International Scientific Journal of Engineering and Management (ISJEM) ISSN: 2583-6129
Volume: 04 Issue: 04 | April – 2025 DOI: 10.55041/ISJEM02961
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

# Title: Developing Ensured and Effective Bio-Security for Cloud Services

**Authors:** M. SriKari SriHariPriya, M. Asmitha, S. Sandeep Teja

**Affiliation:** Department of Data Science, Anurag University, Venkatapur (V), Ghatkesar (M), Medchal(D), T.S-500088

**Abstract:** The demand for remote data storage and computation services is increasing exponentially in our data-driven society, creating a pressing need for secure access to such data and services. This paper proposes a biometric-based authentication protocol designed to provide secure access to remote cloud servers. The approach leverages biometric data from users as secret credentials, deriving unique identities that facilitate the generation of private and session keys essential for secure communication. Our comprehensive security analysis, including a formal Real-Or-Random (ROR) model examination and verification using the Automated Validation of Internet Security Protocols and Applications (AVISPA) tool, highlights the robustness of the proposed system against various adversarial attacks. Experiments demonstrate the efficiency and utility of the proposed approach.

**Keywords:** Authentication, biometric-based security, cloud service access, session key

**1. Introduction** Cloud services have become an integral aspect of contemporary computing; however, ensuring secure access remains a substantial hurdle. The design of effective authentication, authorization, and accounting mechanisms is crucial. This paper aims to address these challenges through the development of a new bio-security protocol.

**1.1 Motivation** With an escalating reliance on cloud services for data management, the necessity for stringent security measures has never been more critical.

**1.2 Problem Definition** Traditional authentication methods are often vulnerable to various security threats, emphasizing the need for innovative solutions.

**1.3 Objective of the Project** To develop an effective and efficient bio-security mechanism for cloud service authentication using biometric data.

**2. Literature Review** This section reviews existing research and frameworks surrounding biometric-based security systems, focusing on applications within cloud services. Notable contributions include biometric authentication schemes and privacy-preserving protocols against known vulnerabilities.

## 3. Analysis

**3.1 Existing System** Outlines the current limitations of existing cloud security frameworks and identifies areas for improvement.

**3.2 Proposed System** Description of the new biometric-based authentication protocol and its architecture.

### 3.3 System Requirements:

This section elaborates on the functional requirements of the application. The

SRS itself can be divided into module, each module having specifications. In order to carry out

the project, the following hardware and software is required.

**HARDWARE REQUIREMENTS:**

- **System :** i3
- **Hard Disk :** 40 GB.
- **Floppy Drive :** 1.44 Mb**.**
- **Monitor :** 15 VGA Colour**.**
- **Mouse :** Logitech.
- **Ram :** 512 Mb.

**SOFTWARE REQUIREMENTS:**

**Software Requirements**

**Technology :** Java 2 Standard Edition, JDBC

**Web Server :** Tomcat 7.0

**Client Side Technologies :** HTML, CSS, JavaScript

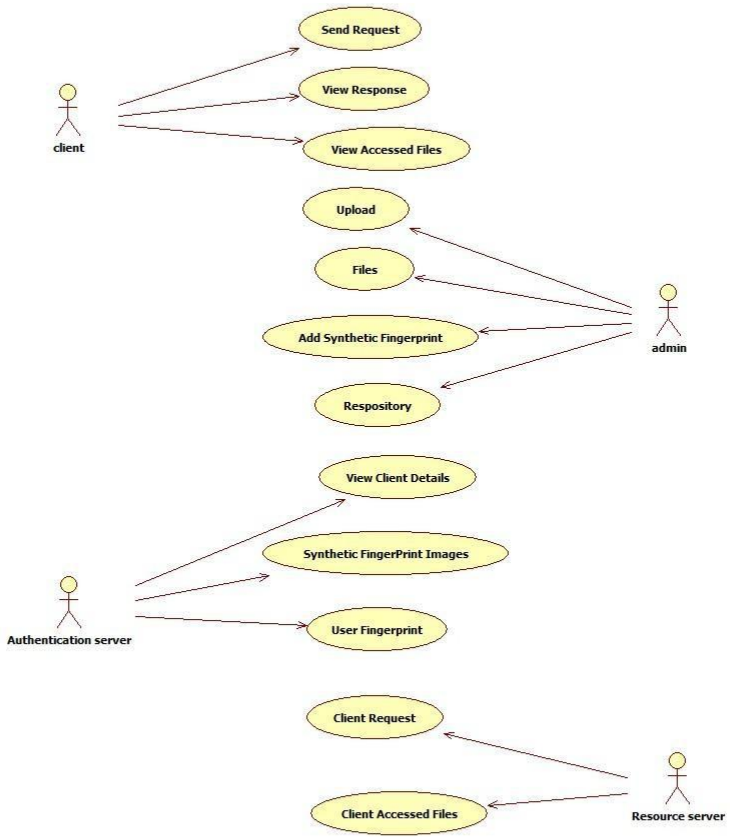
**Server Side Technologies :** Servlets, JSP

