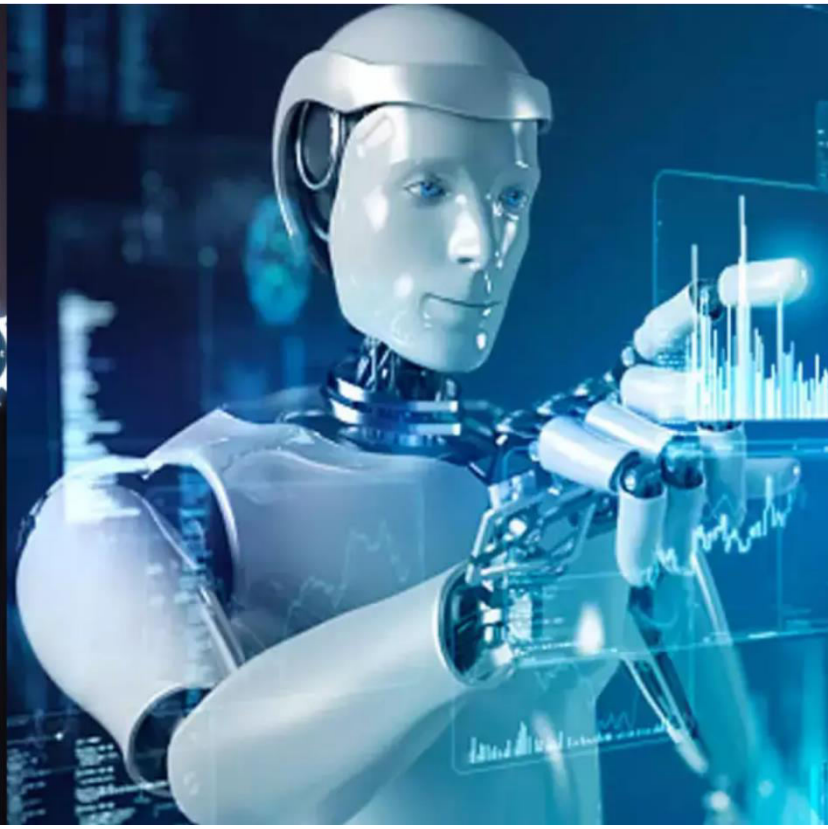
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 14, Issue 4, April 2025

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404167|

Designing Secure and Efficient Biometric-Based Secure Access Mechanism for Cloud Services

Dr. E.Srinvasa Raju, M.Vasudeva chary, Ch.VS Ganesh, B.Vikas, M.VishnuVardhan

Department of Computer Science & Engineering Malla Reddy University, Hyderabad

Maisammaguda, Kompally, Medchal, Hyderabad, India

ABSTRACT: The demand for remote data storage and computation services is increasing exponentially in our data-driven society; thus, the need for secure access to such data and services. In this paper, we design a new biometric-based authentication protocol to provide secure access to a remote(cloud) server. In the proposed approach, we consider biometric data of a user as a secret credential. We then derive a unique identity from the user's biometric data, which is further used to generate the user's private key. In addition, we propose an efficient approach to generate a session key between two communicating parties using two biometric templates for a secure message transmission. In other words, there is no need to store the user's private key anywhere and the session key is generated without sharing any prior information. A detailed Real-Or-Random model based formal security analysis, informal security analysis and also formal security verification using the broadly-accepted Automated Validation of Internet Security Protocols and Applications (AVISPA) tool reveal that the proposed approach can resist several known attacks against (passive/active) adversary. Finally, extensive experiments and a comparative study demonstrate the efficiency and utility of the proposed approach.

I. INTRODUCTION

In today's digital age, cloud services are crucial for storing and accessing data, but ensuring secure and efficient access has become a significant challenge. Traditional authentication methods like passwords and PINs are increasingly vulnerable to cyber threats. To address this, the project titled "Designing Secure & Efficient Biometric-Based Secure Access for Cloud Services" aims to develop a system that leverages biometric authentication for accessing cloud resources. The proposed system consists of four key modules: the Owner, Remote Server, Authentication Server, and Client. The Owner is responsible for managing the cloud environment, configuring the system, and assigning access permissions to users. The Remote Server hosts the cloud services and stores the data, processing requests from clients securely. The Authentication Server acts as the core component that verifies users' identities using biometric data, such as fingerprints or facial recognition, ensuring that only authorized users can access the cloud services. Finally, the Client represents the end-users who access the cloud resources by submitting their biometric information for authentication. Once authenticated, they are granted access to the cloud services. Together, these modules work in tandem to provide a secure, efficient, and user-friendly biometric authentication system, protected against unauthorized access.

