

# **HYBRID INTRUSION DETECTION SYSTEM FOR CLOUD COMPUTING ENVIRONMENTS**

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

by

**Kasi satya, (Reg.No38110243)**



**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**

**MARCH - 2020**



# **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](http://www.sathyabama.ac.in)



## **DEPARTMENT OF COMPUTER SCIENCE ENGINEERING**

### **BONAFIDE CERTIFICATE**

**This is to certify that this Project Report is the bonafide work of Kasi satya, (Reg.No38110243) who Carried out the project entitle "HYBRID INTRUSION DETECTION SYSTEM FOR CLOUD COMPUTING ENVIRONMENTS" under my supervision from November 2019 to March 2020**

**Internal Guide**

**Dr.SrideviM.E.,Ph.D.,**

**Head of the Department**

**Dr. S. VIGNESHWARI, M.E., Ph.D.**

---

**Submitted for Viva voce Examination held on \_\_\_\_\_**

**Internal Examiner**

**External Examiner**

## **DECLARATION**

**I Kasi satya, (Reg.No38110243) hereby declare that the Project Report entitled “HYBRID INTRUSION DETECTION SYSTEM FOR CLOUD COMPUTING ENVIRONMENTS” done by me under the guidance of Dr.Sridevi M.E.,Ph.D is submitted in partial fulfillment of the requirements for the award of Bachelor of Engineering degree in Computer Science and Engineering.**

**DATE:**

**PLACE:**

**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.SAIKALA, M.E., Ph.D, Dean**, School of Computing ,

**Dr.S.VIGNESHWARI, M.E., Ph.D. and Dr.L.LAKSHMANAN, M.E., Ph.D. ,**

Heads of the Department of Computer Science & 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 **Dr.Sridevi M.E.,Ph.D** for his 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 & Engineering** who were helpful in many ways for the completion of the project.

## **ABSTRACT**

Today data sharing and maintaining its security is major challenge. User in the data sharing system upload their file with the encryption using private key. This property is especially important to any large scale data sharing system, as any user leak the key information then it will become difficult for the data owner to maintain security of the information. In this paper provide a concrete and efficient instantiation of scheme, prove its security and provide an implementation to show its practicality. There are lots of challenges for data owner to share their data on servers or cloud. There are different solutions to solve these problems. These techniques are very much critical to handle key shared by the data owner. This paper will introduce the trusted authority to authenticate user those who have the access to the data on cloud. SHA algorithm is used by the trusted authority to generate the key and that key will get share to user as well as the owner. The trusted authority module receives encrypted file using AES Algorithm from the data owner and computes hash value using MD-5 algorithm. It stores key in its database which will be used during the dynamic operations and to determine the cheating party in the system (CSP or Owner). Trusted authority send file to CSP module to store on cloud. The resulting key sets are shown to have a number of desirable properties that ensure the confidentiality of communication sessions against collusion attacks by other network nodes

# TABLE OF CONTENTS

| <b>CHAPTER No.</b> | <b>CHAPTER NAME</b>                                  | <b>PAGE No.</b> |
|--------------------|------------------------------------------------------|-----------------|
|                    | <b>ABSTRACT</b>                                      | <b>v</b>        |
|                    | <b>LIST OF TABLES</b>                                | <b>viii</b>     |
|                    | <b>LIST OF FIGURES</b>                               | <b>ix</b>       |
|                    | <b>LIST OF ABBREVIATIONS</b>                         | <b>x</b>        |
| <b>1</b>           | <b>INTRODUCTION</b>                                  | <b>01</b>       |
|                    | 1.1 Establishment                                    | <b>01</b>       |
|                    | 1.2 Objective                                        | <b>02</b>       |
|                    | 1.3 Literature Survey                                | <b>02</b>       |
|                    | 1.3.1 Efficient and verifiable<br>outsourcing Scheme | <b>02</b>       |
|                    | 1.3.2 Secure Outsourcing                             | <b>03</b>       |
|                    | 1.3.3 Secure and private<br>sequence comparisions    | <b>03</b>       |
|                    | 1.4 Existing System                                  | <b>05</b>       |
|                    | 1.5 Disadvantages                                    | <b>05</b>       |
|                    | 1.6 Proposed System                                  | <b>05</b>       |
|                    | 1.7 Advantages of Proposed System                    | <b>06</b>       |
| <b>2</b>           | <b>SYSTEM REQUIREMENTS</b>                           | <b>08</b>       |
|                    | 2.1 Hardware Requirements                            | <b>08</b>       |
|                    | 2.2 Software Requirements                            | <b>08</b>       |
|                    | 2.3 Introduction                                     | <b>08</b>       |
|                    | 2.4 Application of Java                              | <b>08</b>       |
|                    | 2.5 Features of Java                                 | <b>09</b>       |
|                    | 2.6 Collection Framework                             | <b>10</b>       |
|                    | 2.7 MySql                                            | <b>11</b>       |
|                    | 2.8 Feasibility Study                                | <b>12</b>       |
|                    | 2.10 Technical Feasibility                           | <b>12</b>       |

|          |                                    |           |
|----------|------------------------------------|-----------|
|          | 2.11 Social Feasibility            | 13        |
|          | 2.12 Requirement Analysis          | 13        |
|          | 2.13 Functional Requirements       | 13        |
|          | 2.14 Non Functional Requirements   | 14        |
|          | 2.14.1 Portability                 | 14        |
|          | 2.14.2 Performance                 | 14        |
|          | 2.14.3 Accuracy                    | 14        |
| <b>3</b> | <b>SYSTEM IMPLEMENTATION</b>       | <b>15</b> |
|          | 3.1 Implementation                 | 15        |
|          | 3.2 Login Module                   | 15        |
|          | 3.3 Registration Module            | 15        |
|          | 3.4 Creation Storage and Instance  | 16        |
|          | 3.5 Find Collusion Module          | 16        |
|          | 3.6 Find Third Party Module        | 16        |
|          | 3.7 UML Diagram                    | 16        |
|          | 3.8 Goals                          | 17        |
|          | 3.9 Use Case Diagram               | 17        |
|          | 3.10 Class Diagram                 | 18        |
|          | 3.11 Sequence Diagram              | 19        |
| <b>4</b> | <b>RESULTS AND DISCUSSION</b>      | <b>20</b> |
|          | 4.1 System Design and Testing Plan | 22        |
|          | 4.1.1 Input Design                 | 22        |
|          | 4.1.2 Output Design                | 23        |
|          | 4.2 Testing Process                | 23        |
|          | 4.2.1 Unit Testing                 | 23        |
|          | 4.2.2 Integration Testing          | 24        |
|          | 4.2.3 Functional Testing           | 24        |
|          | 4.3 Test Strategy and Approach     | 25        |
|          | 4.3.1 Test objectives              | 25        |

|          |                                   |           |
|----------|-----------------------------------|-----------|
|          | 4.4 Integration Testing           | 25        |
|          | 4.4.1 Acceptance Testing          | 26        |
|          | 4.4.2 Alpha Testing               | 26        |
|          | 4.4.3 Beta Testing                | 26        |
| <b>5</b> | <b>CONCLUSION AND FUTURE WORK</b> | <b>27</b> |
|          | 5.1 Conclusion                    | 27        |
|          | 5.2 Future Work                   | 27        |
|          | <b>REFERENCES</b>                 | <b>28</b> |
|          | <b>APPENDIX</b>                   | <b>29</b> |

## LIST OF FIGURES

| FIGURE No. | FIGURE NAME          | PAGE No. |
|------------|----------------------|----------|
| 1.1        | System Architecture  | 13       |
| 2.1        | Compile Procedure    | 17       |
| 2.2        | Collection Framework | 18       |
| 3.1        | User Case Diagram    | 19       |
| 3.2        | Class Diagram        | 20       |
| 3.3        | Sequence Diagram     | 26       |
| 4.1        | Unit Testing         |          |
| 4.2        | Login Page           |          |
| 4.3        | Admin Login Page     |          |

## LIST OF ABBREVIATIONS

|     |                              |
|-----|------------------------------|
| SHA | Secure Hashing Algorithm     |
| MD5 | Message Digest Alogorithm    |
| AES | Advanced encryption Standard |

# CHAPTER-1

## INTRODUCTION

### 1.1 ESTABLISHMENT

One possible solution is to migrate character sequences to public cloud computing platforms and to request that Cloud Service Providers process sequence comparisons. At present, primary sequence comparison algorithms are deployed as a universal outsourcing service on public clouds. But at the same time, its security and privacy issues are increasingly emerging. The outsourced data stored as plaintext could easily be exposed to malicious external intruders and internal attackers in the CSP, and the individual private information carried by character sequences (e.g., personal identification, financial transaction records, genetic markers for some diseases, information that is used to identify paternity or maternity, etc.) could more or less be disclosed or abused. Therefore, secure outsourcing is designed to protect the privacy of character sequences, and to ensure that the scheduled computing requests are normally performed on the cloud servers.

For this purpose, we present a scheme called Encrypted Sequence Comparison based on a single-server model. Some novel salted hash and encryption techniques are employed to allow public clouds to perform sequence comparisons directly on the character sequences outsourced as ciphertext. Overall, E-SC achieves a user-controlled reliable storage and a collusion-resistant outsourcing service, which plays an important role in the trade-off between security and execution performance. Our scheme is easy in deployment, efficient in processing and controllable in overhead. Based on the universal model of a public cloud outsourcing, we propose an overall architecture for E-SC. This architecture is built on the end user and the unmodified CSP. Its overall system model, which has been demonstrated to be secure under the threat model, is user-friendly and implementation-friendly.

A salted hash algorithm is improved to hash the character sequences and the indexes of cost matrices, so as to defend against statistical attacks. An additive order preserving encryption algorithm is designed to encrypt the elements of cost matrices. Also, this algorithm can achieve an indistinguishability under additive ordered chosen-plaintext attack with linear time complexity.

A single cloud server works for the first time to provide a privacy-preserving computable outsourcing service to effectively resist collusion attacks from the cloud. With pre-processing modules of padding, partition, and expansion, there is no need to decrypt any outsourced data in the non-interactive sequence comparison stage.

Simulation results show that the overall execution performance of our E-SC is negatively correlated with its security.

## **1.2 OBJECTIVE**

The main objective of this system is, SHA algorithm is used by the trusted authority to generate the key and that key will get share to user as well as the owner. The trusted authority module receives encrypted file using AES Algorithm from the data owner and computes hash value using MD-5 algorithm.

## **1.3 LITERATURE SURVEY**

Literature survey is the most important step in software development process. Before developing the tool it is necessary to determine the time factor, economy and company strength. Once these things are satisfied, then the next step is to determine which operating system and language can be used for developing the tool. Once the programmers start building the tool the programmers need lot of external support. This support can be obtained from senior programmers, from book or from websites. Before building the system the above consideration are taken into account for developing the proposed system.