**Data Base Server :** MySQL

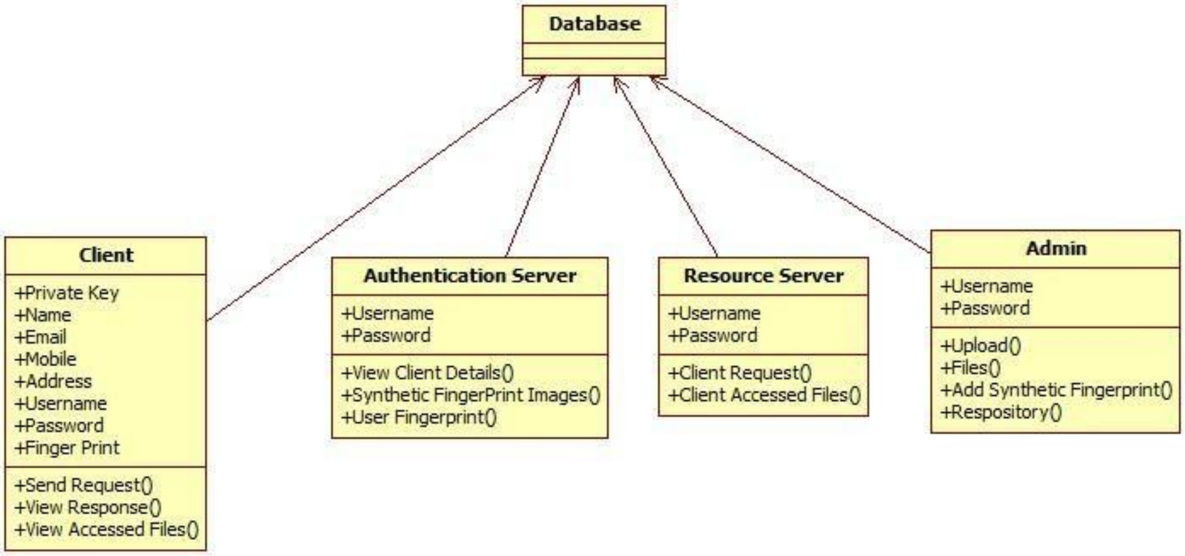
**Editor** : Netbeans8.1

**4. Design 4.1 UML Diagrams** Illustrate key components and interactions within the proposed system:

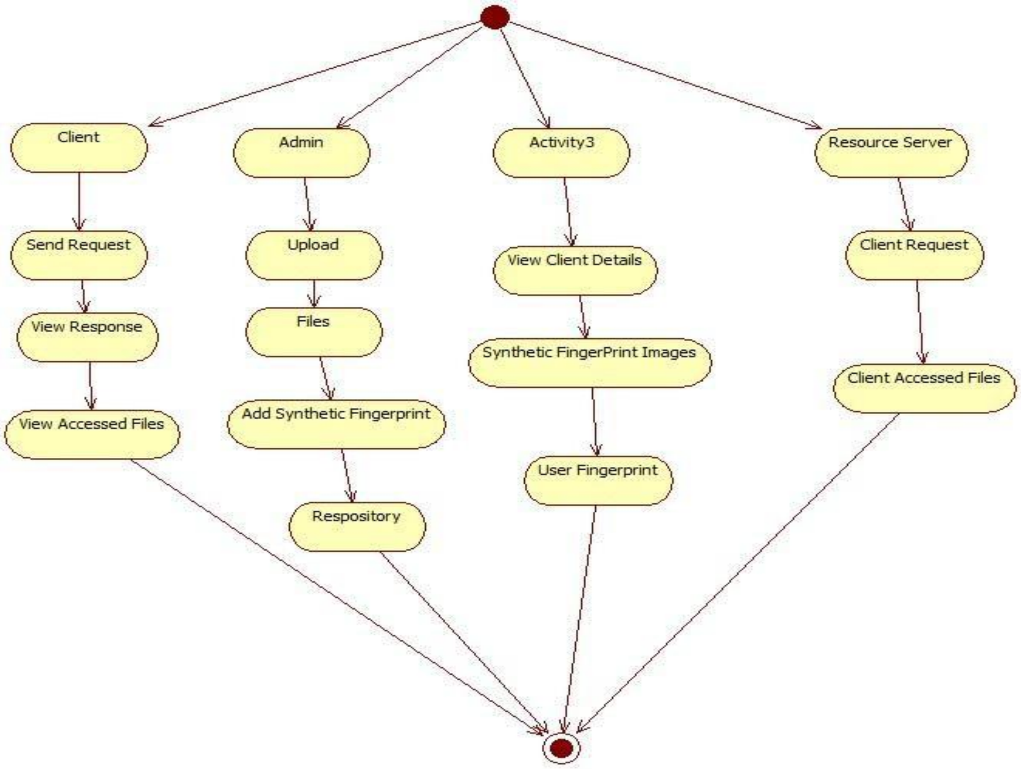
- **4.1.1 Use Case Diagram**



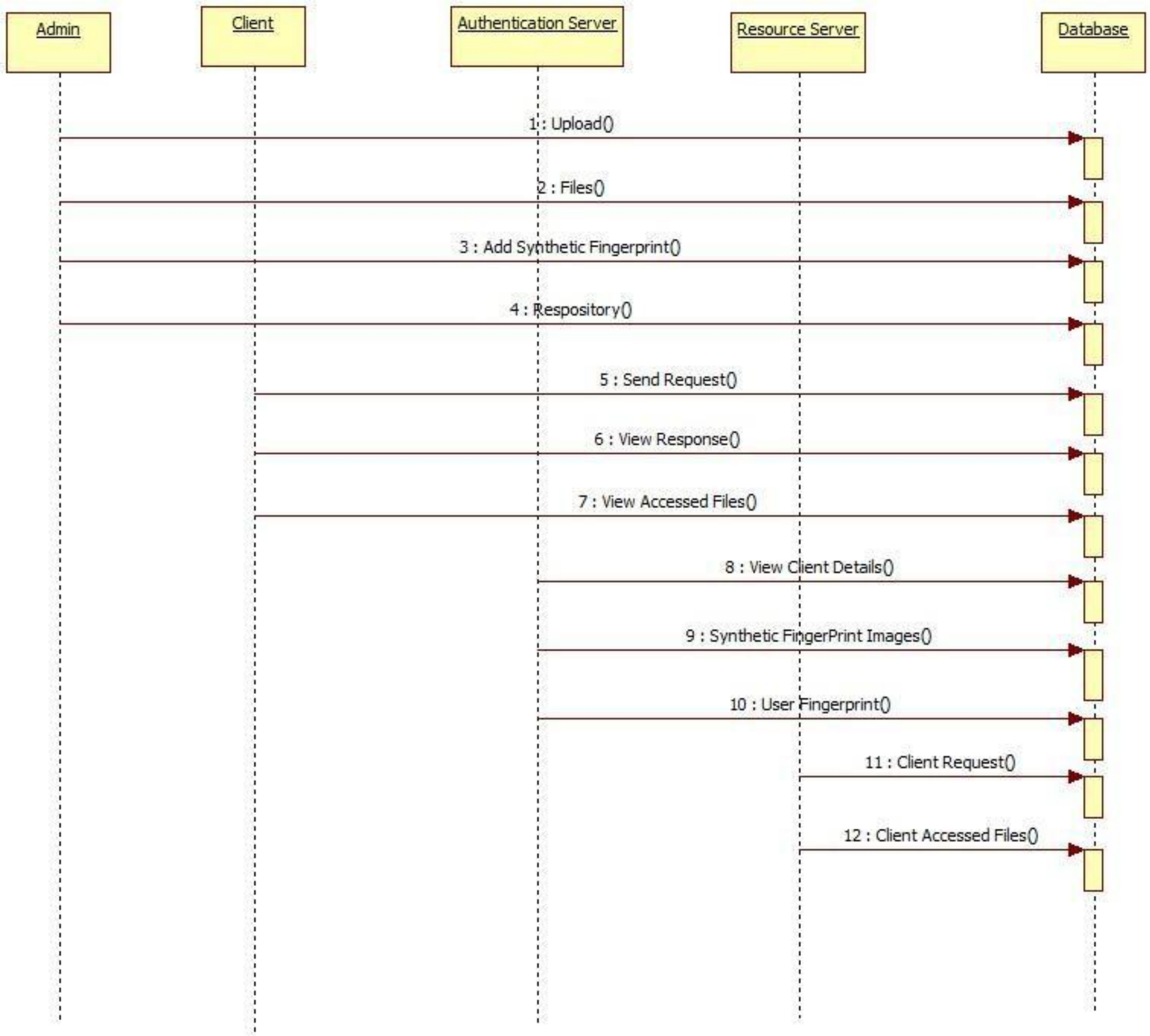
- **4.1.2 Class Diagram**



- **4.1.3 Activity Diagram**



- **4.1.4 Sequence Diagram**



## 5. Implementation 5.1 Module Description

- **5.1.1 User Input Module**
- **5.1.2 Image Processing Module**
- **5.1.3 AI Model Integration Module**
- **5.1.4 Report Generation Module**
- **5.1.5 MongoDB Storage Module**

**5.2 Introduction to Technologies Used** Technologies employed in the implementation:

- **5.2.1 Flask (Backend Framework)**
- **5.2.2 Streamlit (Frontend UI)**
- **5.2.3 OpenCV & NumPy (Image Processing)**
- **5.2.4 TensorFlow/Keras (AI Model Integration)**
- **5.2.5 MongoDB (Database for Storing Reports)**

### 5.3 Sample Code HTML

Html is a language which is used to create web pages with html marking up a page to indicate its format, telling the web browser where you want a new line to begin or how you want text or images aligned and more are possible.

We used the following tags in our project.

**Table**:

Tables are so popular with web page authors is that they let you arrange the elements of a web page in such a way that the browser won’t rearrange them web page authors frequently use tables to structure web pages.

**TR**:

TR is used to create a row in a table encloses <TH> and <TD> elements. <TR> contain many attributes. Some of them are,

**ALIGN**: specifies the horizontal alignment of the text in the table row.

**BGCOLOR**: Specifies the background color for the row.

**BORDERCOLOR**: Sets the external border color for the row.

**VALIGN**: Sets the vertical alignment of the data in this row. **TH**:

TH is used to create table heading.

**ALIGN**: Sets the horizontal alignment of the content in the table cell. Sets LEFT, RIGHT, CENTER.

**BACKGROUND**: Species the back ground image for the table cell.

**BGCOLOR**: Specifies the background color of the table cell

**VALIGN**: Sets the vertical alignment of the data. Sets to TOP, MIDDLE, BOTTOM or BASELINE.

**WIDTH**: Specifies the width of the cell. Set to a pixel width or a percentage of the display area.

**TD**:

TD is used to create table data that appears in the cells of a table.

**ALIGN**: Species the horizontal alignment of content in the table cell. Sets to LEFT, CENTER, RIGHT.

**BGCOLOR**: Specifies the background image for the table cell.

**BGCOLOR**: sets the background color of the table cells.

**WIDTH**: Species the width of the cell

**Frames**:

Frames are used for either run off the page or display only small slices of what are supposed to be shown and to configure the frame we can use <FRAMESET>There are two important points to consider when working with <FRAMESET>.

<FRAMESET> element actually takes the place of the <BODY> element in a document. Specifying actual pixel dimensions for frames .

<FRAME> Elements are used to create actual frames.

From the frameset point of view dividing the browser into tow vertical frames means creating two columns using the <FRAMESET> elements COLS attribute.

The syntax for vertical fragmentation is,

<FRAMESET COLS =”50%, 50%”>

</FRAMESET>

Similarly if we replace COLS with ROWS then we get horizontal fragmentation. The syntax for horizontal fragmentation is,

<FRAMESET ROWS=”50%, 50%”>

</FRAMESET>

**Form**:

The purpose of FORM is to create an HTML form; used to enclose HTML controls, like buttons and text fields.

**Attribute:**

**ACTION**: Gives the URL that will handle the form data.

**NAME**: Gives the name to the form so you can reference it in code set to an alphanumeric string.

**METHOD**: method or protocol is used to sending data to the target action URL. The GET method is the default, it is used to send all form name/value pair information in an URL. Using the POST method, the content of the form are encoded as with the GET method, but are sent in environment variables.

**Controls in HTML**:

<INPUT TYPE =BUTTON>:

Creates an html button in a form.

**ATTRIBUTES**:

**NAME**: gives the element a name. Set to alphanumeric characters.

**SIZE**: sets the size.

**VALUE**: sets the caption of the element.

<INPUT TYPE = PASSWORD>:

Creates a password text field, which makes typed input.

