucket:

This mechanism is explicitly designed to allow the user to recover deleted data or manipulated by a 3rd person.

Bucket serves as a reflection; whichever data the user enters is automatically saved in it.

BCH Algorithm:

The BCH codes, or Bose–Chaudhuri–Hocquenghem codes, are a type of cyclic error correcting codes that are developed using polynomials over a finite field in coding theory. One of the major benefits of BCH codes is that the amount of symbol errors that the code will correct could be accurately monitored during validation phase. It is possible to build binary BCH codes that can resolve several bit errors in particular. One attribute of BCH codes is its ease of decoding, which is accomplished using an arithmetic procedure known as

syndrome decryption. It optimises the decoder process for these codes, enabling over the use of compact, reduced embedded software.

MODULE DESCRIPTION

MODULES

- Entry
- Registration
- Storage Scheme
- Recovery Scheme

register module:

The user registers their account identification using this module by giving the absolute necessities of details. Users must only include minimum necessary of details, such as their email address, title, contact details, and pin, that would be used for subsequent logins. In order for them to be able to access the portal.

entry module:

It enables users to access the webpage via their authorized account and a valid pin. He or she would not be permitted to log in if he or she is not a legitimate user. The website can only be accessed and is used by authorized individuals.

storage module:

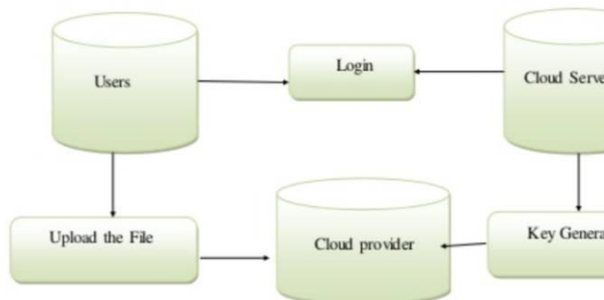
Users can store their files in three separate cloud server using this module. cloud server, fog server, and local server are the storage centers. we place 80% of our information on a central server. We store 15% of crucial information on the fog server. we hold 5% of the details on the local computer.

recovery module:

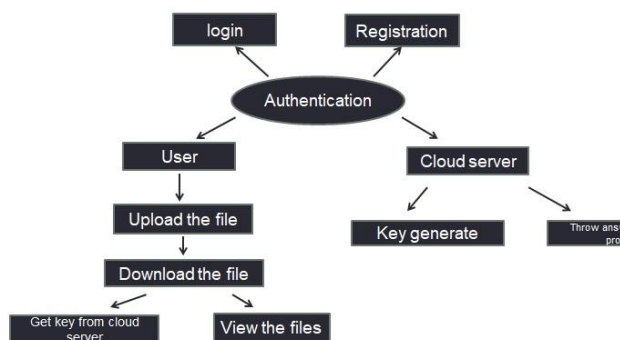
Users can retrieve documents from three separate cloud server using this module. If

data fits these three volumes of information, it is preserved in the bucket by using BCH method. The person can simply recover data from bin if its been hacked in any of the levels.

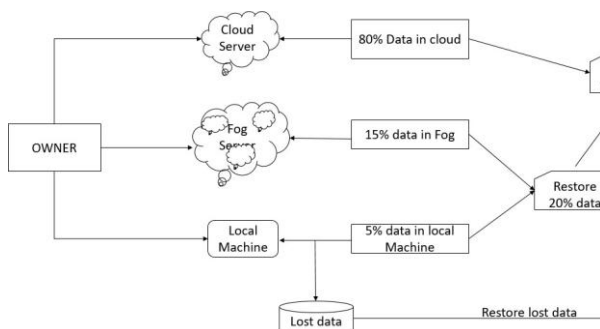
DATA FLOW DIAGRAM



ER Diagram



SYSTEM ARCHITECTURE



OUTPUT:

Register Module:

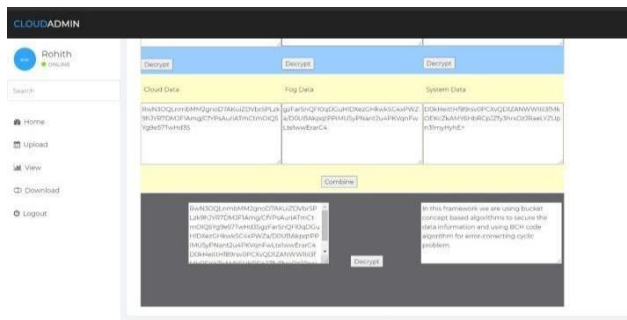
- This Module is used for registering new accounts by giving minimal info such as e-mail Id ,Name, Mobile number, password.

Login Module:

- The Entry module is used to login with the already registered account.

Storage Module:

- The above figure is used to upload the file which we want to store it in cloud.



- The above figure displays how the process behind encryption and decryption of the uploaded file.