The major part of the project development sector considers and fully survey all the required needs for developing the project. For every project Literature survey is the most important sector in software development process. Before developing the tools and the associated designing it is necessary to determine and survey the time factor, resource requirement, man power, economy, and company strength. Once these things are satisfied and fully surveyed, then the next step is to determine about the software specifications in the respective system such as what type of operating system the project would require, and what are all the necessary software are needed to proceed with the next step such as developing the tools, and the associated operations.

### **1.3.1 TITLE: Efficient and verifiable outsourcing scheme of sequence comparisons**

**AUTHOR:** Y. Feng, H. Ma, and X. Chen

With the rapid development of cloud computing, the techniques for securely outsourcing prohibitively expensive computations are getting widespread attentions in the scientific community. In the outsourcing computation paradigm, the clients with resource-constrained abilities can outsource the heavy computation workloads into the cloud server and enjoy unlimited computing resources in a pay-per-use manner. One of the most critical functionalities in outsourcing computation is the verifiability of the result. That is, the client should efficiently verify the validity of the result returned by the cloud servers. In this paper, we solve the problem of verifiable outsourcing computation of sequence comparisons by integrating the technique of Yao's garbled circuit with homomorphic encryption. Compared with the existing schemes, our proposed solution enables clients to efficiently detect the misbehavior of dishonest servers. Furthermore, our construction re-garbles the circuit only for malformed responses and thus is very efficient for real-world applications. Besides, we also present the formal analysis for our proposed construction.

### **1.3.2 TITLE: Secure outsourcing of sequence comparisons**

**AUTHOR:** M. J. Atallah and J. Li

With the advent of cloud computing, secure outsourcing techniques of sequence comparisons are becoming increasingly valuable, especially for clients with limited resources. One of the most critical functionalities in data outsourcing is verifiability. However, there is very few secure outsourcing scheme for sequence comparisons that the clients can verify whether the servers honestly execute a protocol or not. In this paper, we tackle the problem by integrating the technique of garbled circuit with homomorphic encryption. As compared to existing schemes, our proposed solution enables clients to efficiently detect the dishonesty of servers. In particular, our construction re-garbles the circuit only for malformed responses and hence is very efficient. Besides, we also present the formal analysis for our proposed construction.

### **1.3.3 TITLE: Secure and private sequence comparisons**

**AUTHOR:** M. J. Atallah, F. Kerschbaum, and W. Du

We give an efficient protocol for sequence comparisons of the edit-distance kind, such that neither party reveals anything about their private sequence to the other party (other than what can be inferred from the edit distance between their two sequences – which is unavoidable because computing that distance is the purpose of the protocol). The amount of communication done by our protocol is proportional to the time complexity of the best-known algorithm for performing the sequence comparison. The problem of determining the similarity between two sequences arises in a large number of applications, in particular in bioinformatics. In these application areas, the edit distance is one of the most widely used notions of sequence similarity: It is the least-cost set of insertions, deletions, and substitutions required to transform one string into the other. The generalizations of edit distance that are solved by the same kind of dynamic programming recurrence relation as the one for edit distance, cover an even wider domain of applications.

#### **1.3.4 TITLE: Toward a practical data privacy scheme for a distributed implementation of the Smith-Waterman genome sequence comparison algorithm**

**AUTHOR:** D. Szajda, M. Pohl, J. Owen, and B. Lawson

Volunteer distributed computations utilize spare processor cycles of personal computers that are connected to the Internet. The resulting platforms provide computational power previously available only through the use of expensive clusters or supercomputers. However, distributed computations running in untrustworthy environments raise a number of security concerns, including computation integrity and data privacy. This paper introduces a strategy for enhancing data privacy in some distributed volunteer computations, providing an important first step toward a general data privacy solution for these computations. The strategy is used to provide enhanced data privacy for the Smith-Waterman local nucleotide sequence comparison algorithm. Our modified Smith-Waterman algorithm provides reasonable performance, identifying most, and in many cases all, sequence pairs that exhibit statistically significant similarity according to the unmodified algorithm, with reasonable levels of false positives. Moreover the modified algorithm achieves a net decrease in execution time, with no increase in memory requirements. Most importantly, our scheme

represents an important first step toward providing data privacy for a practical and important real-world algorithm.

### **1.3.5 TITLE: New algorithms for secure outsourcing of modular exponentiations**

**AUTHOR:** X. Chen, J. Li, J. Ma, Q. Tang, and W. Lou

Modular exponentiations have been considered the most expensive operation in discrete-logarithm based cryptographic protocols. In this paper, we propose a new secure outsourcing algorithm for exponentiation modular a prime in the one-malicious model. Compared with the state-of-the-art algorithm [33], the proposed algorithm is superior in both efficiency and checkability. We then utilize this algorithm as a subroutine to achieve outsource-secure Cramer-Shoup encryptions and Schnorr signatures. Besides, we propose the first outsource-secure and efficient algorithm for simultaneous modular exponentiations. Moreover, we prove that both the algorithms can achieve the desired security notions.

## **1.4 EXISTING SYSTEM**

Large-scale problems in the physical and life sciences are being revolutionized by Internet computing technologies, like grid computing, that make possible the massive cooperative sharing of computational power, bandwidth, storage, and data. A weak computational device, once connected to such a grid, is no longer limited by its slow speed, small amounts of local storage, and limited bandwidth: It can avail itself of the abundance of these resources that is available elsewhere on the network. An impediment to the use of “computational outsourcing” is that the data in question is often sensitive, e.g., of national security importance, or proprietary and containing commercial secrets, or to be kept private for legal requirements such as the HIPAA legislation, Gramm-Leach-Bliley, or similar laws. This motivates the design of techniques for computational outsourcing in a privacy-preserving manner, i.e., without revealing to the remote agents whose computational power is being used, either one’s data or the outcome of the computation on the data.

## **1.5 DISADVANTAGES OF EXISTING SYSTEM**

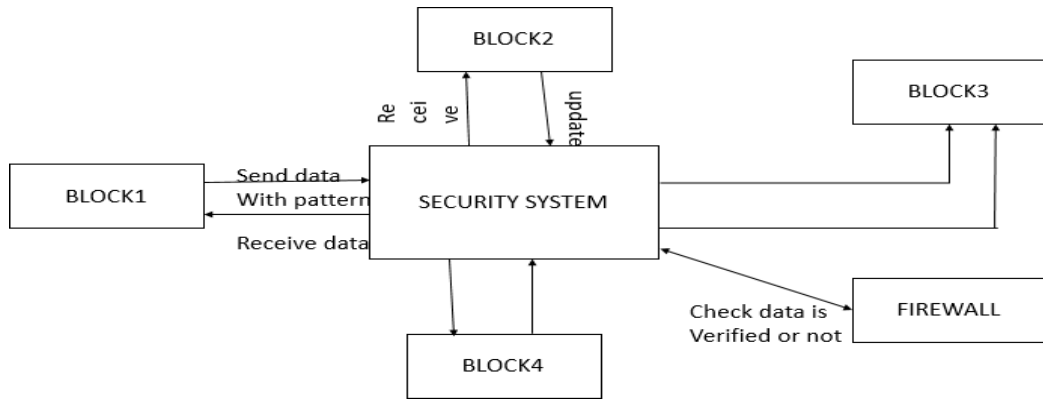
- Secure outsourcing for widely applicable sequence comparison problems
- Risk of Leak of Secret Information

## **1.6 PROPOSED SYSTEM**

We propose a secure data sharing scheme, which can achieve secure key distribution and data sharing for dynamic group. We provide a secure way for key distribution without any secure communication channels. The users can securely obtain their private keys from group manager without any Certificate Authorities due to the verification for the public key of the user. Our scheme can achieve fine-grained access control, with the help of the group user list, any user in the group can use the source in the cloud and revoked users cannot access the cloud again after they are revoked. We propose a secure data sharing scheme which can be protected from collusion attack. The revoked users can not be able to get the original data files once they are revoked even if they conspire with the untrusted cloud. Our scheme can achieve secure user revocation with the help of polynomial function. Our scheme is able to support dynamic groups efficiently, when a new user joins in the group or a user is revoked from the group, the private keys of the other users do not need to be recomputed and updated. We provide security analysis to prove the security of our scheme.

## **1.7 ADVANTAGES OF PROPOSED SYSTEM**

- Power Means of Persuasion and control
- More Reliable
- It's more secure and efficient.
- Data confidentiality



***Fig 1.1 SYSTEM ARCHITECTURE***

## **CHAPTER-2**

### **SYSTEM REQUIREMENTS**

#### **2.1 HARDWARE REQUIREMENTS:**

- System - Pentium-IV
- Speed - 2.4GHZ
- Hard disk - 40GB
- Monitor - 15VGA color
- RAM - 512MB

#### **2.2 SOFTWARE REQUIREMENTS:**

- Operating System - Windows XP
- Coding language - Java
- IDE - Net beans
- Database -MYSQL

#### **2.3 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 weared with passage of time, while Java's has grown.

#### **2.4 APPLICATION OF JAVA**

Java is widely used in every corner of world and of human life. Java is not only used in softwares 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.

#### **2.5 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

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.

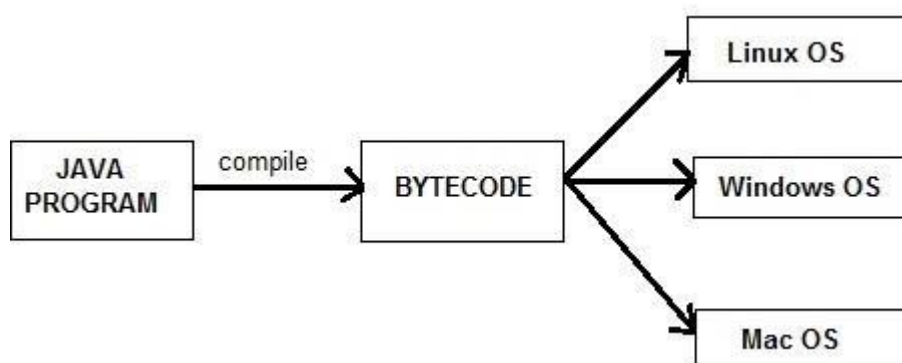
*Eg:* Pointers and Operator Overloading are not there in java but were an important part of C++

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

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.

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 provide security. Any machine with Java Runtime Environment can run Java Programs.



### ***Fig 2.1 compile procedure***

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 it is more secure.

Java multithreading feature makes it possible to write program that can do many tasks 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.