**ATTRIBUTES**:

**NAME**: gives the element a name, set to alphanumeric characters.

**VALUE**: sets the default content of the element.

<INPUT TYPE=RADIO>:

Creates a radio button in a form.

**ATTRIBUTE**:

**NAME**: Gives the element a name. Set to alphanumeric character.

**VALUE**: Sets the default content of the element.

<INPUT TYPE=SUBMIT>:

Creates a submit button that the user can click to send data in the form back to the web server.

**ATTRIBUTES**:

**NAME**: Gives the element a name. Set to alphanumeric characters.

**VALUE**: Gives this button another label besides the default, Submit Query. Set to alphanumeric characters.

<INPUT TYPE=TEXT>:

Creates a text field that the user can enter or edit text in.

**ATTRIBUTES**:

**NAME**: Gives the element a name. Set to alphanumeric characters.

**VALUE**: Holds the initial text in the text field. Set to alphanumeric characters.

**Java Script**:

Java script originally supported by Netscape navigator is the most popular web scripting language today.

Java script lets you embedded programs right in your web pages and run these programs using the web browser. You place these programs in a <SCRIPT> element, usually within the <HEAD> element. If you want the script to write directly to the web page, place it in the <BODY> element.

**Java script Methods**:

**Writeln**:

Document.writeln () is a method, which is used to write some text to the current web page.

**onClick**:

Occurs when an element is clicked.

**onLoad**:

Occurs when the page loads.

**onMouseDown**:

Occurs when a mouse button goes down.

**onMouseMove**:

Occurs when the mouse moves.

**OnUnload**:

Occurs when a page is unloaded.

**MySQL**:

MySQL is an open source relational database management system (RDBMS).This is the most popular database system used with PHP. MySQL is distributed and supported by Oracle Corporation.

MySQL runs on almost all platforms including Linux, Unix and Windows. Although it can be used in a wide range of applications, MySQL is often associated with web applications and online publishing.

MySQL is an essential constituent of an open source enterprise stack called LAMP. LAMP is a web development platform that uses Linux as an operating system, in the form of Apache web server, MySQL relational database management system and PHP object-oriented scripting language.

**Advantages of MySQL**:

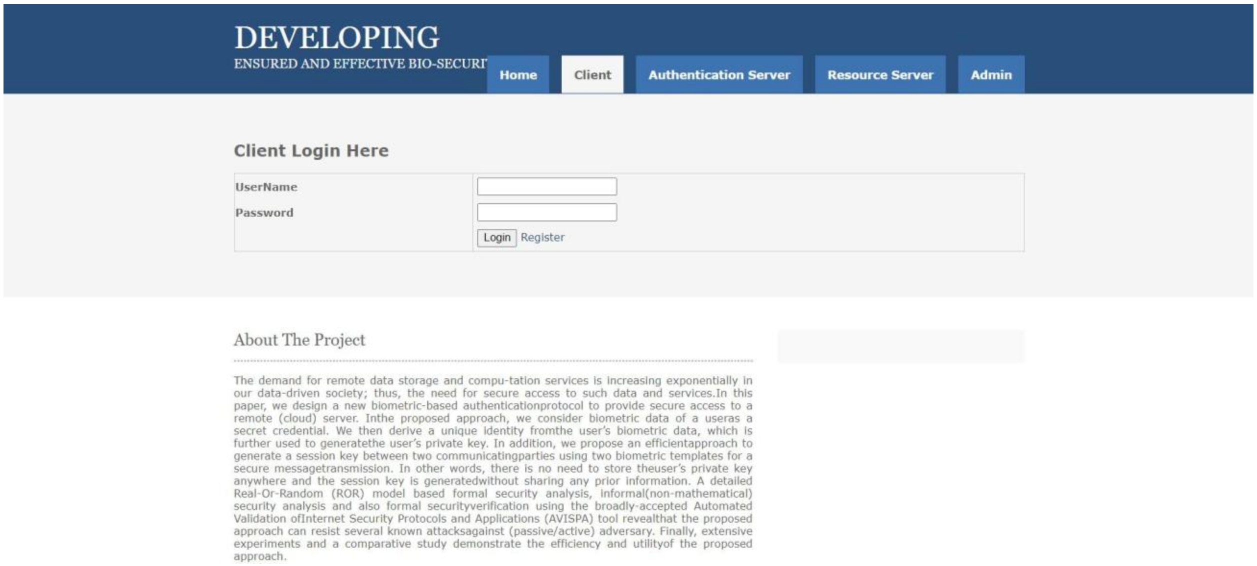
**Data Security**: MySQL is globally renowned for being the most secure and reliable database management system used in popular web applications including WordPress, Drupal, Joomla, Facebook and Twitter.

**High Performance**: MySQL features a distinct storage-engine framework that facilitates system administrators to configure the MySQL database server for a flawless performance. Round-the-Clock Up-time: MySQL comes with the assurance of 24×7 up-time and offers a wide range of high-availability solutions, including specialized cluster servers and master/slave replication configurations.

**The Flexibility of Open Source**: All the fears and worries that arise in an open-source solution can be brought to an end with MySQL's round-the-clock support and enterprise indemnification. The secure processing and trusted software of MySQL combine to provide effective transactions for large-volume projects. It makes maintenance, debugging and upgrades fast and easy while enhancing the end-user experience.

## 6. Results and Discussion Screenshots of Outputs

- ### 6.1 Client Login



Client Login Here

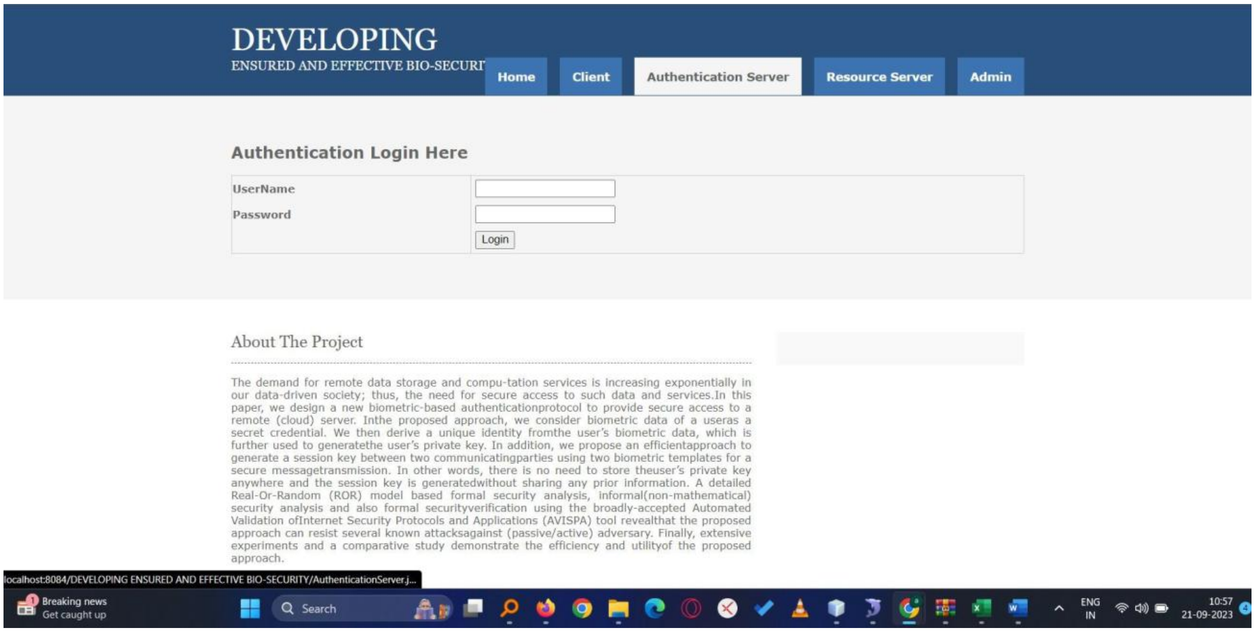
UserName

Password

About The Project

The demand for remote data storage and compu-tation 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 authenticationprotocol to provide secure access to a remote (cloud) server. Inthe proposed approach, we consider biometric data of a useras a secret credential. We then derive a unique identity fromthe user's biometric data, which is further used to generatethe user's private key. In addition, we propose an efficientapproach to generate a session key between two communicatingparties using two biometric templates for a secure messagetransmission. In other words, there is no need to store theuser's private key anywhere and the session key is generatedwithout sharing any prior information. A detailed Real-Or-Random (ROR) model based formal security analysis, informal(non-mathematical) security analysis and also formal securityverification using the broadly-accepted Automated Validation ofInternet Security Protocols and Applications (AVISPA) tool revealthat the proposed approach can resist several known attacksagainst (passive/active) adversary. Finally, extensive experiments and a comparative study demonstrate the efficiency and utilityof the proposed approach.