CONCLUSION

We have a ton of space in our computing command center, ts.Cloud, which is a versatile platform that allows users to maximize their floor space. Even so, this leaves the door open to a slew of safe cloud storage difficulties. When people used cloud storage, it affected user management, and a monitoring resulting in the separation of information privacy of a website as well as its own users. To resolve a storage issue, protect our privacy in a cloud of fog under the TLS computer model to design and code the BCH algorithm. By the analysis of theoretical mastery, the knowledge of the safety of such a man is, so that when an asset is achievable. Due to the fact that the resource blocks are stored correctly in specific regions, we can guarantee the confidentiality of the info of each server.

REFERENCE

- [1] P. Mell and T. Grance, "The NIST definition of cloud computing," Nat.Inst. Stand. Technol., vol. 53, no. 6, pp. 50–50, 2009.
- [2] H. T. Dinh, C. Lee, D. Niyato, and P. Wang, "A survey of mobile cloud computing: Architecture, applications, and approaches," Wireless Commun. Mobile Comput., vol. 13, no. 18, pp. 1587–1611, 2013.
- [3] J. Chase, R. Kaewpuang, W. Yonggang, and D. Niyato, "Joint virtual machine and bandwidth allocation in software defined network (sdn) and cloud computing environments," in Proc. IEEE Int. Conf. Commun., 2014, pp. 2969–2974.
- [4] H. Li, W. Sun, F. Li, and B. Wang, "Secure and privacy-preserving data storage service in public cloud," J. Comput. Res. Develop., vol. 51, no. 7, pp. 1397–1409, 2014.
- [5] Y. Li, T. Wang, G. Wang, J. Liang, and H. Chen, "Efficient data collection in sensor-cloud system with multiple mobile sinks," in Proc. Adv. Serv. Comput., 10th Asia-Pac. Serv. Comput. Conf., 2016, pp. 130–143.
- [6] L. Xiao, Q. Li, and J. Liu, "Survey on secure cloud storage," J. Data Acquis. Process., vol. 31, no. 3, pp. 464–472, 2016.
- [7] R. J. McEliece and D. V. Sarwate, "On sharing secrets and reed-solomon codes," Commun. ACM, vol. 24, no. 9, pp. 583–584, 1981.

[8] J. S. Plank, "T1: Erasure codes for storage applications," in Proc. 4th USENIX Conf. File Storage Technol., 2005, pp. 1–74.

[9] R. Kulkarni, A. Forster, and G. Venayagamoorthy, "Computational intelligence in wireless sensor networks: A survey," IEEE Commun. Surv. Tuts.,

vol. 13, no. 1, pp. 68–96, First Quarter 2011.

[10] Z. Xia, X. Wang, L. Zhang, Z. Qin, X. Sun, and K. Ren, "A privacy-preserving and copy-deterrence content-based image retrieval scheme in cloud computing," IEEE Trans. Inf. Forensics Security, vol. 11, no. 11, pp. 2594–2608, Nov. 2016.

D. Source code

Login page

```
<%@ Page Language="C#" AutoEventWireup="true" CodeFile="Login.aspx.cs"
Inherits="Login" %>
```

```
<!DOCTYPE html>
```

```
<html xmlns="http://www.w3.org/1999/xhtml">
```

```
<head runat="server">
```

```
    <meta charset="utf-8">
```

```
    <meta name="viewport" content="width=device-width, initial-scale=1">
```

```
    <title>Lumino - Login</title>
```

```
    <link href="css/bootstrap.min.css" rel="stylesheet">
```

```
    <link href="css/datepicker3.css" rel="stylesheet">
```

```
    <link href="css/styles.css" rel="stylesheet">
```

```
    <!--[if lt IE 9]>
```

```
    <script src="js/html5shiv.js"></script>
```

```
    <script src="js/respond.min.js"></script>
```

```
    <![endif]-->
```

```
</head>
```

```
<body>
```

```
    <div class="row">
```

```

<div class="col-xs-10 col-xs-offset-1 col-sm-8 col-sm-offset-2 col-md-4
col-md-offset-4">
    <div class="login-panel panel panel-default">
        <div class="panel-heading">Log in</div>
        <div class="panel-body">
            <form id="form1" runat="server" role="form">

                <fieldset>
                    <div class="form-group">
                        <asp:TextBox ID="TextBox1" runat="server" class="form-control" placeholder="E-
                        mail" name="email" ></asp:TextBox>

                    </div>
                    <div class="form-group">
                        <asp:TextBox ID="TextBox2" runat="server" class="form-control"
                        placeholder="Password" name="password" type="password" ></asp:TextBox>

                    </div>
                    <div class="form-group">
                        <asp:Button ID="Button1"
                        runat="server" class="btn btn-primary" Text="Login" OnClick="Button1_Click"
                        Width="101px" />
                    </div>
                    <div class="form-group">
                        <asp:Button ID="Button2" runat="server" class="btn btn-primary"
                        Text="Register" OnClick="Button2_Click" />
                    </div>

                </form>
            </div>
        </div>
    </div><!-- /.col-->
</div><!-- /.row -->

```

```

<script src="js/jquery-1.11.1.min.js"></script>
    <script src="js/bootstrap.min.js"></script>
</body>
</html>

```

Register:

```

<%@ Page Language="C#" AutoEventWireup="true" CodeFile="Register.aspx.cs"
Inherits="Register" %>