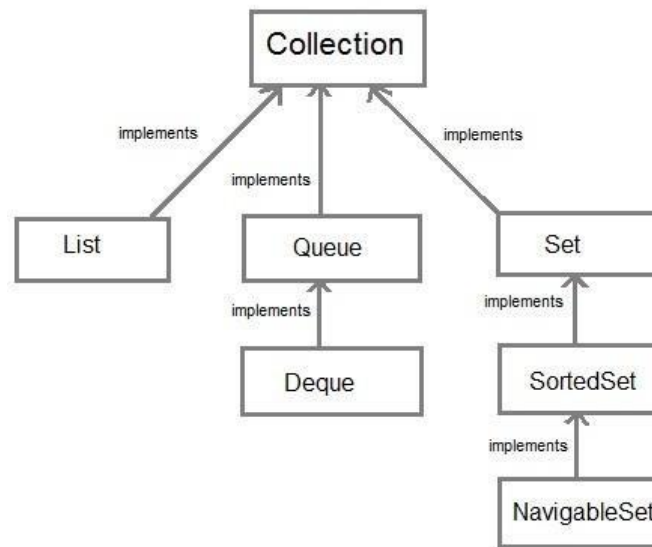
Compiler generates byte codes, which have nothing to do with a particular computer architecture, hence a Java program is easy to interpret on any machine.

Java Byte code can be carried to any platform. No implementation dependent features. Everything related to storage is predefined, example: size of primitive data types.

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.

## **2.6 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 2.2 collection framework**

## 2.7 MYSQL

MySQL, officially, but also called "My Sequel" is the world's most widely used open-source relational database management system (RDBMS) that runs as a server providing multi-user access to a number of databases, though SQLite probably has more total embedded deployments. The SQL phrase stands for Structured Query Language.

The MySQL development project has made its source code available under the terms of the GNU General Public License, as well as under a variety of proprietary agreements. MySQL was owned and sponsored by a single for-profit firm, the Swedish company MySQL AB, now owned by Oracle Corporation. MySQL is a popular choice of database for use in web applications, and is a central component of the widely used LAMP open source web application software stack (and other 'AMP' stacks).

LAMP is an acronym for "Linux, Apache, MySQL, Perl/PHP/Python." Freesoftware-open source projects that require a full-featured database management system often use MySQL.

For commercial use, several paid editions are available, and offer additional functionality. Applications which use MySQL databases include: TYPO3, MODx, Joomla, WordPress, phpBB, MyBB, Drupal and other software. MySQL is also used

in many high-profile, large-scale websites, including Wikipedia, Google (though not for searches), Facebook, Twitter, Flickr and YouTube.

## **2.8 FEASIBILITY STUDY**

The feasibility of the project is analyzed in this phase and business proposal is put forth with a very general plan for the project and some cost estimates. During system analysis the feasibility study of the proposed system is to be carried out. This is to ensure that the proposed system is not a burden to the company. For feasibility analysis, some understanding of the major requirements for the system is essential.

The feasibility study investigates the problem and the information needs of the stakeholders. It seeks to determine the resources required to provide an information systems solution, the cost and benefits of such a solution, and the feasibility of such a solution.

The goal of the feasibility study is to consider alternative information systems solutions, evaluate their feasibility, and propose the alternative most suitable to the organization. The feasibility of a proposed solution is evaluated in terms of its components.

## **2.9 ECONOMICAL FEASIBILITY**

This study is carried out to check the economic impact that the system will have on the organization. The amount of fund that the company can pour into the research and development of the system is limited. The expenditures must be justified. Thus the developed system is well within the budget and this was achieved because most of the technologies used are freely available. Only the customized products had to be purchased.

## **2.10 TECHNICAL FEASIBILITY**

This study is carried out to check the technical feasibility, that is, the technical requirements of the system. Any system developed must not have a high demand on the available technical resources. This will lead to high demands on the available technical resources. This will lead to high demands being placed on the client. The developed system must have a modest requirement, as only minimal or null changes are required for implementing this system.

## **2.11 SOCIAL FEASIBILITY**

The aspect of study is to check the level of acceptance of the system by the user. This includes the process of training the user to use the system efficiently. The user must not feel threatened by the system, instead must accept it as a necessity.

## **2.12 REQUIREMENT ANALYSIS**

Requirement analysis, also called requirement engineering, is the process of determining user expectations for a new modified product. It encompasses the tasks that determine the need for analysing, documenting, validating and managing software or system requirements. The requirements should be documentable, actionable, measurable, testable and traceable related to identified business needs or opportunities and define to a level of detail, sufficient for system design.

## **2.13 FUNCTIONAL REQUIREMENTS**

It is a technical specification requirement for the software products. It is the first step in the requirement analysis process which lists the requirements of particular software systems including functional, performance and security requirements. The function of the system depends mainly on the quality hardware used to run the software with given functionality.

It specifies how easy the system must be use. It is easy to ask queries in any format which is short or long, porter stemming algorithm stimulates the desired response for user.

It refers to a program that performs well not only under ordinary conditions but also under unusual conditions. It is the ability of the user to cope with errors for irrelevant queries during execution.

The state of providing protected access to resource is security. The system provides good security and unauthorized users cannot access the system there by providing high security.

It is the probability of how often the software fails. The measurement is often expressed in MTBF (Mean Time Between Failures). The requirement is needed in order to ensure that the processes work correctly and completely without being

aborted. It can handle any load and survive and survive and even capable of working around any failure.

It is supported by version above all web browsers. Using any web servers like localhost makes the system real-time experience.

The flexibility of the project is provided in such a way that is has the ability to run on different environments being executed by different users.

Safety is a measure taken to prevent trouble. Every query is processed in a secured manner without letting others to know one's personal information.

## **2.14 NON- FUNCTIONAL REQUIREMENTS**

### **2.14.1 Portability**

It is the usability of the same software in different environments. The project can be run in any operating system.

### **2.14.2 Performance**

These requirements determine the resources required, time interval, throughput and everything that deals with the performance of the system.

### **2.14.3 Accuracy**

The result of the requesting query is very accurate and high speed of retrieving information. The degree of security provided by the system is high and effective.

## **CHAPTER-3**

### **SYSTEM IMPLEMENTATION**

#### **3.1 IMPEAMNTATION**

- Login Module
- Registration Module
- Creation Storage and Instance
- Find collusion Module
- Find Third-Party Module

#### **3.2 LOGIN MODULE**

This is the first activity, User needs to provide a correct contact number and a password, which user enters while registering, in order to login into the app. If information provided by the user matches with the data in the database table then user successfully login into the app else message of login failed is displayed and user need to re-enter correct information. A link to the register activity is also provided for registration of new users.

#### **3.3 REGISTRATION MODULE**

A new user who wants to access the app needs to register first before login. By clicking on register button in login activity, the register activity gets open. A new user registers by entering full name, password and contact number. A user needs to enter password again in confirm password textbox for confirmation. When user enters the information in all textboxes, on the click of register button, the data is transferred to database and user is directed to login activity again. Registered user then needs to login in order to access the app. Validations are applied on all the textboxes for proper functioning of the app. Like information in each textbox is must that is each textbox, either it is of name, contact, password or confirm password, will not be empty while registering. If any such textbox is empty app will give message of information is must in each textbox. Also data in password and confirm password fields must match for successful registration. Another validation is contact number must be valid one that is of 10 digits. If any such validation is violated then registration will be unsuccessful and then user needs to register again. Message that app will display when one of the field

is empty. If all such information is correct user will be directed to login activity for login into the app.

### **3.4 CREATION STORAGE AND INSTANCE**

The data owner has not control over the data after it is uploaded on cloud. In this module, the original data get encrypted into two different values. The data in each slice can be encrypted by using different cryptographic algorithm's and encryption key before storing them in the Cloud.

### **3.5 FIND COLLUSION MODULE**

In this Module, Receiver can find collusion occurring or not using calculating a distance.

### **3.6 FIND THIRD-PARTY MODULE**

In this Module, receiver can also find third-parties. Third party refers to another company making software for the original vendors product.

### **3.7 UML DIAGRAM**

UML stands for Unified Modelling Language. UML is a standardized general-purpose modelling language in the field of object-oriented software engineering. The standard is managed, and was created by, the Object Management Group.

The goal is for UML to become a common language for creating models of object oriented computer software. In its current form UML is comprised of two major components: a Meta-model and a notation. In the future, some form of method or process may also be added to; or associated with, UML.

The Unified Modelling Language is a standard language for specifying, Visualization, Constructing and documenting the artefacts of software system, as well as for business modelling and other non-software systems.

The UML represents a collection of best engineering practices that have proven successful in the modelling of large and complex systems.

The UML is a very important part of developing objects oriented software and the software development process. The UML uses mostly graphical notations to express the design of software projects.

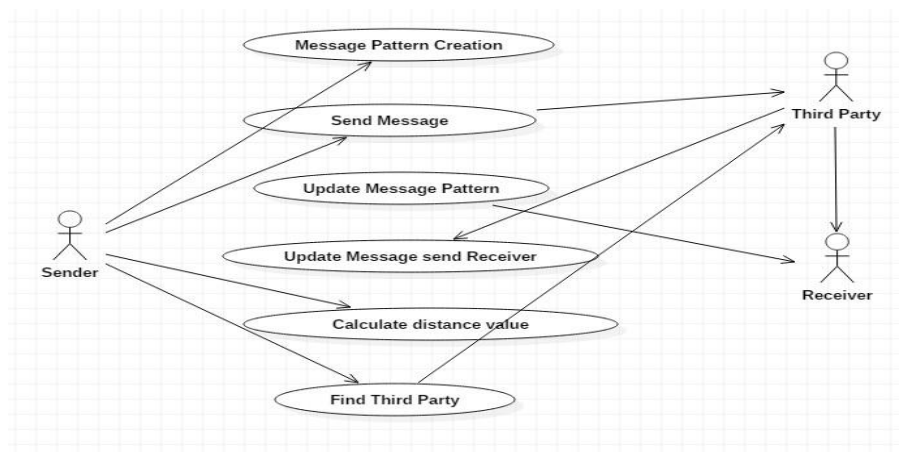
### **3.8 GOALS:**

The Primary goals in the design of the UML are as follows:

1. Provide users a ready-to-use, expressive visual modelling Language so that they can develop and exchange meaningful models.
2. Provide extendibility and specialization mechanisms to extend the core concepts.
3. Be independent of particular programming languages and development process.
4. Provide a formal basis for understanding the modelling language.
5. Encourage the growth of OO tools market.
6. Support higher level development concepts such as collaborations, frameworks, patterns and components.
7. Integrate best practices.

### 3.9 USE CASE DIAGRAM

A use case diagram in the Unified Modelling Language (UML) is a type of behavioural diagram defined by and created from a Use-case analysis. Its purpose is to present a graphical overview of the functionality provided by a system in terms of actors, their goals (represented as use cases), and any dependencies between those use cases.