- ### 6.2 Authentication Login


DEVELOPING
ENSURED AND EFFECTIVE BIO-SECURI
Home
Client
Authentication Server
Resource Server
Admin
Login
localhost:8084/DEVELOPING ENSURED AND EFFECTIVE BIO-SECURITY/AuthenticationServer.j...
Breaking news
Get caught up
Search
ENG
IN
10:57
21-09-2023

Authentication Login Here

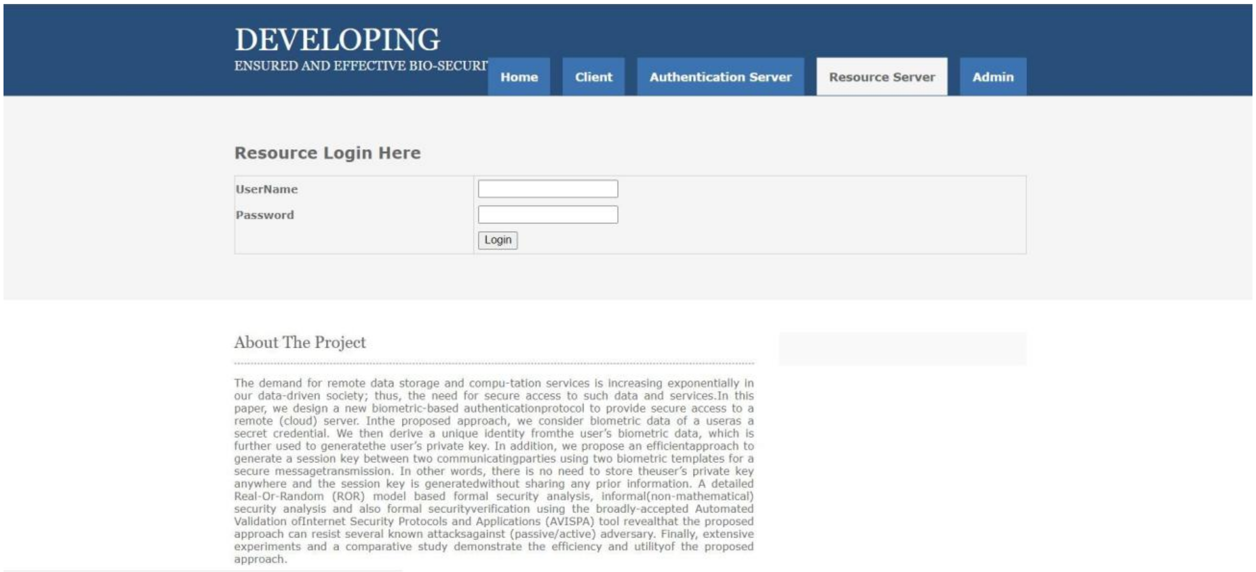
UserName

Password

About The Project

The demand for remote data storage and compu-tation 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 authenticationprotocol to provide secure access to a remote (cloud) server. Inthe proposed approach, we consider biometric data of a useras a secret credential. We then derive a unique identity fromthe user's biometric data, which is further used to generatethe user's private key. In addition, we propose an efficientapproach to generate a session key between two communicatingparties using two biometric templates for a secure messagetransmission. In other words, there is no need to store theuser's private key anywhere and the session key is generatedwithout sharing any prior information. A detailed Real-Or-Random (ROR) model based formal security analysis, informal(non-mathematical) security analysis and also formal securityverification using the broadly-accepted Automated Validation ofInternet Security Protocols and Applications (AVISPA) tool revealthat the proposed approach can resist several known attacksagainst (passive/active) adversary. Finally, extensive experiments and a comparative study demonstrate the efficiency and utilityof the proposed approach.

- **6.3 Resource Login**



Resource Login Here

UserName

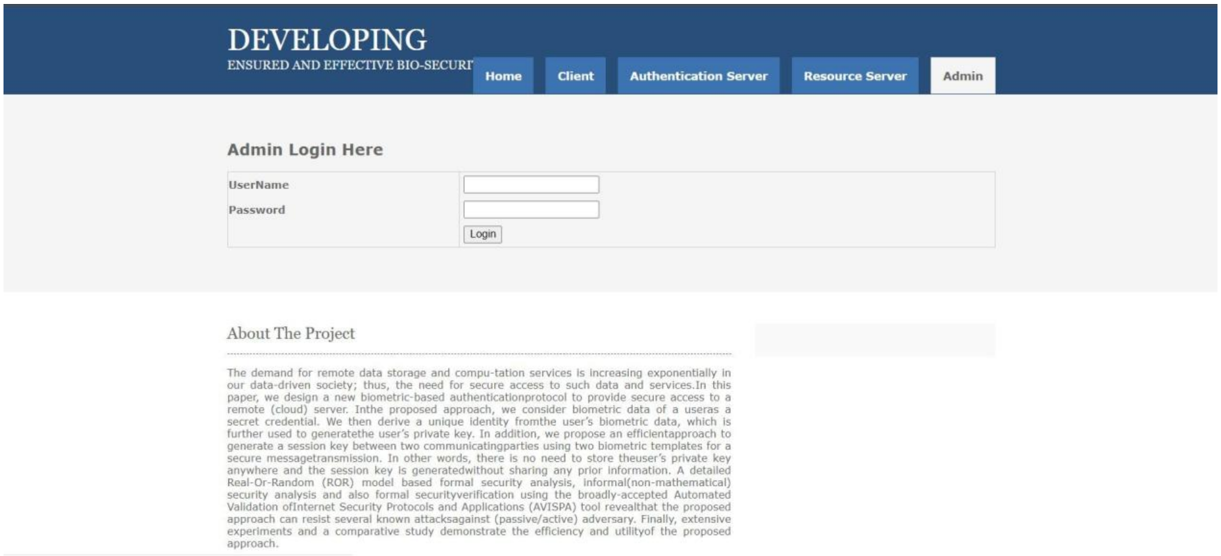
Password

Login

About The Project

The demand for remote data storage and compu-tation 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 authenticationprotocol to provide secure access to a remote (cloud) server. Inthe proposed approach, we consider biometric data of a useras a secret credential. We then derive a unique identity fromthe user's biometric data, which is further used to generatethe user's private key. In addition, we propose an efficientapproach to generate a session key between two communicatingparties using two biometric templates for a secure messagetransmission. In other words, there is no need to store theuser's private key anywhere and the session key is generatedwithout sharing any prior information. A detailed Real-Or-Random (ROR) model based formal security analysis, informal(non-mathematical) security analysis and also formal securityverification using the broadly-accepted Automated Validation ofInternet Security Protocols and Applications (AVISPA) tool revealthat the proposed approach can resist several known attacksagainst (passive/active) adversary. Finally, extensive experiments and a comparative study demonstrate the efficiency and utilityof the proposed approach.