```

```

<!DOCTYPE html>

```

```

<html xmlns="http://www.w3.org/1999/xhtml">
<head runat="server">

```

```

    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <title>Lumino - Login</title>
    <link href="css/bootstrap.min.css" rel="stylesheet">
    <link href="css/datepicker3.css" rel="stylesheet">
    <link href="css/styles.css" rel="stylesheet">
    <!--[if lt IE 9]>
    <script src="js/html5shiv.js"></script>
    <script src="js/respond.min.js"></script>
    <![endif]-->

```

```

</head>

```

```

<body>

```

```

    <div class="row">

```

```

        <div class="col-xs-10 col-xs-offset-1 col-sm-8 col-sm-offset-2 col-md-4
col-md-offset-4">

```

```

            <div class="login-panel panel panel-default">

```

```

                <div class="panel-heading">Register</div>

```

```

                <div class="panel-body">

```

```

                    <form id="form1" runat="server" role="form">

```

[illegible]


```

<tr>
  <td style="width: 77px; height: 557px"></td>
  <td style="width: 498px; height: 557px">
    <asp:Panel      ID="Panel1"      runat="server"      Height="737px"
BorderColor="#CCFFFF">
      <table style="width:100%; background-color: #99CCFF;">
        <tr>
          <td style="width: 184px; height: 20px;"></td>
          <td style="width: 227px; height: 20px;">
            <asp:Label      ID="StatusLabel"      runat="server"
ForeColor="Red"></asp:Label>
          </td>
          <td style="height: 20px"></td>
        </tr>
        <tr>
          <td style="width: 184px">
            <asp:Label      ID="Label1"      runat="server"      Text="Select
File"></asp:Label>
          </td>
          <td style="width: 227px">&nbsp;</td>
          <td>&nbsp;</td>
        </tr>
        <tr>
          <td style="width: 184px">&nbsp;</td>
          <td style="width: 227px">
            <asp:FileUpload ID="FileUpload1" runat="server" />
          </td>
          <td>&nbsp;</td>
        </tr>
        <tr>
          <td style="width: 184px">&nbsp;</td>
          <td style="width: 227px">&nbsp;</td>
          <td>&nbsp;</td>
        </tr>
      </table>
    </td>
  </tr>

```

```

        <tr>
            <td style="width: 184px">&nbsp;</td>
            <td style="width: 227px">&nbsp;</td>
            <td>&nbsp;</td>
        </tr>
        <tr>
            <td style="width: 184px">&nbsp;</td>
            <td style="width: 227px">&nbsp;</td>
            <td>
                <asp:Button ID="Button1" runat="server" Text="Upload"
Width="85px" OnClick="Button1_Click" />
            </td>
        </tr>
    </table>
</asp:Panel>
</td>
<td style="height: 557px"></td>
</tr>
<tr>
    <td style="width: 77px">&nbsp;</td>
    <td style="width: 498px">&nbsp;</td>
    <td>&nbsp;</td>
</tr>
</table>
</div>
</asp:Content>

```

View page :

```

<%@ Page Title="" Language="C#" MasterPageFile="~/Home.master"
AutoEventWireup="true" CodeFile="view.aspx.cs" Inherits="view" %>

<asp:Content ID="Content1" ContentPlaceHolderID="ContentPlaceHolder1"
Runat="Server">

```



```

        <asp:Button ID="Button4" runat="server" OnClick="Button4_Click"
Text="Decrypt" />
    </asp:Panel>
</td>
<td style="height: 259px">
    <asp:Panel ID="Panel2" runat="server" BackColor="#99CCFF"
Height="253px">
        <br />
        &nbsp;
        <asp:Label ID="Label2" runat="server" Text="Fog Data"></asp:Label>
        <br />
        <br />
        <asp:TextBox ID="TextBox4" runat="server" Height="132px"
TextMode="MultiLine" Width="315px"></asp:TextBox>
        <br />
        <br />
        <asp:Button ID="Button2" runat="server" OnClick="Button2_Click"
Text="Decrypt" />
    </asp:Panel>
</td>
<td style="height: 259px">
    <asp:Panel ID="Panel3" runat="server" BackColor="#99CCFF"
Height="253px">
        &nbsp;<br />
        <asp:Label ID="Label3" runat="server" Text="System Data"></asp:Label>
        <br />
        <br />
        <asp:TextBox ID="TextBox5" runat="server" Height="131px"
TextMode="MultiLine" Width="315px"></asp:TextBox>
        <br />
        <br />
        <asp:Button ID="Button3" runat="server" OnClick="Button3_Click"
Text="Decrypt" />
    </asp:Panel>

```



```
</Columns>
</asp:GridView>
</asp:Content>
```

Delete:

```
<%@ Page Title="" Language="C#" MasterPageFile="~/Home.master"
AutoEventWireup="true" CodeFile="Delete.aspx.cs" Inherits="Delete" %>
```

```
<asp:Content ID="Content1" ContentPlaceHolderID="ContentPlaceHolder1"
Runat="Server">
</asp:Content>
```