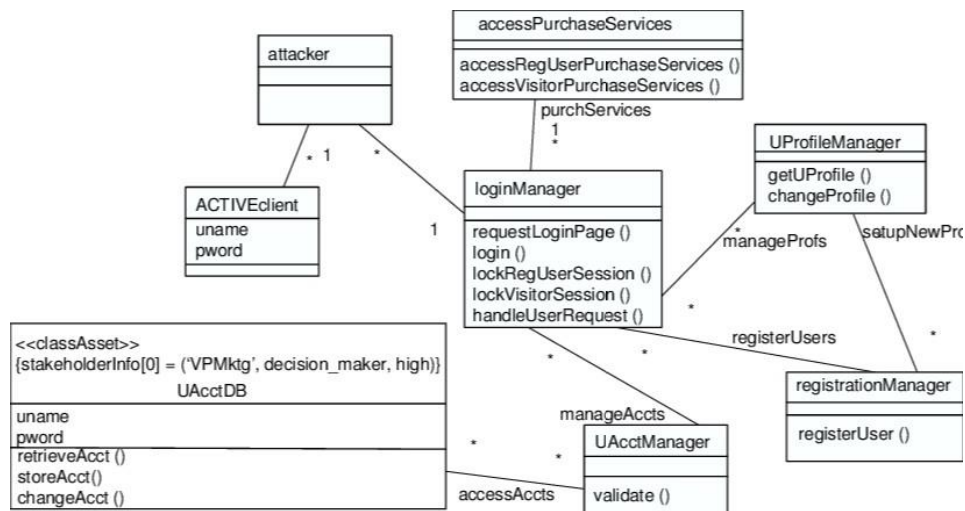


**FIG 3.1 USER CASE DIAGRAM**

### 3.10 CLASS DIAGRAM

In software engineering, a class diagram in the Unified Modeling Language (UML) is a type of static structure diagram that describes the structure of a system by

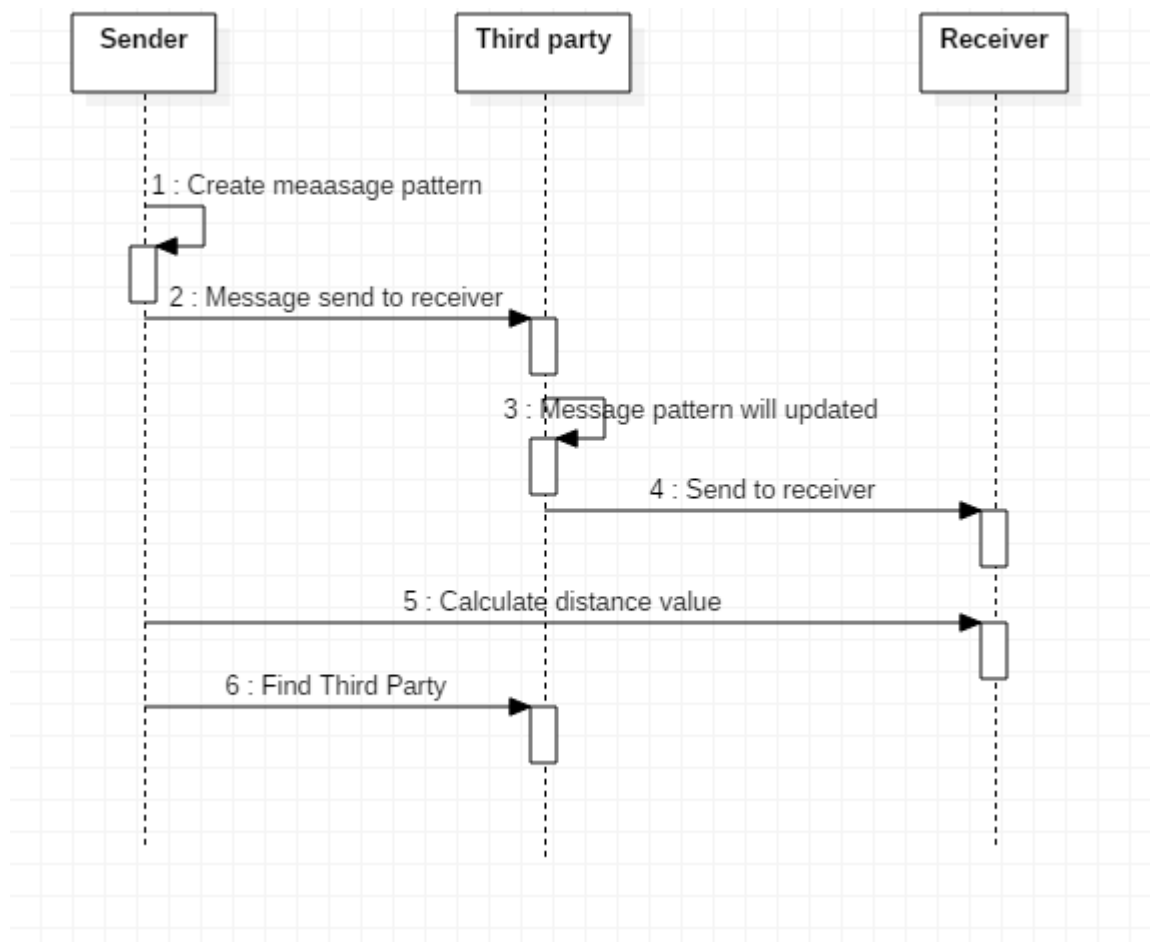
showing the system's classes, their attributes, operations (or methods), and the relationships among the classes. It explains which class contains information



**FIG 3.2 10 CLASS DIAGRAM**

### 3.11 SEQUENCE DIAGRAM

A sequence diagram in Unified Modeling Language (UML) is a kind of interaction diagram that shows how processes operate with one another and in what order. It is a construct of a Message Sequence Chart. Sequence diagrams are sometimes called event diagrams, event scenarios, and timing diagrams.



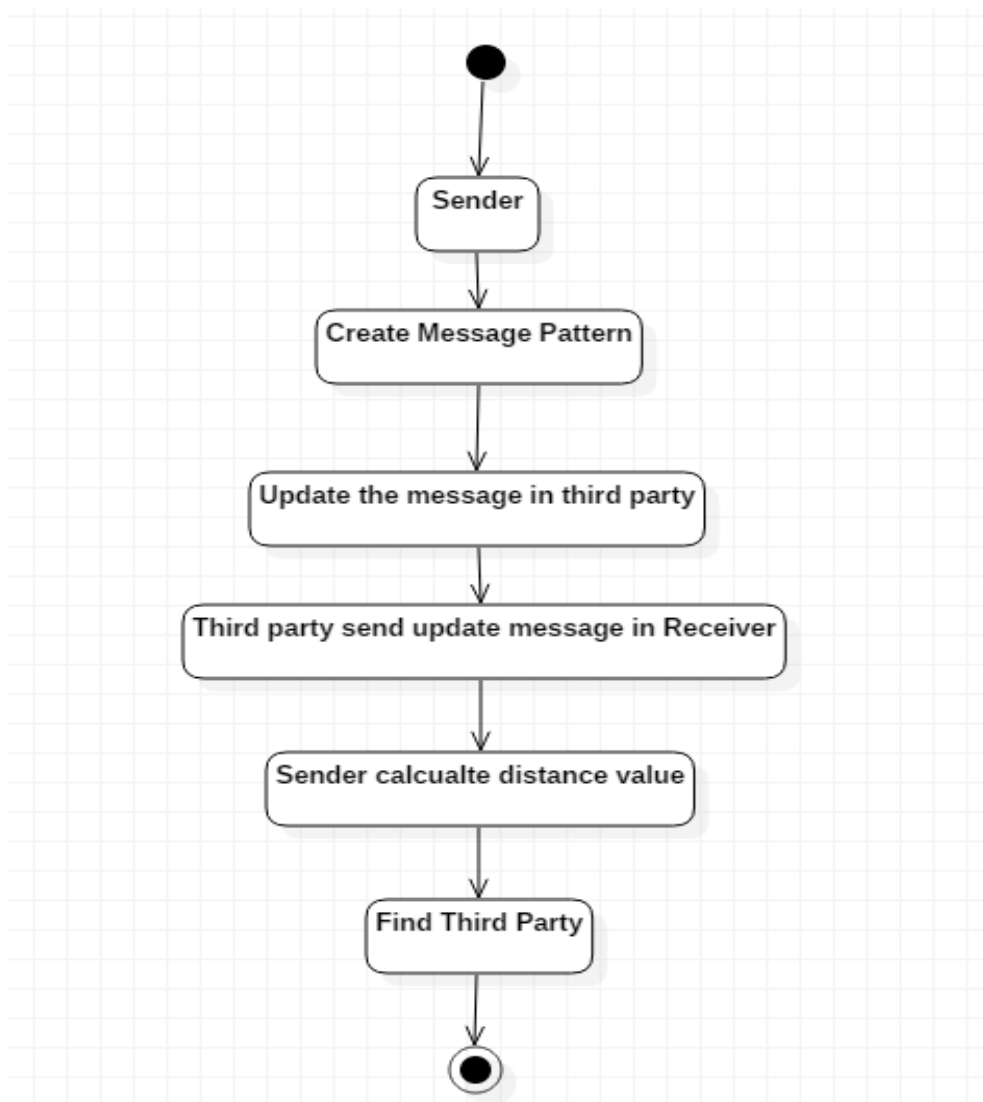
**FIG 3.3 11 SEQUENCE DIAGRAM**

## CHAPTER-4

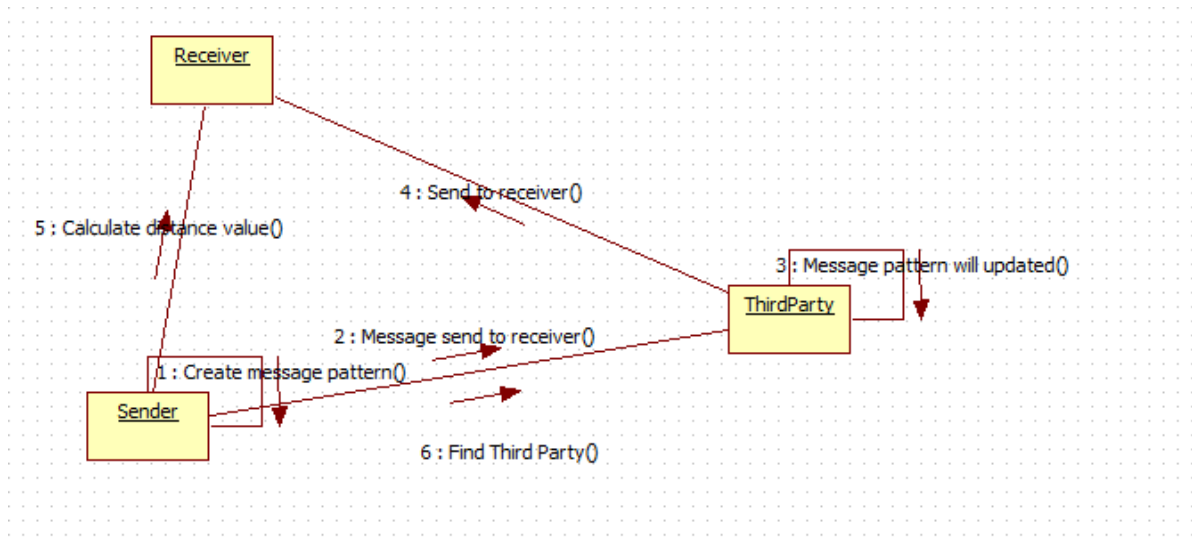
### RESULTS AND DISCUSSIONS

#### ACTIVITY DIAGRAM

Activity diagrams are graphical representations of workflows of stepwise activities and actions with support for choice, iteration and concurrency. In the Unified Modeling Language, activity diagrams can be used to describe the business and operational step-by-step workflows of components in a system. An activity diagram shows the overall flow of control.