II. PROBLEM STATEMENT

Jiang et al. [13] designed a password based user authentication scheme for wireless sensor networks (WSNs). This is a two-factor authentication scheme as it relies on both a smart card and some password. During the user registration process, an authorized user registers or re-registers with the trusted gateway node (GWN).

Althobaiti et al. [14] proposed a biometric-based user authentication mechanism for WSNs. However, their scheme is insecure against impersonation attacks and man-in-the- middle attacks [23]. Das [23] then proposed a new biometric-based user authentication approach.

Xue et al. [15] also designed a temporal-credential-based mutual authenticated key agreement mechanism for WSNs. In their scheme, the remote authorized users are permitted to access authorized sensor nodes in order to obtain information and also to send some important commands to the sensor nodes in WSN. In this scheme, the GWN issues temporal

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404167|

credentials to each user and sensor node deployed in WSN with the help of the password-based authentication mechanism.

III. PROPOSED SYSTEM

In the proposed approach, the system considers a fingerprint image of a user as a secret credential. From the fingerprint image, we generate a private key that is used to enroll the user's credential secretly in the database of an authentication server.

In the authentication phase, we capture a new biometric fingerprint image of the user, and subsequently generate the private key and encrypt the biometric data as a query. This queried biometric data is then transmitted to the authentication server for matching with the stored data. Once the user is authenticated successfully, he/she is ready to access his/her service from the desired server.

To obtain secure access to the service server, mutual authentication between the user and authentication server, and also between the user and service server have been proposed using a short-term session key. Using two fingerprint data, we present a fast and robust approach to generate the session key. In addition, a biometric based message authenticator is also generated for message authenticity purpose.

IV. LITERATURE SURVAY

Title: Designing Secure and Efficient Biometric-Based Access Mechanism for Cloud Services
Author: S. K. H. Islam, M. K. Khan, M. K. Islam and M. S. Obaidat
Description: This paper proposes a new biometric-based authentication protocol to provide secure access to a remote (cloud) server using fingerprint data. It claims to resist several known attacks and to be efficient and practical.
Title: Designing Secure and Efficient Biometric-Based Secure Access Mechanism for Cloud Services
Author: S. Gandi and V. Rajasekhar
Description: This paper also proposes a biometric-based authentication scheme using fingerprint images, but with a different approach to generate the user's private key and the session key. It also claims to be secure and efficient.

Title: Design of Secure Biometric-based Access Mechanism for Cloud Services
Author: A. Kaur, A. Singh and R. Singh
Description: This paper proposes a biometric-based authentication scheme using iris data, which is claimed to be more reliable and accurate than fingerprint data. It also claims to be secure against various attacks and to have low computational cost.

Title: Designing Secure and Efficient Biometric-Based Secure Access Mechanism for Cloud Services
Author: Dhillon and Kalra
Description: This paper proposes a biometric-based user authenticated key agreement mechanism for secure access to services provided by Internet of Things (IoT) devices. It uses bio hashing instead of fuzzy extractor, which is claimed to be more efficient but less secure.

V. ANALYSIS MODEL

Threat Assessment*:*
To design a secure biometric-based access mechanism, it is crucial to conduct a comprehensive threat assessment. This involves identifying potential threats, such as biometric data theft, spoofing attacks, and unauthorized access to the cloud services. Understanding the threats helps in determining the necessary security measures and countermeasures to mitigate them.

Biometric Data Management:
Efficient management of biometric data is critical for both security and performance. The analysis model should address how biometric data is collected, stored, and processed. It should consider aspects such as encryption techniques, secure transmission protocols, data storage mechanisms, and the handling of user consent and privacy concerns. Additionally, the model should explore methods to handle data integrity, availability, and backup to ensure uninterrupted access to cloud services.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404167|

Authentication Algorithm:
An effective biometric-based access mechanism requires a robust authentication algorithm. The analysis model should evaluate various algorithms and techniques, such as feature extraction, matching algorithms, and machine learning-based approaches, for accurate and reliable authentication. Additionally, the model should consider the computational efficiency of these algorithms to ensure real-time or near-real-time authentication.