- **6.4 Admin Login**



Admin Login Here

UserName

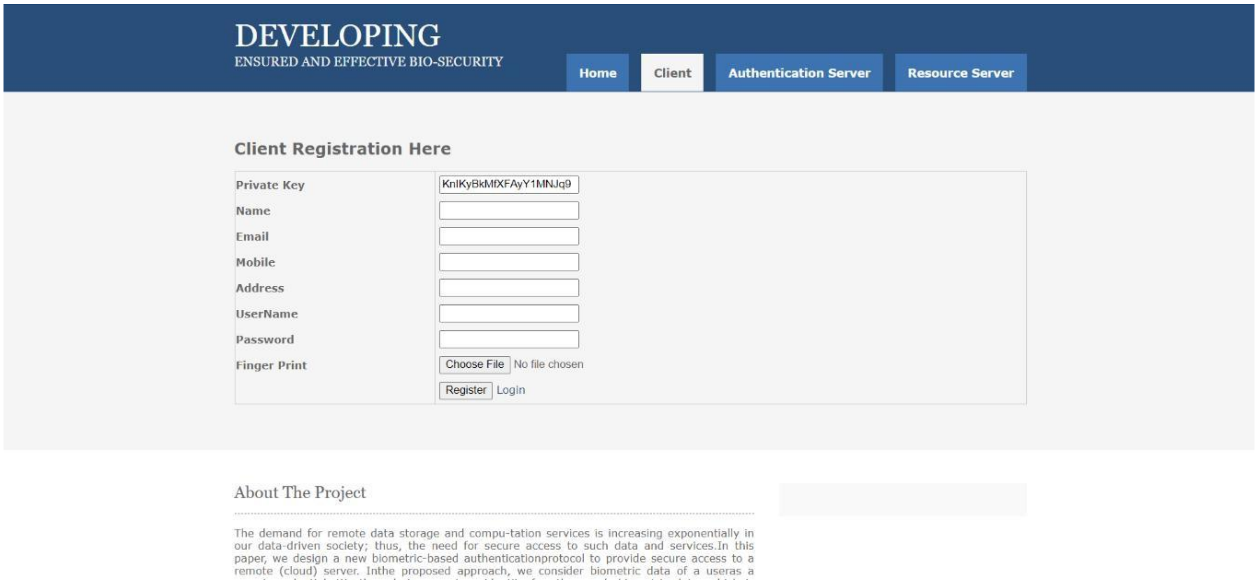
Password

Login

About The Project

The demand for remote data storage and compu-tation 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 authenticationprotocol to provide secure access to a remote (cloud) server. Inthe proposed approach, we consider biometric data of a useras a secret credential. We then derive a unique identity fromthe user's biometric data, which is further used to generatethe user's private key. In addition, we propose an efficientapproach to generate a session key between two communicatingparties using two biometric templates for a secure messagetransmission. In other words, there is no need to store theuser's private key anywhere and the session key is generatedwithout sharing any prior information. A detailed Real-Or-Random (ROR) model based formal security analysis, informal(non-mathematical) security analysis and also formal securityverification using the broadly-accepted Automated Validation ofInternet Security Protocols and Applications (AVISPA) tool revealthat the proposed approach can resist several known attacksagainst (passive/active) adversary. Finally, extensive experiments and a comparative study demonstrate the efficiency and utilityof the proposed approach.

- **6.5 Client Registration Page**



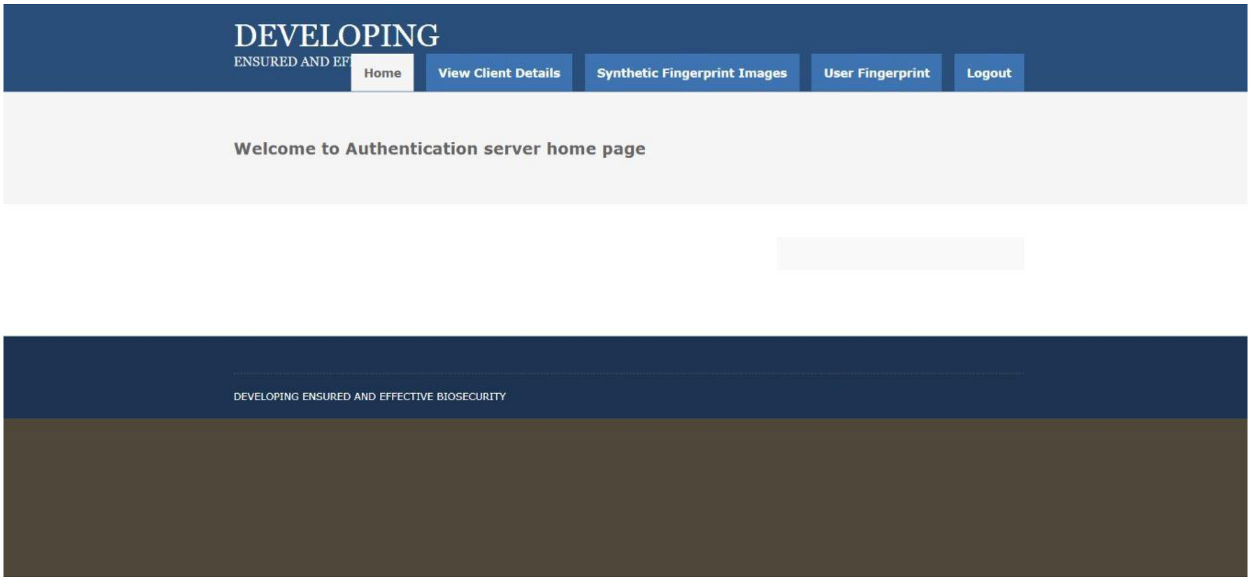
Client Registration Here

| | |
|---|---|
| Private Key | KnlKyBkMfXFAyY1MNJq9 |
| Name | |
| Email | |
| Mobile | |
| Address | |
| UserName | |
| Password | |
| Finger Print | Choose File No file chosen |
| | Register Login |

About The Project

The demand for remote data storage and compu-tation 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 authenticationprotocol to provide secure access to a remote (cloud) server. Inthe proposed approach, we consider biometric data of a useras a

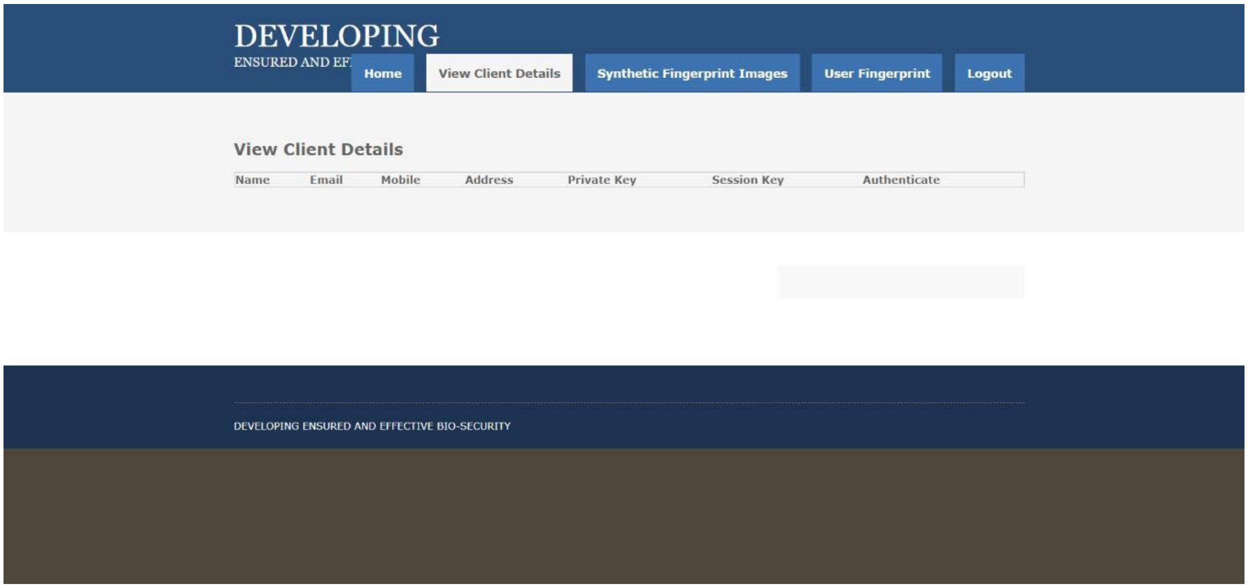
- **6.6 Authentication server home page**



Welcome to Authentication server home page

DEVELOPING ENSURED AND EFFECTIVE BIOSECURITY

- **6.7 Client details**

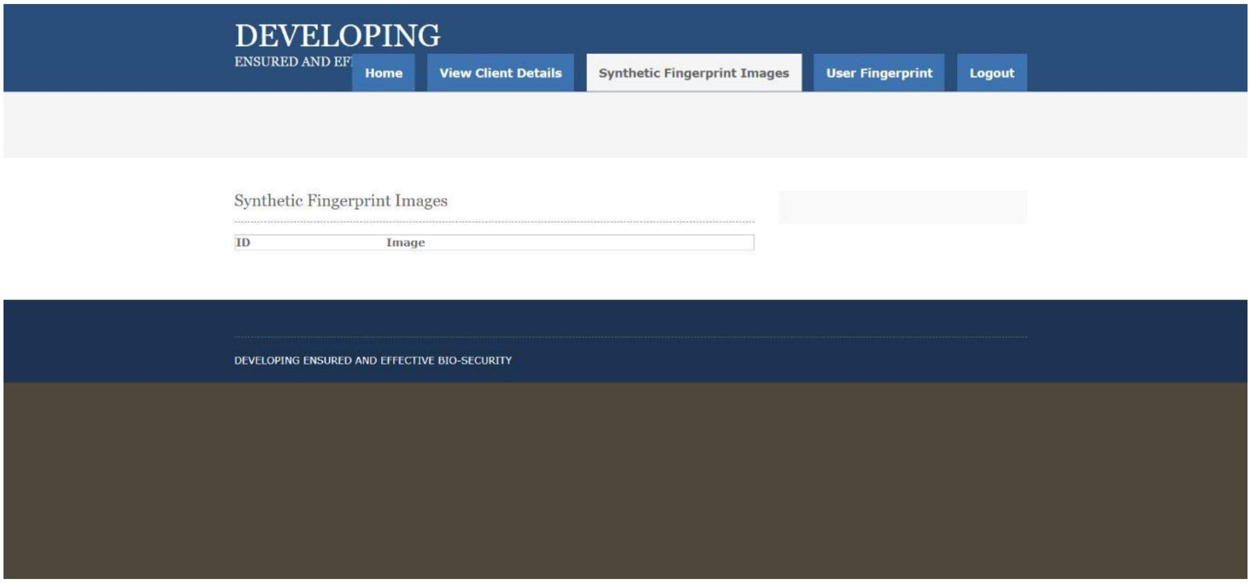


View Client Details

| Name | Email | Mobile | Address | Private Key | Session Key | Authenticate |
|---|---|---|---|---|---|---|