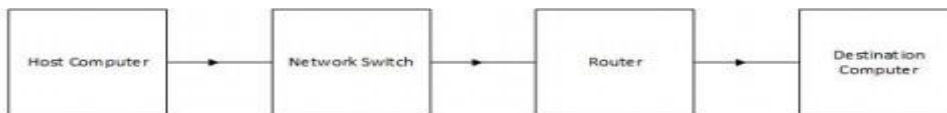
#### COLLABORATION DIAGRAM



## DATA FLOW DIAGRAM

A Data Flow Diagram (DFD) is a graphical representation of the “flow” of data through an information system, modeling its process aspects. Often they are a preliminary step used to create an overview of the system which can later be elaborated. DFD’s can also be used for the visualization of data processing (structured design).

### LEVEL-1



### LEVEL-2



### LEVEL-3



## 4.1 SYSTEM DESIGN AND TESTING PLAN

#### **4.1.1 INPUT DESIGN**

The input design is the link between the information system and the user. It comprises the developing specification and procedures for data preparation and those steps are necessary to put transaction data in to a usable form for processing can be achieved by inspecting the computer to read data from a written or printed document or it can occur by having people keying the data directly into the system. The design of input focuses on controlling the amount of input required, controlling the errors, avoiding delay, avoiding extra steps and keeping the process simple. The input is designed in such a way so that it provides security and ease of use with retaining the privacy. Input Design considered the following things:

- What data should be given as input?
- How the data should be arranged or coded?
- The dialog to guide the operating personnel in providing input.
- Methods for preparing input validations and steps to follow when error occur.

#### **4.1.2 OUTPUT DESIGN**

A quality output is one, which meets the requirements of the end user and presents the information clearly. In any system results of processing are communicated to the users and to other system through outputs. In output design it is determined how the information is to be displaced for immediate need and also the hard copy output. It is the most important and direct source information to the user. Efficient and intelligent output design improves the system's relationship to help user decision-making.

The output form of an information system should accomplish one or more of the following objectives.

- Convey information about past activities, current status or projections of the
- Future.
- Signal important events, opportunities, problems, or warnings.
- Trigger an action.
- Confirm an action.

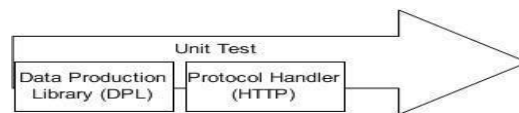
#### **4.2 TESTING PROCESS**

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. Each test type addresses a specific testing requirement.

#### **4.2.1 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.



**Fig 4.1 Unit Testing**

#### **4.2.2 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.

#### **4.2.3 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.

Functional testing is centered on the following items:

**Valid Input** is used to identified classes of valid input must be accepted.

**Invalid Input** is used to identified classes of invalid input must be rejected.

**Functions** is used to identified functions must be exercised.

**Output** is used to identify classes of application outputs.

**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.

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.

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 its purpose. It is used to test areas that cannot be reached from a black box level.

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 requirements 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.

## **4.3 TEST STRATEGY AND APPROACH**

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

### **4.3.1 TEST OBJECTIVES**

1. All field entries must work properly.
2. Pages must be activated from the identified link.

3. The entry screen, messages and responses must not be delayed.
4. Features to be tested
5. Verify that the entries are of the correct format
6. No duplicate entries should be allowed

#### **4.4 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.

##### **4.4.1 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.

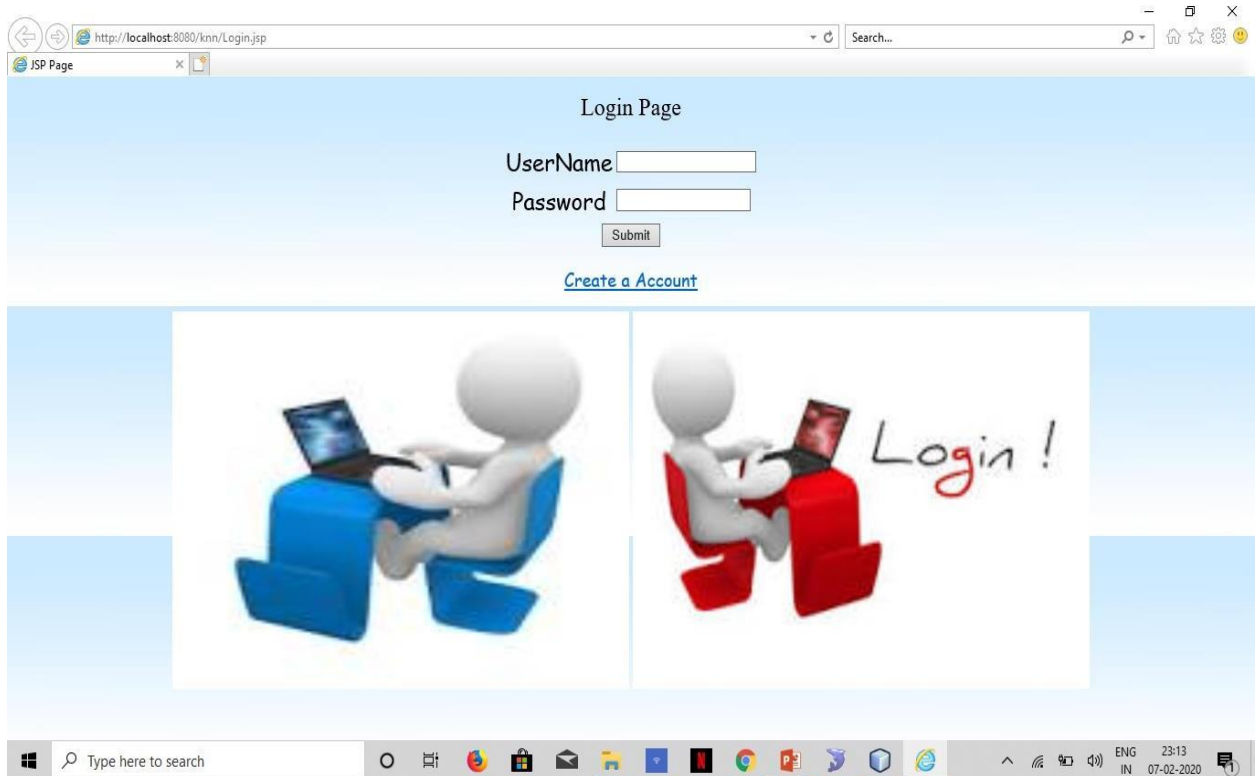
##### **4.4.2 ALPHA TESTING**

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 pre loaders work.

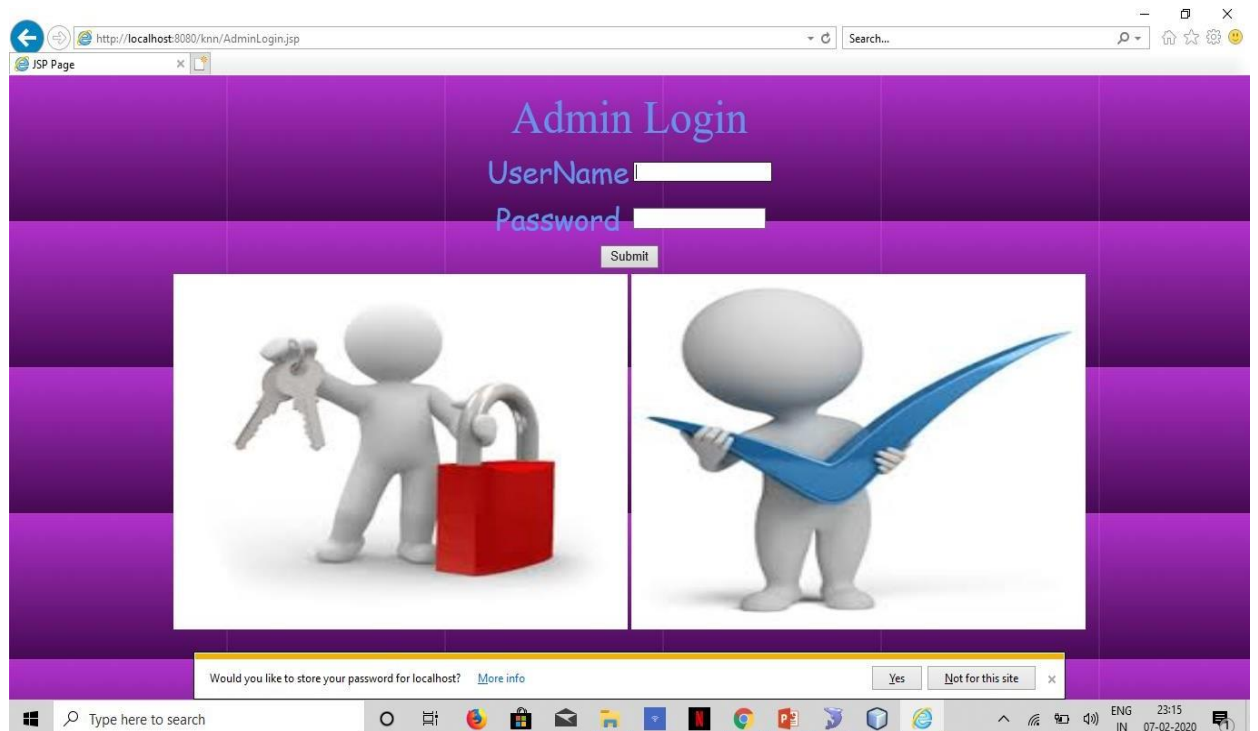
##### **4.4.3 BETA TESTING**

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 are now distributed to curriculum specialists and teachers to give the program a "real world" test

#### **OUTPUT AND RESULT SCREENS**



**FIG 4.2 Login Page**



**FIG 4.3 Admin Login Page**

## **CHAPTER-5**

### **CONCLUSION AND FUTURE WORK**

#### **CONCLUSION**

Through the above summary, due to the problems about the collusion attacks that are widespread in the secure outsourcing of sequence comparison algorithms, this paper will introduce the trusted authority to authenticate user those who have the access to the data on cloud. SHA algorithm is used by the trusted authority to generate the key and that key will get share to user as well as the owner. The trusted authority module receives encrypted file using AES Algorithm from the data owner and computes hash value using MD-5 algorithm. It stores key in its database which will be used during the dynamic operations and to determine the cheating party in the system. Trusted authority send file to CSP module to store on cloud. The resulting key sets are shown to have a number of desirable properties that ensure the confidentiality of communication sessions against collusion attacks by other network nodes.