Multi-Factor Authentication:
Incorporating multi-factor authentication strengthens the overall security of the access mechanism. The analysis model should explore the integration of biometric authentication with other factors, such as passwords, tokens, or smart cards. It should assess the effectiveness of combining biometrics with other authentication methods to achieve a higher level of security without compromising usability.

User Experience and Usability:
A successful access mechanism should prioritize user experience and usability. The analysis model should consider factors such as user acceptance, ease of enrollment, user interface design, and adaptability to different user environments. It should assess the impact of biometric-based access on user convenience, and overall user satisfaction

Scalability and Performance:
For cloud services with a large user base, scalability and performance are crucial considerations. The analysis model should evaluate the scalability of the biometric- based access mechanism, including the ability to handle a high volume of authentication requests concurrently. It should assess the impact on system performance, response times, and resource utilization, ensuring the mechanism can accommodate increasing user demand.

Continuous Monitoring and Updates:
A biometric-based access mechanism should be continuously monitored and updated to address emerging threats and vulnerabilities. The analysis model should explore mechanisms for monitoring system logs, detecting anomalies, and responding to security incidents promptly. It should consider the integration of threat intelligence and security patches to ensure the mechanism remains up-to-date and resilient against evolving attack vectors.

Scalability and Performance:
For cloud services with a large user base, scalability and performance are crucial considerations. The analysis model should evaluate the scalability of the biometric- based access mechanism, including the ability to handle a high volume of authentication requests concurrently. It should assess the impact on system performance, response times, and resource utilization, ensuring the mechanism can accommodate increasing user demand.

Continuous Monitoring and Updates:
A biometric-based access mechanism should be continuously monitored and updated to address emerging threats and vulnerabilities. The analysis model should explore mechanisms for monitoring system logs, detecting anomalies, and responding to security incidents promptly. It should consider the integration of threat intelligence and security patches to ensure the mechanism remains up-to-date and resilient against evolving attack vectors.

VI. 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.

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.

Economical Feasibility:

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404167|

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 as 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.

Operational Feasibility:
The examination of the operational feasibility of a system is focused on the prospects of that system. This method eradicates all of the stresses that come with being a project manager and helps him properly monitor his project's progress.

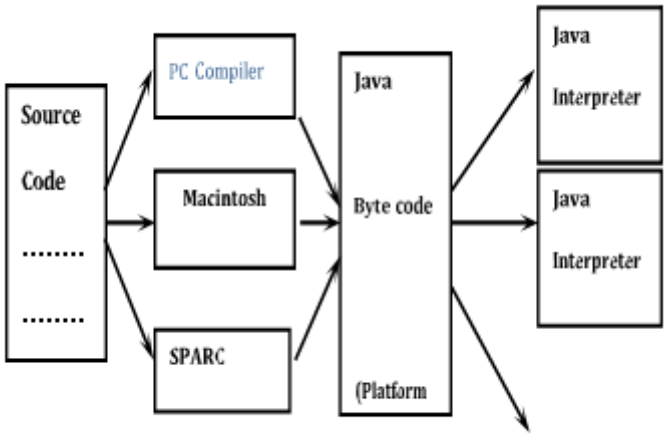
VII. FEATURES OF THE LANGUAGE USED

In my project, I have chosen Java language for developing the code.

About Java
Initially the language was called as "oak" but it was renamed as "Java" in 1995. The primary motivation of this language was the need for a platform-independent (i.e., architecture neutral) language that could be used to create software to be embedded in various consumer electronic devices.
Java is a programmer's language.

Java is cohesive and consistent.
Except for those constraints imposed by the Internet environment, Java gives the programmer, full control.

Compilation of code
When you compile the code, the Java compiler creates machine code (called byte code) for a hypothetical machine called Java Virtual Machine (JVM). The JVM is supposed to execute the byte code. The JVM is created for overcoming the issue of portability. The code is written and compiled for one machine and interpreted on all machines. This machine is called Java Virtual Machine.



During run-time the Java interpreter tricks the byte code file into thinking that it is running on a Java Virtual Machine. In reality this could be a Intel Pentium Windows 95 or Sun SARC station running Solaris or Apple Macintosh running system and all could receive code from any computer through Internet and run the Applets.