DEVELOPING ENSURED AND EFFECTIVE BIO-SECURITY

- **6.8 Viewing synthetic fingerprints**

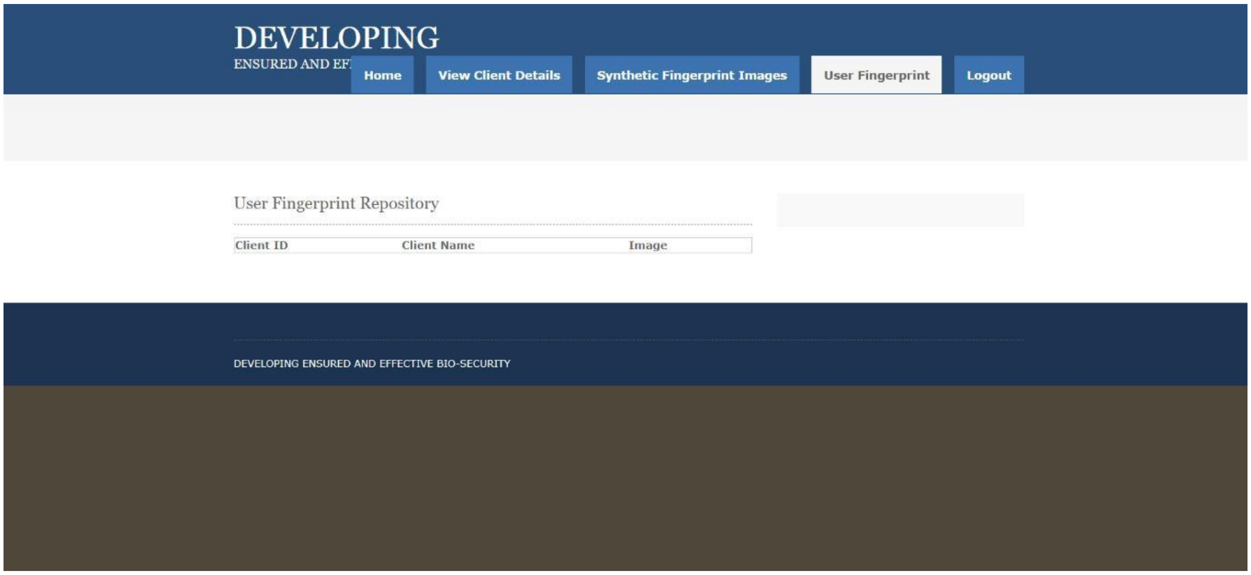


Synthetic Fingerprint Images

| ID | Image |
|---|---|

DEVELOPING ENSURED AND EFFECTIVE BIO-SECURITY

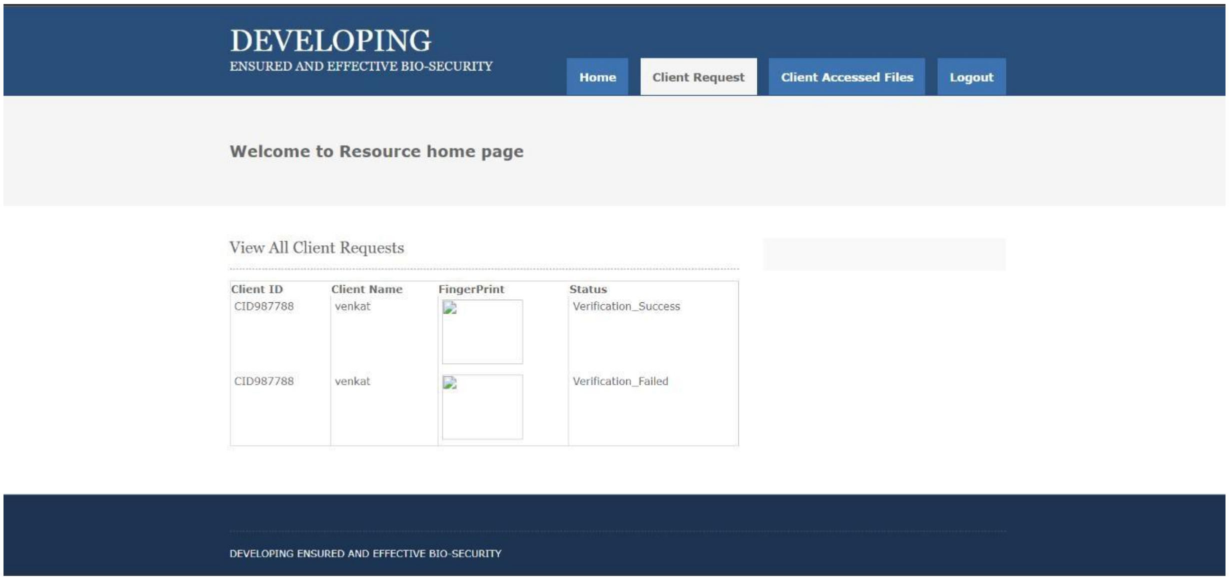
- **6.9 Viewing user fingerprint repository**


DEVELOPING
ENSURED AND EF
Home
View Client Details
Synthetic Fingerprint Images
User Fingerprint
Logout
DEVELOPING ENSURED AND EFFECTIVE BIO-SECURITY

User Fingerprint Repository

| Client ID | Client Name | Image |
|---|---|---|

- **6.10 Viewing all client requests in Resource home page**

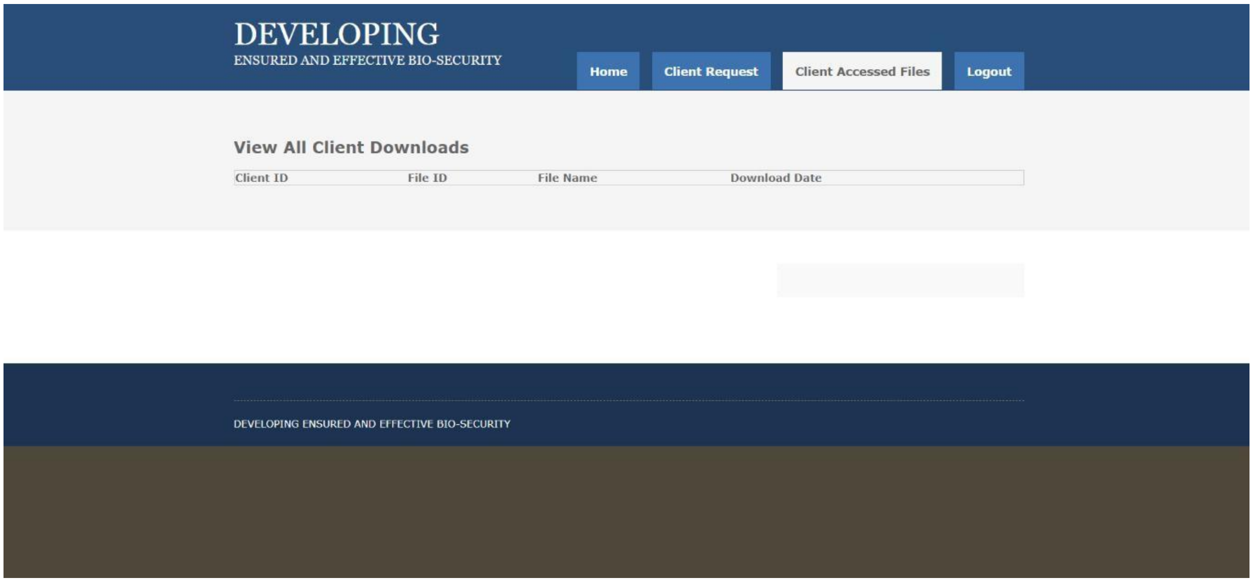

DEVELOPING
ENSURED AND EFFECTIVE BIO-SECURITY
Home
Client Request
Client Accessed Files
Logout
DEVELOPING ENSURED AND EFFECTIVE BIO-SECURITY

Welcome to Resource home page

View All Client Requests

| Client ID | Client Name | FingerPrint | Status |
|---|---|---|---|
| CID987788 | venkat | | Verification_Success |
| CID987788 | venkat | | Verification_Failed |