#### **FUTURE WORK**

It is somewhat hard to extend the work in our paper to certain applications with multi-data source. Firstly, two character sequences from different sources should be encrypted respectively with different keys. Secondly, three cost matrices should be encrypted together after being constructed by the negotiation between both sides. The security target is to complete sequence comparison on a single cloud server in the way of privacy preservation and to ensure that the string typed data of the end user on any side will not be arbitrarily stolen by the other user or the CSP.

## REFERENCES

- [1] Y.Feng,H.Ma,andX.Chen,“Efficient and verifiable outsourcing scheme of sequence comparisons,” *Intell. Autom. Soft Comput.*, vol. 21, no. 1, pp. 51–63, Jan. 2015.
- [2] M. J. Atallah and J. Li, “Secure outsourcing of sequence comparisons,” in *Proc. Int. Workshop Privacy Enhancing Technol. (PET)*, Toronto, ON, Canada, 2004, pp. 63–78.
- [3] M. J. Atallah, F. Kerschbaum, and W. Du, “Secure and private sequence comparisons,” in *Proc. ACM Workshop Privacy Electron. Soc. (WPES)*, Washington, DC, USA, 2003, pp. 39–44.
- [4] D. Szajda, M. Pohl, J. Owen, and B. Lawson, “Toward a practical data privacy scheme for a distributed implementation of the Smith-Waterman genome sequence comparison algorithm,” in *Proc. Netw. Distrib. Syst. Secur. Symp. (NDSS)*, San Diego, CA, USA, 2006, pp. 253–265.
- [5] X. Chen, J. Li, J. Ma, Q. Tang, and W. Lou, “New algorithms for secure outsourcing of modular exponentiations,” *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 9, pp. 2386–2396, Sep. 2014.
- [6] Dhage, Sudhir N., and B. B. Meshram. "Intrusion detection system in cloud computing environment." *International Journal of Cloud Computing* 1.2-3 (2012): 261-282.
- [7] Dhage, S. N., & Meshram, B. B. (2012). Intrusion detection system in cloud computing environment. *International Journal of Cloud Computing*, 1(2-3), 261-282.

- [8] Dhage, Sudhir N., and B. B. Meshram. "Intrusion detection system in cloud computing environment." *International Journal of Cloud Computing* 1, no. 2-3 (2012): 261-282.
- [9] Dhage, S.N. and Meshram, B.B., 2012. Intrusion detection system in cloud computing environment. *International Journal of Cloud Computing*, 1(2-3), pp.261-282.
- [10] Dhage SN, Meshram BB. Intrusion detection system in cloud computing environment. *International Journal of Cloud Computing*. 2012 Jan 1;1(2-3):261-82.
- [11] Shelke, M.P.K., Sontakke, M.S. and Gawande, A.D., 2012. Intrusion detection system for cloud computing. *International Journal of Scientific & Technology Research*, 1(4), pp.67-71.
- [12] Shelke, Ms Parag K., Ms Sneha Sontakke, and A. D. Gawande. "Intrusion detection system for cloud computing." *International Journal of Scientific & Technology Research* 1, no. 4 (2012): 67-71.
- [13] Shelke, M.P.K., Sontakke, M.S. and Gawande, A.D., 2012. Intrusion detection system for cloud computing. *International Journal of Scientific & Technology Research*, 1(4), pp.67-71.
- [14] Shelke MP, Sontakke MS, Gawande AD. Intrusion detection system for cloud computing. *International Journal of Scientific & Technology Research*. 2012 May 4;1(4):67-71.
- [15] Modi, Chirag N., et al. "Bayesian Classifier and Snort based network intrusion detection system in cloud computing." *2012 Third International Conference on Computing, Communication and Networking Technologies (ICCCNT'12)*. IEEE, 2012.

[16] Modi, C. N., Patel, D. R., Patel, A., & Muttukrishnan, R. (2012, July). Bayesian Classifier and Snort based network intrusion detection system in cloud computing. In *2012 Third International Conference on Computing, Communication and Networking Technologies (ICCCNT'12)* (pp. 1-7). IEEE.

[17] Modi, Chirag N., Dhiren R. Patel, Avi Patel, and Rajarajan Muttukrishnan. "Bayesian Classifier and Snort based network intrusion detection system in cloud computing." In *2012 Third International Conference on Computing, Communication and Networking Technologies (ICCCNT'12)*, pp. 1-7. IEEE, 2012.

# INTRUDER (HYBRID) DETECTION SYSTEM FOR CLOUD COMPUTING ENVIRONMENTS

M.UDAY KUMAR, T.CHAITANYA

Department of computer science and Engineering, Sathyabama Institute of science and Technology

Faculty of computing, Sathyabama institute of science and Technology

E-mail:[mailavaramudaykumar@gmail.com](mailto:mailavaramudaykumar@gmail.com)

**Abstract** -Cloud computing is the Technology where we can store the information somewhere using the Internet. We can upload our information into it. We can work in many computing environments, as it is serving well. Some intruders can steal the data from it. Virtualization helps us in forming many systems which help us in server building. The intrusion detection system is used to detect the intruders who are trying to manipulate the information in the cloud, which is a bad scenario. We are trying to develop an algorithm that helps us in finding the intruders in cloud computing environments. We should take care of security as the data is uttermost important, so the safety of it is also important. We have sections divided where each section would help us our research better understand it. Many technologies are used for protecting the data in these environments. It is very much great that protecting data in cloud areas is not an easy task. Many researchers are finding new algorithms to protect the data.

## I.INTRODUCTION

Cloud computing is the demanding technology where we can do all our computations in the cloud by avoiding the use of physical devices. It helps us a lot in storing the data and doing the computations online. The Internet is the key requirement for doing all the cloud operations. Virtualization helps us in sharing the single system into multiple systems we call them as virtual machines which helps us in computing online. These days everyone is using cloud because it provides great features to work on from uploading the data to doing all the computations. To secure this information we are coming up with algorithms like SHA, MD5, AES these algorithms are very much useful in protecting the data in the area. We used these algorithms for safety of data because we have SHA. For suppose it is a very powerful algorithm which helps us keep the data unmodified it has patterns to secure the data this is how we protect the data in cloud environments. They are the family of cryptography

hash functions it is released by NIST. National institute of standards and Technology.

## II.RELATED WORKS

Intrusion detection system or preventing of intruders from the cloud computing environments is a difficult task everyone has contributed their own contribution in order to protect the cloud computing environments. some of them are approached many hashing algorithms to protect the data in the environments we referred all their research papers so that we will get an idea about the approaches they followed to detect the intruder and the way they approached to detect the intruders in the cloud computing environments some used alarm management techniques and also machine learning techniques for detecting the intrusion.

Ms Parag Shelke et al [2] approached cloud security which is intrusion detection which is researched by this team about the cloud intrusion

detection they did research on the implementing the models which handles the large flow of data packets using this technology they tried to detect the intrusion system their system also handles the data even the flow of data is large as the implementation using behaviour analysis to detect intrusions in the cloud environments this was their research on the cloud security where to find the intruder so that we can secure the cloud.

Ajith Abraham et al [3] developed a evolutionary design for intrusion detection program he used Genetic programming techniques helps us in detecting the intruders who are trying to modify the data in the cloud so that the data or information stored in it will be protected in their approach they have used Linear genetic programming, multi expression Programming and gene expression programming. Used to analyse the intrusion detection prevention system they thought using this approach which is lightweight and easy to use and which is better than approaching machine learning models used for detection programs.

### EXISTING SYSTEM

The Cloud data sharing system has evolved so much where we can store a large amount of data in the system where it is not physically stored, but it feels like it is stored in our real system. The main important thing in cloud environments is securing the cloud data. Researchers are trying to secure the cloud data by implementing many algorithms and implementations for only protecting the data in the cloud it is a challenging process all the existing systems include the intrusion detection system using anomaly detection, network intrusion detection systems host-based intrusion detection system and signature-based detection system all these systems secure the cloud in different ways by taking the different inputs for the better security of the cloud as the existing systems uses some downgraded implementations which are not sufficient for the storing the cloud in a large size, so the existing systems are protecting the resources only to the minimal content which is going to store in the cloud. the internet is the key thing for the running of the cloud sharing systems.

### III. PROPOSED SYSTEM

We propose a secure data sharing scheme, which can achieve secure key distribution and data sharing for dynamic groups. We provide a secure way for key distribution without any secure communication channels. The users can securely obtain their private keys from the group manager without any Certificate. Authorities due to the

verification of the public key of the user. . We provide security analysis to prove the security of our scheme. . We provide security analysis to prove the security of our scheme. We propose a secure data sharing scheme which can be protected from collusion attacks. Our paper can get the fine-grained control of data with the help of the user list of the group user in the group can use the source in the cloud and revoked users cannot get the access to the cloud again after they revoked.. Our scheme can achieve secure user revocation with the help of polynomial function, this scheme supports dynamic groups when a new user joins the group the private keys of the other users need not to be generated again or updated.

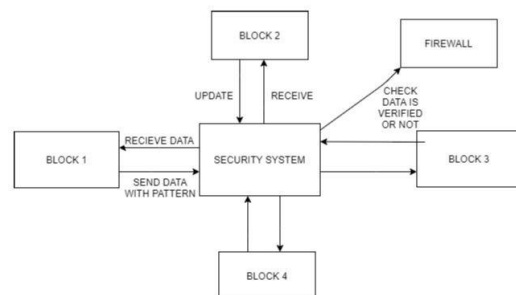


Fig 1 Architecture Diagram

### MODULES

#### A.LOGIN MODULE

This is the first activity module in our project where we use our credentials to login into the system . We have a user account and Admin account separately because Admin has more privileges than the user as Admin has to create the account for every user when creating an account has been assigned to some group. if the details provided by the user or admin did not match it will show error where we have to validate the details correctly in order to use the system.

#### B.REGISTRATION MODULE

A new user who wants to use the application needs to be registered first before he uses all the features of the application. In order to use the application a user must create an account with the help of Admin. the user has to set a unique strong password which contains all the alphabets and some special characters which helps the password be strong so that it will be hard for the intruders to crack the password. there will be some validation

for the successful registration of the user. This will help

### C. CREATING INSTANCE

In this type of data securing the data gets secured first by encrypting the data before it gets stored in the cloud so that we can know that the data in the cloud is modified or not as the data has no control over the internet because the owner itself can't say that whether the data in the cloud systems are secured or not. In this module the data gets protected before it gets stored in the cloud environment it is encrypted using the cryptographic algorithms.