Object-Oriented
Java was not designed to be source-code compatible with any other language. This allowed the Java team the freedom to design with a blank slate. One outcome of this was a clean usable, pragmatic approach to objects. The object model in Java is simple and easy to extend, while simple types, such as integers, are kept as high-performance non-objects.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404167|

JAVA SCRIPT

JavaScript is a script-based programming language that was developed by Netscape Communication Corporation. JavaScript was originally called Live Script and renamed as JavaScript to indicate its relationship with Java. JavaScript supports the development of both client and server components of Web-based applications. On the client side, it can be used to write programs that are executed by a Web browser within the context of a Web page. On the server side, it can be used to write Web server programs that can process information submitted by a Web browser and then updates the browser's display accordingly.

Even though Java Script supports both client and server web programming ,we prefer java script at Client side programming since most of the browsers supports it. JavaScript is almost as easy to learn as HTML and Java Script statements can be included in HTML documents

VIII. SYSTEM DESIGN

Introduction:

In today's digital age, cloud services have become an integral part of our lives, providing convenient storage and access to a vast amount of data. However, with the increasing reliance on cloud services, security concerns have also risen. Traditional methods of authentication, such as passwords and tokens, are susceptible to theft, loss, and unauthorized access. To address these challenges, the development of a secure and efficient biometric-based access mechanism for cloud services is crucial.

The goal of the "Designing Secure and Efficient Biometric-Based Secure Access Mechanism for Cloud Services - Shortcut" project is to provide a robust and reliable solution that combines the security of biometric authentication with the convenience of cloud services. By leveraging biometric data, such as fingerprints, iris patterns, or facial recognition, this access mechanism aims to enhance the security of cloud services while minimizing the burden on users.

Data Base Design:

In the project of designing a secure and efficient biometric-based access mechanism for cloud services, the database plays a crucial role in storing and managing various components of the system. The database design should prioritize security, scalability, and efficient data retrieval. Here are some considerations for the database design:

User Profile Storage:

The database should include a table to store user profiles, which contain information such as user ID, biometric data (encrypted), and other relevant user attributes.

User profiles should be securely stored and encrypted to ensure privacy and prevent unauthorized access.

Proper indexing should be applied to enable efficient retrieval of user profiles during authentication.

Access Logs:

A separate table should be created to store access logs, capturing details such as user ID, timestamp, and outcome of each authentication attempt.

The access logs will assist in auditing and monitoring the system's activity, allowing identification of any suspicious or unauthorized access attempts.

Biometric Templates:

Biometric templates extracted from users' biometric data should be stored in a dedicated table.

These templates should be securely encrypted and linked to the respective user profiles.

Efficient indexing should be applied to enable quick retrieval and comparison of templates during the authentication process.

Security Measures:

The database should implement robust security measures, including access controls, role-based permissions, and encryption of sensitive data.User authentication and authorization should be enforced at the database level, ensuring that only authorized individuals can access and modify the data.

Scalability and Performance:

The database design should consider scalability to accommodate a growing number of users and access

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

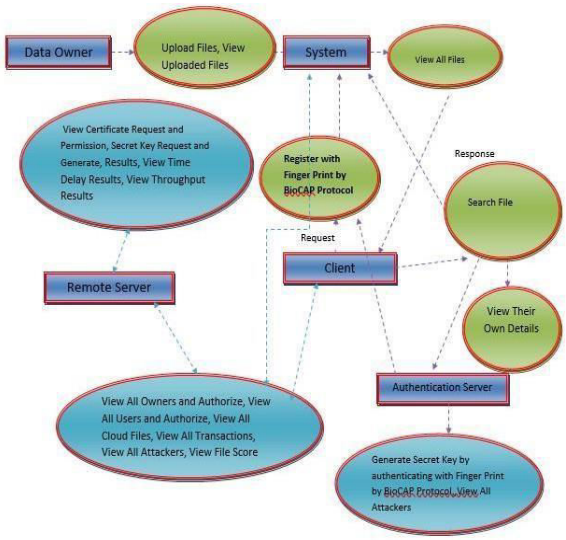
|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404167|

requests.Techniques such as horizontal partitioning or sharding can be employed to distribute the data across multiple servers, improving performance and scalability.

IX. DATA FLOW DIARAM



This diagram illustrates a secure file management system architecture, outlining the interactions between key entities. The **Data Owner** initiates the process by uploading files and can subsequently view their uploaded content through the **System**. The **System** acts as a central hub, providing a comprehensive view of all files and managing various administrative tasks. A **Client** seeking access to files sends a request to the **System**. This triggers an authentication process handled by the **Authentication Server**, which utilizes fingerprint verification through a custom "BioCAP Protocol" to generate a secret key for the Client. Upon successful authentication and authorization, the **Client** can retrieve the requested file from the **Remote Server**, which stores the files. The **Remote Server** responds to the Client's request by delivering the file. Additionally, the Client can view their own details within the system. The **System** also provides administrative functionalities, allowing for the management of all owners, users, files, transactions, attackers, and file scores. This system emphasizes security through biometric authentication and role-based access control, indicating a robust approach to file management in a likely cloud-based environment.