- **6.11 Downloading all client details**

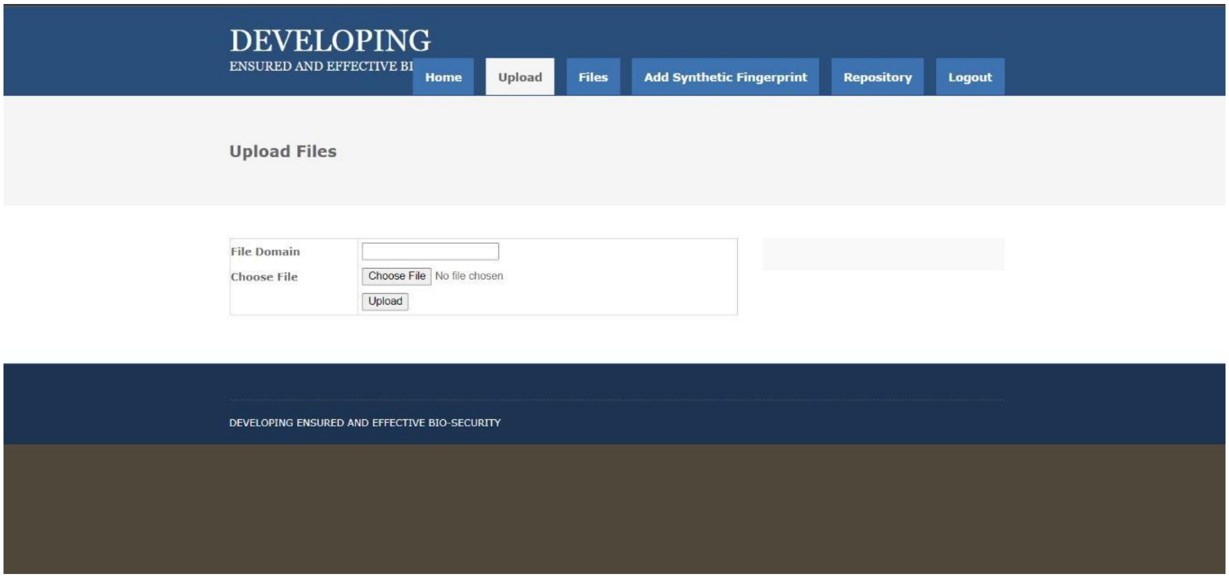

DEVELOPING
ENSURED AND EFFECTIVE BIO-SECURITY
Home
Client Request
Client Accessed Files
Logout

View All Client Downloads

| Client ID | File ID | File Name | Download Date |
|---|---|---|---|

DEVELOPING ENSURED AND EFFECTIVE BIO-SECURITY

- **6.12 Upload the files**

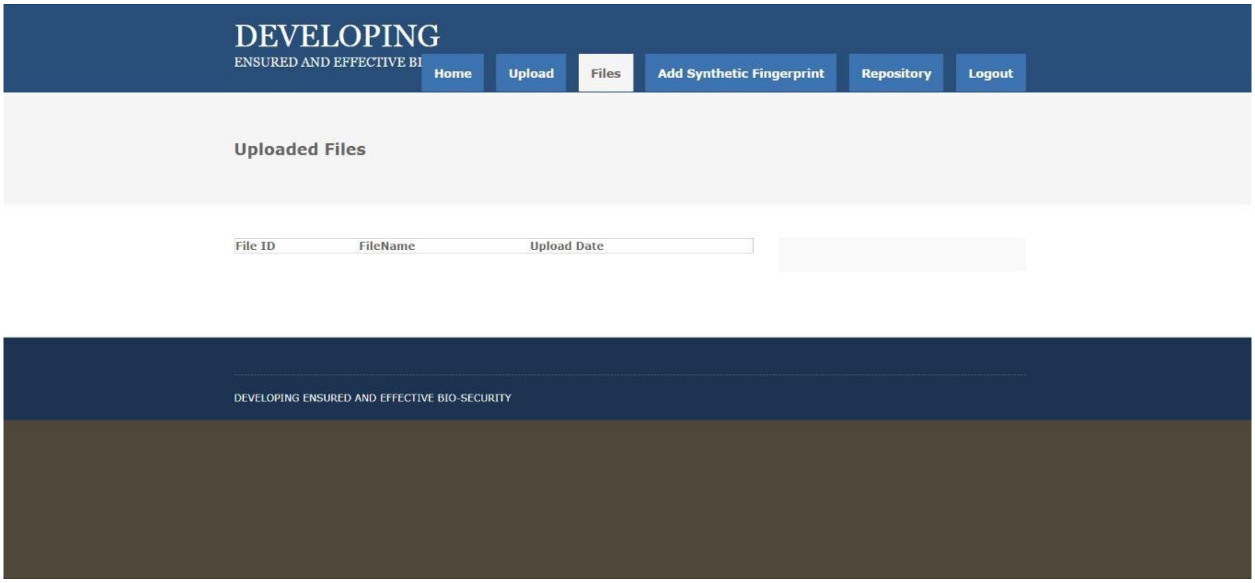

DEVELOPING
ENSURED AND EFFECTIVE BI
Home
Upload
Files
Add Synthetic Fingerprint
Repository
Logout

Upload Files

| | |
|---|---|
| File Domain | |
| Choose File | Choose File No file chosen |
| | Upload |

DEVELOPING ENSURED AND EFFECTIVE BIO-SECURITY

- ### 6.13 Viewing Uploaded files



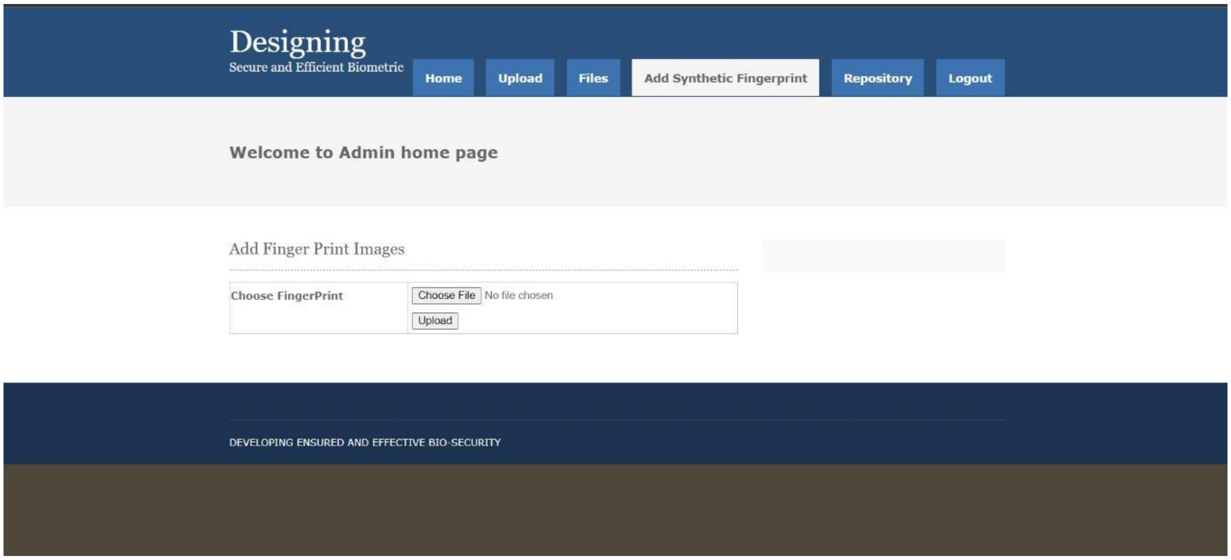
DEVELOPING
ENSURED AND EFFECTIVE BI

Uploaded Files

| File ID | FileName | Upload Date |
|---|---|---|

DEVELOPING ENSURED AND EFFECTIVE BIO-SECURITY

- ### 6.14 Adding fingerprints



Designing
Secure and Efficient Biometric

Welcome to Admin home page

Add Finger Print Images

| | |
|---|---|
| Choose FingerPrint | Choose File No file chosen<br>Upload |

DEVELOPING ENSURED AND EFFECTIVE BIO-SECURITY

## 7. Testing

### 7.1 Introduction

Testing involves operation of a system or application under controlled conditions and evaluating the results. The controlled conditions should include both normal and abnormal conditions. Testing should intentionally attempt to make things go wrong to determine if things

happen when they shouldn't or things don't happen when they should. It is oriented to 'detection'**.**

### 7.2 Types of Testing

- **Unit Testing:** Unit testing is a software development process in which the smallest testable parts of an application, called units, are individually and independently scrutinized for proper operation. Unit testing is often automated but it can also be done manually. This testing mode is a component of Extreme Programming (XP), a pragmatic method of software development that takes a meticulous approach to building a product by means of continual testing and revision. Unit tests are written from a programmer's perspective. They ensure that a particular method of a class successfully performs a set of specific tasks. Each test confirms that a method produces the expected output when given a known input.
- **Performance Testing:** Performance testing is the process of determining the speed or effectiveness of a computer, network, software program or device. This process can involve quantitative tests done in a lab, such as measuring the response time or the number of MIPS (millions of instructions per second) at which a system functions. Qualitative attributes such as Reliability, scalability and interoperability may also be evaluated. Performance testing is often done in conjunction with stress testing. Performance testing can verify that a system meets the specifications claimed by its manufacturer or vendor. The process can compare two or more devices or programs in terms of parameters such as speed, data transfer rate, bandwidth, throughput, efficiency or reliability. Performance testing can also be used as a diagnostic aid in locating communications bottlenecks. Often a system will work much better if a problem is resolved at a single point or in a single component. For example, even the fastest computer will function poorly on today's Web if the connection occurs at only 40 to 50 Kbps (kilobits per second).
- **Integration Testing:**Integration testing, also known as integration and testing (I&T), is a software development process which program units are combined and tested as groups in multiple ways. In this context, a unit is defined as the smallest testable part of an application. Integration testing can expose problems with the interfaces among program components before trouble occurs in real-world program execution.