### D. FIND COLLUSION MODULE

This module will help in finding the collusion which is intruder who is trying to modify the data which is present in the cloud platform.

## IV RESULTS AND DISCUSSION

By this research paper we are here by to discuss the output of our project which helps in protecting the cloud environments, here the data which is going to store in cloud environments will be undergone to these methods like AES, MD5, SHA so that the file will be set some pattern whenever someone is trying to steal the information or updating of the information the pattern gets changed and we will capture the identity of the intruder who tried to steal or modify our information. We use the key for the group so that whenever we upload the file or send the file to receiver in between we may have intruder who tries to steal our data so we should take care of the data and finding the intruder is much needful for the protection of the data this method of finding the intruder in the cloud computing environments will help in finding the intruder for the protection of data.

## V CONCLUSION

The problems in the cloud environments mostly are security issues which are very problematic for the people who are storing the data in the cloud environments which they thought like safe but protecting the data in the cloud environments is a challenging task we have three Algorithms namely SHA, AES, MD5. which helps in protecting the data by encrypting the data which are going to store in the cloud which helps us protecting our data which is being stored in the cloud

environments there is key generation using the Secure hashing Algorithm

Through the above summary, due to the problems about the collusion attacks that are widespread in the secure outsourcing of sequence comparison algorithms, this paper will introduce the trusted authority to authenticate users who have the access to the data on cloud. SHA algorithm is used by the trusted authority to generate the key and that key will get shared to the user as well as the owner. The trusted authority module receives encrypted files using AES Algorithm from the data owner and computes hash value using MD-5 algorithm. It stores key in its database which will be used during the dynamic operations and to determine the cheating party in the system. Trusted authority sends file to CSP module to store on cloud. The resulting key sets are shown to have a number of desirable properties that ensure the confidentiality of communication sessions against collusion attacks by other network nodes.

## VI FUTURE WORK

It is very much difficult to extend our work on intrusion detection system for cloud computing we can implement Machine learning models like KNN, and some unsupervised Machine Learning Algorithms which helps us in securing the data by giving the training to model by giving the possibilities of the occurrences of the intruders so that it becomes faster to protect the data and using machine learning the cloud security would help us more securable and also in addition to that deep learning might help us in securing the data which is utter most important in the cloud data storage systems.

## REFERENCES

- [1] Y. Feng, H. Ma, and X. Chen, "Efficient and verifiable outsourcing scheme of sequence comparisons," *Intell. Autom. Soft Comput.*, vol. 21, no. 1, pp. 51–63, Jan. 2015.
- [2] M. J. Atallah and J. Li, "Secure outsourcing of sequence comparisons," in *Proc. Int. Workshop Privacy Enhancing Technol. (PET)*, Toronto, ON, Canada, 2004, pp. 63–78.
- [3] M. J. Atallah, F. Kerschbaum, and W. Du, "Secure and private sequence comparisons," in *Proc. ACM Workshop Privacy Electron. Soc. (WPES)*, Washington, DC, USA, 2003, pp. 39–44.

- [4] D. Szajda, M. Pohl, J. Owen, and B. Lawson, "Toward a practical data privacy scheme for a distributed implementation of the Smith-Waterman genome sequence comparison algorithm," in Proc. Netw. Distrib. Syst. Secur. Symp. (NDSS), San Diego, CA, USA, 2006, pp. 253–265.
- [5] X. Chen, J. Li, J. Ma, Q. Tang, and W. Lou, "New algorithms for secure outsourcing of modular exponentiations," IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 9, pp. 2386–2396, Sep. 2014.
- [6] R. Akimana, O. Markowitch, and Y. Roggeman, "Secure outsourcing of DNA sequences comparisons in a Grid environment," WSEAS Trans. Comput. Res., vol. 2, no. 2, pp. 262–269, Feb. 2007.
- [7] M. Blanton, M. J. Atallah, K. B. Frikken, and Q. Malluhi, "Secure and efficient outsourcing of sequence comparisons," in Proc. Eur. Symp. Res. Comput. Secur. (ESORICS), Pisa, Italy, 2012, pp. 505–522.
- [8] Y. Feng, H. Ma, X. Chen, and H. Zhu, "Secure and verifiable outsourcing of sequence comparisons," in Proc. Int. Conf. Inf. Commun. Technol. (ICT-EurAsia), Yogyakarta, Indonesia, 2013, pp. 243–252.
- [9] S. Salinas, X. Chen, J. Li, and P. Li, "A tutorial on secure outsourcing of large-scale computations for big data," IEEE Access, vol. 4, pp. 1406–1416, Apr. 2016.
- [10] X. Chen, J. Li, J. Weng, J. Ma, and W. Lou, "Verifiable computation over large database with incremental updates," IEEE Trans. Comput., vol. 65, no. 10, pp. 3184–3195, Oct. 2016.



# 04

*by* 04 04

---

**Submission date:** 29-Apr-2020 08:51AM (UTC-0400)

**Submission ID:** 1311071741

**File name:** myprojectPaper\_1.pdf (178.54K)

**Word count:** 2178

**Character count:** 10858

# INTRUDER (HYBRID) DETECTION SYSTEM FOR CLOUD COMPUTING ENVIRONMENTS

M.UDAY KUMAR, T.CHAITANYA

<sup>9</sup> Department of computer science and Engineering, <sup>8</sup> Sathyabama Institute of science and Technology

Faculty of computing, Sathyabama institute of science and Technology

E-mail: <sup>9</sup> mailavaramudaykumar@gmail.com

**Abstract** -Cloud computing is the Technology where we can store the information somewhere using the Internet. We can upload our information into it. We can work in many computing environments, as it is serving well. Some intruders can steal <sup>14</sup> data from it. Virtualization helps us in forming many systems which help us in server building. The intrusion detection system is used to detect the intruders who are trying to manipulate the information in the cloud, which is a bad scenario. We are trying to develop an algorithm that helps us in finding the intruders in cloud computing environments. We should take care of security as the data is uttermost important, so the safety of it is also important. We have sections divided where each section would help us our research better understand it. Many technologies are used for protecting the data in these environments. It is very much great that protecting data in cloud areas is not an easy task. Many researchers are finding new algorithms to protect the data.

## I.INTRODUCTION

Cloud computing is the demanding technology where we can do all our computations in the cloud by avoiding the use of physical devices. It helps us a lot in storing the data and doing the computations online. The Internet is the key requirement for doing all the cloud operations. Virtualization helps us in sharing the single system into multiple systems we call them as virtual machines which helps us in computing online. These days everyone is using cloud because it provides great features to work on from uploading the data to doing all the computations. To secure this information we are coming up with algorithms like SHA, MD5, AES these algorithms are very much useful in protecting the data in the area. We used these algorithms for safety of data because we have SHA. For suppose it is a very powerful algorithm which helps us keep the data unmodified it has patterns to secure the data this is how we protect <sup>12</sup> the data in cloud environments. They are the family of cryptography

<sup>12</sup> hash functions it is released by NIST. National institute of standards and Technology.

## II.RELATED WORKS

Intrusion detection system or preventing of intruders from the cloud computing environments is a difficult task everyone has contributed their own contribution in order to protect the cloud computing environments. some of them are approached many hashing algorithms to protect the data in the environments we referred all their research papers so that we will get an idea about the approaches they followed to detect the intruder and the way they approached to detect the intruders in the cloud computing environments some used alarm management techniques and also machine learning techniques for detecting the intrusion.

Ms Parag Shelke et al [2] approached cloud security which is intrusion detection which is researched by this team about the cloud intrusion

detection they did research on the implementing the models which handles the large flow of data packets using this technology they tried to detect the intrusion system their system also handles the data even the flow of data is large as the implementation using behaviour analysis to detect intrusions in the cloud environments this was their research on the cloud security where to find the intruder so that we can secure the cloud.

Ajith Abraham et al [3] developed a evolutionary design for intrusion detection program he used Genetic programming techniques helps us in detecting the intruders who are trying to modify the data in the cloud so that the data or information stored in it can be protected in their approach they have used Linear genetic programming, multi expression Programming and gene expression programming. Used to analyse the intrusion detection prevention system they thought using this approach which is lightweight and easy to use and which is better than approaching machine learning models used for detection programs.

### EXISTING SYSTEM

The Cloud data sharing system has evolved so much where we can store a large amount of data in the system where it is not physically stored, but it feels like it is stored in our real system. The main important thing in cloud environments is securing the cloud data. Researchers are trying to secure the cloud data by implementing many algorithms and implementations for only protecting the data in the cloud it is a challenging process all the existing systems include the intrusion detection system using anomaly detection, network intrusion detection systems host-based intrusion detection system and signature-based detection system all these systems secure the cloud in different ways by taking the different inputs for the better security of the cloud as the existing systems uses some downgraded implementations which are not sufficient for the storing the cloud in a large size, so the existing systems are protecting the resources only to the minimal content which is going to store in the cloud. the internet is the key thing for the running of the cloud sharing systems.

### III.PROPOSED SYSTEM

We propose a secure data sharing scheme, which can achieve secure key distribution and data sharing for dynamic groups. We provide a secure way for key distribution without any secure communication channels. The users can securely obtain their private keys from the group manager without any Certificate. Authorities due to the

verification of the public key of the user. We provide security analysis to prove the security of our scheme. We provide security analysis to prove the security of our scheme. We propose a secure data sharing scheme which can be protected from collusion attacks. Our paper can get the fine-grained control of data with the help of the user list of the group user in the group can use the source in the cloud and revoked users cannot get the access to the cloud again after they revoked.. Our scheme can achieve secure user revocation with the help of polynomial function. this scheme supports dynamic groups when a new user joins the group the private keys of the other users need not to be generated again or updated.

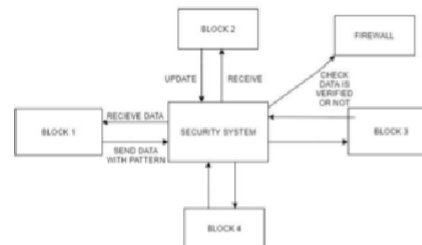


Fig 1 Architecture Diagram

### MODULES

#### A.LOGIN MODULE

This is the first activity module in our project where we use our credentials to login into the system. We have a user account and Admin account separately because Admin has more privileges than the user as Admin has to create the account for every user when creating an account has been assigned to some group. if the details provided by the user or admin did not match it will show error where we have to validate the details correctly in order to use the system.