X. SYSTEM TESTING & IMPLEMENTATION

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, subassemblies, 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.

Types of Testing:
Unit Test:
Unit testing involves the design of test cases that validate that the internal program logic is functioning properly, and that program inputs produce 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 a business process performs accurately to the documented specifications and contains clearly defined inputs and expected results.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404167|

Integration tests:

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.

Functional Test:

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: Identified classes of valid input must be accepted.

Invalid Input: Identified classes of invalid input must be rejected.

Functions: identified functions must be exercised.

Output: identified classes of application outputs must be exercised. Systems/Procedures: 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 Test:

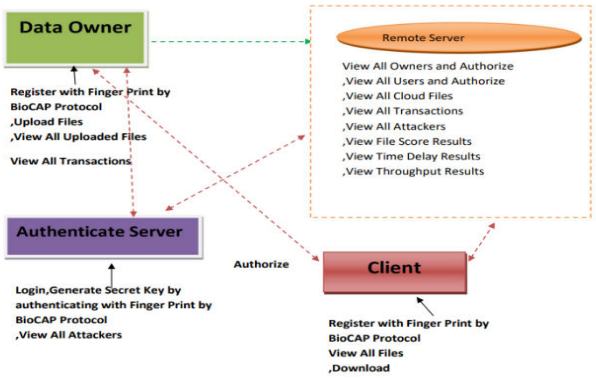
System testing ensures that the entire integrated software system meets requirements. It tests a configuration to ensure known and predictable results. An example of system testing is the configuration oriented system integration test. System testing is based on process descriptions and flows, emphasizing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

Black Box Testing:

Black Box Testing is testing the software without any knowledge of the inner workings, structure or language of the module being 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.

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

XI. ARCITECTURE



This diagram depicts a secure file management architecture focused on biometric authentication and access control. The central entity is the **Authenticate Server**, responsible for verifying user identity through fingerprint authentication

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404167|

using the "BioCAP Protocol." This process generates a secret key for the **Client**, granting them access to the system. The **Client**, after successful authentication, can view and download files, as well as register their fingerprint via the BioCAP Protocol.

The **Data Owner**, on the other hand, is responsible for uploading files and can view all uploaded files. They also have the privilege to view all transactions, suggesting a level of administrative oversight. The **Remote Server** acts as the storage location for the files, but it also appears to hold administrative functions. It allows authorized users to view and authorize all owners and users, view cloud files, transactions, attackers, file scores, time delay results, and throughput results. This indicates a comprehensive monitoring and management capability residing within the Remote Server.
The architecture emphasizes security by using biometric authentication and segregating user roles. The Client has limited access, while the Data Owner and the Remote Server possess more extensive administrative privileges. The BioCAP Protocol, though not elaborated upon, seems to be a crucial component for secure authentication and access control across the system. This setup suggests a system designed for secure file management with a focus on access control and monitoring.

XII. HARDWARE AND SOFTWARE REQUIREMENTS

Hardware System Configuration:

Processor	-	**Intel Core I3**
RAM	-	**4GB (min)**
Hard Disk	-	**250GB**

Software Requirements:

Operating System	-	**Windows**
Coding Language	-	**Java/J2EE(JSPServlets)**
Front End	-	**J2EE**
Back End	-	**My SQL**

REFERENCES

Reference for The Project Development Were Taken From The Following Books And Websites:

Oracle:

1. PL/SQL Programming by Scott Urman
2. SQL complete reference by Livion

JAVA Technologies:

3. JAVA Complete Reference
4. Java Script Programming by Yehuda Shiran Mastering JAVA Security
5. JAVA2 Networking by Pistoria
6. JAVA Security by Scotl oaks
7. J2EE Professional by Shadab Siddiqui

8. JAVA server pages by Larne Pekowsley
9. JAVA Server pages by Nick Todd

HTML:

10. HTML Black Book by Holzner

JDBC:

11. Java Database Programming with JDBC by Patel moss. Software Engineering by Roger Pressman

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details