#### B.REGISTRATION MODULE

A new user who wants to use the application needs to be registered first before he uses all the features of the application. In order to use the application a user must create an account with the help of Admin. the user has to set a unique strong password which contains all the alphabets and some special characters which helps the password be strong so that it will be hard for the intruders to crack the password. there will be some validation

for the successful registration of the user. This will help

### C. CREATING INSTANCE

In this type of data securing the data gets secured first by encrypting the data before it gets stored in the cloud so that we can know that the data in the cloud is modified or not as the data has no control over the internet because the owner itself cant say that whether the data in the cloud systems are secured or not. in this module the data gets protected before it gets stored in the cloud environment it is encrypted using the cryptographic algorithms.

### D.FIND COLLUSION MODULE

this module will help in finding the collusion which is intruder who is trying to modify the data which is present in the cloud platform.

## IV RESULTS AND DISCUSSION

By this research paper we are here by to discuss the output of our project which helps in protecting the cloud environments, here the data which is going to store in cloud environments will be undergone to these methods like AES, MD5, SHA so that the file will be set some pattern whenever someone is trying to steal the information or updating of the information the pattern gets changed and we will capture the identity of the intruder who tried to steal or modify our information. We use the key for the group so that whenever we upload the file or send the file to receiver in between we may have intruder who tries to steal our data so we should take care of the data and finding the intruder is much needful for the protection of the data this method of finding the intruder in the cloud computing environments will help in finding the intruder for the protection of data.

### V CONCLUSION

The problems in the cloud environments mostly are security issues which are very problematic for the people who are storing the data in the cloud environments which they thought like safe but protecting the data in the cloud environments is a challenging task we have three Algorithms namely SHA,AES,MD5. which helps in protecting the data by encrypting the data which are going to store in the cloud which helps us protecting our data which is being stored int the cloud

environments there is key generation using the Secure hashing Algorithm

5

Through the above summary, due to the problems about the collusion attacks that are widespread in the secure outsourcing of sequence comparison algorithms, this paper will introduce the trusted authority to authenticate users who have the access to the data on cloud. SHA algorithm is used by the trusted authority to generate the key and that key will get shared to the user as well as the owner. The trusted authority module receives encrypted files using AES Algorithm from the data owner and computes hash value using MD-5 algorithm. It stores key in its database which will be used during the dynamic operations and to determine the cheating party in the system. Trusted authority sends file to CSP module to store on cloud. The resulting key sets are shown to have a number of desirable properties that ensure the confidentiality of communication sessions against collusion attacks by other network nodes.

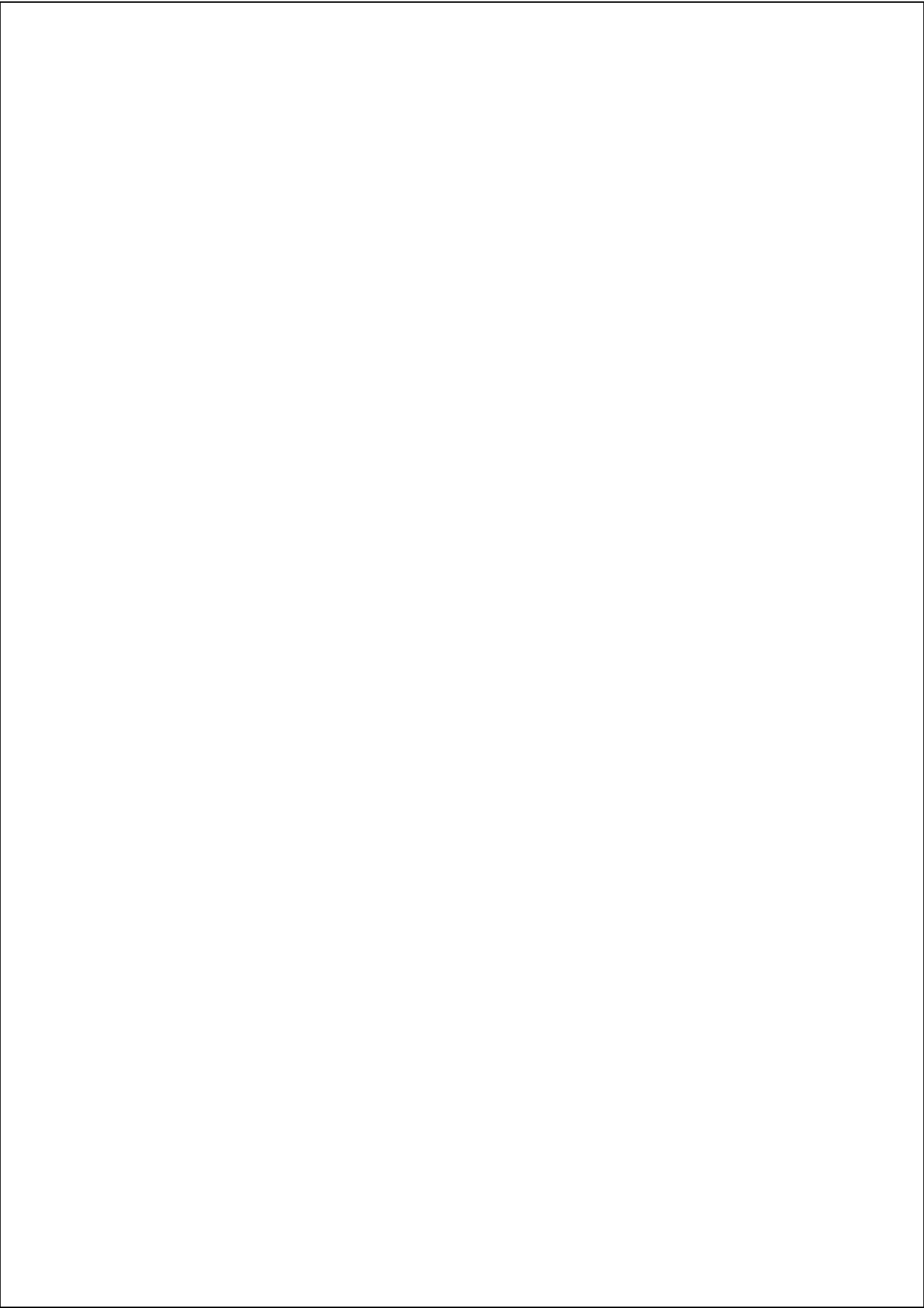
### VI FUTURE WORK

it is very much difficult to extend our work on intrusion detection system for cloud computing we can implement Machine learning models like KNN, and some unsupervised Machine Learning Algorithms which helps us in securing the data by giving the training to model by giving the possibilities of the occurrences of the intruders so that it becomes faster to protect the data and using machine learning the cloud security would help us more securable and also in addition to that deep learning might help us in securing the data which is utter most important in the cloud data storage systems.

### REFERENCES

- [1] Y.Feng,H.Ma,andX.Chen,“Efficient and verifiable outsourcing scheme of sequence comparisons,” *Intell. Autom. Soft Comput.*, vol. 21, no. 1, pp. 51–63, Jan. 2015.
- [2] M. J. Atallah and J. Li, “Secure outsourcing of sequence comparisons,” in *Proc. Int. Workshop Privacy Enhancing Technol. (PET)*, Toronto, ON, Canada, 2004, pp. 63–78.
- [3] M. J. Atallah, F. Kerschbaum, and W. Du, “Secure and private sequence comparisons,” in *Proc. ACM Workshop Privacy Electron. Soc. (WPES)*, Washington, DC, USA, 2003, pp. 39–44.

- [4] D. Szajda, M. Pohl, J. Owen, and B. Lawson, "Toward a practical data privacy scheme for a distributed implementation of the Smith-Waterman genome sequence comparison algorithm," in Proc. Netw. Distrib. Syst. Secur. Symp. (NDSS), San Diego, CA, USA, 2006, pp. 253–265.
- [5] X. Chen, J. Li, J. Ma, Q. Tang, and W. Lou, "New algorithms for secure outsourcing of modular exponentiations," IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 9, pp. 2386–2396, Sep. 2014.
- [6] R. Akimana, O. Markowitch, and Y. Roggeman, "Secure outsourcing of DNA sequences comparisons in a Grid environment," WSEAS Trans. Comput. Res., vol. 2, no. 2, pp. 262–269, Feb. 2007.
- [7] M. Blanton, M. J. Atallah, K. B. Frikken, and Q. Malluhi, "Secure and efficient outsourcing of sequence comparisons," in Proc. Eur. Symp. Res. Comput. Secur. (ESORICS), Pisa, Italy, 2012, pp. 505–522.
- [8] Y. Feng, H. Ma, X. Chen, and H. Zhu, "Secure and verifiable outsourcing of sequence comparisons," in Proc. Int. Conf. Inf. Commun. Technol. (ICT-EurAsia), Yogyakarta, Indonesia, 2013, pp. 243–252.
- [9] S. Salinas, X. Chen, J. Li, and P. Li, "A tutorial on secure outsourcing of large-scale computations for big data," IEEE Access, vol. 4, pp. 1406–1416, Apr. 2016.
- [10] X. Chen, J. Li, J. Weng, J. Ma, and W. Lou, "Verifiable computation over large database with incremental updates," IEEE Trans. Comput., vol. 65, no. 10, pp. 3184–3195, Oct. 2016.



## ORIGINALITY REPORT

**21%**

SIMILARITY INDEX

**16%**

INTERNET SOURCES

**14%**

PUBLICATIONS

**17%**

STUDENT PAPERS

## PRIMARY SOURCES

**1****ijrat.org**

Internet Source

**9%****2****www.ijmetmr.com**

Internet Source

**2%****3****ijesc.org**

Internet Source

**2%****4****ru1.cti.gr**

Internet Source

**1%****5****Xiaofei Wang, Yuqing Zhang. "E-SC: Collusion-Resistant Secure Outsourcing of Sequence Comparison Algorithm", IEEE Access, 2018**

Publication

**1%****6****Submitted to Texas A&M University - Corpus Christi**

Student Paper

**1%****7****Submitted to Study Group Australia**

Student Paper

**1%****8****www.sathyabama.ac.in**

Internet Source

**1%**

|    |                                                                                                                                                                             |     |
|----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| 9  | "International Conference on Intelligent Data Communication Technologies and Internet of Things (ICICI) 2018", Springer Science and Business Media LLC, 2019<br>Publication | 1%  |
| 10 | <a href="http://www.ukessays.com">www.ukessays.com</a><br>Internet Source                                                                                                   | 1%  |
| 11 | <a href="http://www.cs.ubbcluj.ro">www.cs.ubbcluj.ro</a><br>Internet Source                                                                                                 | 1%  |
| 12 | "Applied Cryptography and Network Security", Springer Science and Business Media LLC, 2012<br>Publication                                                                   | 1%  |
| 13 | "Advances in Network Security and Applications", Springer Science and Business Media LLC, 2011<br>Publication                                                               | <1% |
| 14 | Submitted to Middlesex University<br>Student Paper                                                                                                                          | <1% |

Exclude quotes      On  
Exclude bibliography      On

Exclude matches      Off