- **7.3 Test Cases**
- **Test case for Login form:**

| | |
|---|---|
| **FUNCTION :** | **LOGIN** |
| **EXPECTED RESULTS :** | Should Validate the user and check his existence in database |
| **ACTUAL RESULTS :** | Validate the user and checking the user against the database |
| **LOW PRIORITY :** | No |
| **LOW PRIORITY :** | Yes |

- **Test case for User Registration form:**

| | |
|---|---|
| **FUNCTION :** | **USER REGISTRATION** |
| **EXPECTED RESULTS :** | Should check if all the fields are filled by the user and saving the user to database. |
| **ACTUAL RESULTS :** | Checking whether all the fields are field by user or not through validations and saving user |
| **LOW PRIORITY :** | No |
| **LOW PRIORITY :** | Yes |

- **Test case for Change Password:**

| | |
|---|---|
| **FUNCTION :** | **USER REGISTRATION** |
| **EXPECTED RESULTS :** | Should check if all the fields are filled by the user and saving the user to database. |
| **ACTUAL RESULTS :** | Checking whether all the fields are field by user or not through validations and saving user |
| **LOW PRIORITY :** | No |
| **LOW PRIORITY :** | Yes |

- **Test case for Forget Password:**

| **Module** | **Functionality** | **Test Case** | **Expected Results** | **Actual Results** | **Results** | **Priority** |
|---|---|---|---|---|---|---|

| | | | | | | |
|---|---|---|---|---|---|---|
| User | Login Use Cases | 1. Navigate ToWww.Sample.Com<br>2. 2.Click On Submit Button Without Entering Username and Password | A Validation Should Be As Below "Please Enter Valid Username & Password" | A Validation Has Been Populated As Expected | Pass | High |
| | | | | | | |
| | | 1. aNavigate To Www.Sample.Com<br>1. 2. Click On Submit Button With Out Filling Password And With Valid Username | Validation Should Be As Below "Please Enter Valid Password Or Password Field Can Not Be Empty | A Validation Is Shown As Expected | Pass | High |

## 8. Conclusion

Biometric has its unique advantages over conventional password and token-based security system, as evidenced by its increased adoption (e.g., on Android and iOS devices). In this paper, we introduced a biometric-based mechanism to authenticate a user seeking to access services and computational resources from a remote location. Our proposed approach allows one to generate a private key from a fingerprint biometric reveals, as it is possible to generate the same key from a fingerprint of a user with 95.12% accuracy. Our proposed session key generation approach using two biometric data does not require any prior information to be shared. A comparison of our approach with other similar authentication protocols reveals that our protocol is more resilient to several known attacks. Future research includes exploring other biometric traits and also multimodal biometrics for other sensitive applications (e.g., in national security matters).

## 9. Future Enhancement

While the proposed biometric-based authentication protocol effectively addresses several limitations of conventional cloud security mechanisms, there remain opportunities for future development and enhancement:

### 1. Integration of Multi-Modal Biometrics

The current system utilizes fingerprint data for authentication. Future work can explore integrating multiple biometric modalities (e.g., face recognition, iris scans, or voice patterns) to enhance accuracy and security. Multi-modal systems are known to be more resistant to spoofing and can improve user verification in diverse environments.

### 2. Biometric Template Protection Techniques

Future iterations can incorporate biometric cryptosystems or cancelable biometrics to ensure that raw biometric data is never exposed, even in the event of a data breach. This would align the system with advanced privacy-preserving authentication frameworks.

### 3. Blockchain-Enabled Audit Trails

Incorporating blockchain technology can ensure tamper-proof audit trails for biometric access logs. This would be beneficial in forensic and compliance scenarios, especially in industries like healthcare, finance, and defense.

### 4. Adaptive Authentication Mechanisms

The system can be enhanced with intelligent access control mechanisms that adjust authentication requirements based on user behavior, location, and device trust level. Such context-aware security can further reduce false positives and prevent unauthorized access.

### 5. Edge Computing Integration

Future deployments could consider edge devices for processing biometric data locally, reducing latency and dependence on constant cloud access. This is particularly relevant for mobile and IoT-based implementations.

### 6. Scalability and Load Balancing

Future work can focus on enhancing the system's ability to handle large-scale user databases with optimized fingerprint matching algorithms and dynamic load balancing across authentication servers.

### 7. User-Friendly Interfaces and Accessibility

Improving the system’s UI/UX and ensuring accessibility for individuals with disabilities (e.g., voice-based or gesture-based controls) can promote inclusivity and adoption.

## 8. Formal Compliance with Global Standards

Future enhancements can aim for compliance with international security standards such as ISO/IEC 30107 (Biometric Presentation Attack Detection) and GDPR for data protection and privacy assurance

## 10. Bibliography

[1] C. Neuman, S. Hartman, K. Raeburn, "The kerberos network authentication service (v5)," RFC 4120, 2005.

[2] "OAuth Protocol." [Online]. Available: http://www.oauth.net/

[3] "OpenID Protocol." [Online]. Available: http://openid.net/

[4] G. Wettstein, J. Grosen, and E. Rodriguez, "IDFusion: An open architecture for Kerberos based authorization," Proc. AFS and Kerberos Best Practices Workshop, June 2006.

[5] A. Kehne, J. Schonwalder, and H. Langendorfer, "A nonce-based protocol for multiple authentications," ACM SIGOPS Operating System Review, vol. 26, no. 4, pp. 84–89, 1992.

[6] B. Neuman and S. Stubblebine, "A note on the use of timestamps as nonces," Oper. Syst. Rev., vol. 27, no. 2, pp. 10–14, 1993.

[7] J. Astorga, E. Jacob, M. Huarte, and M. Higuero, "Ladon : endto-end authorisation support for resource-deprived environments," IET Infomration Security, vol. 6, no. 2, pp. 93–101, 2012.

[8] S. Zhu, S. Setia, and S. Jajodia, "LEAP: efficient security mechanisms for large-scale distributed sensor networks," Washington D.C., USA, October 2003, pp. 62–72.

[9] A. Perrig, R. Szewczyk, D. Tygar, V. Wen, and D. Culler, "SPINS: security protocols for sensor networks," ACM Wireless Networking, vol. 8, no. 5, pp. 521–534, 2002.

[10] P. Kaijser, T. Parker, and D. Pinkas, "SESAME: The solution to security for open distributed systems," Computer Communications, vol. 17, no. 7, pp. 501–518, 1994.

[11] G. Wettstein, J. Grosen, and E. Rodriguez, "IDFusion: An open architecture for Kerberos based authorization," Proc. AFS and Kerberos Best Practices Workshop, June 2006.

[12] M. Walla, “Kerberos explained,” Windows 2000 Advantage Magazine, 2000. [13] Q. Jiang, J. Ma, X. Lu, and Y. Tian, “An efficient two-factor user authentication scheme with unlinkability for wireless sensor networks,” Peer-to-Peer Networking and Applications, vol. 8, no. 6, pp. 1070–1081, 2015. [14] O. Althobaiti, M. Al-Rodhaan, and A. Al-Dhelaan, “An efficient

56

biometric authentication protocol for wireless sensor networks,” International Journal of Distributed Sensor Networks, vol. 2013, pp. 1–13, 2013, Article ID 407971, http://dx.doi.org/ 10.1155/2013/407971.

[15] K. Xue, C. Ma, P. Hong, and R. Ding, “A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks,” Journal of Network and Computer Applications, vol. 36, no. 1, pp. 316 – 323, 2013.

[16] M. Turkanovic, B. Brumen, and M. Holbl, “A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the internet of things notion,” Ad Hoc Networks, vol. 20, pp. 96 – 112, 2014. [17] M. Park, H. Kim, and S. Lee, “Privacy Preserving Biometric-Based User Authentication Protocol Using Smart Cards,” in 17th International Conference on Computational Science and Engineering, Chengdu, China, 2014, pp. 1541–1544. [18] P. K. Dhillon and S. Kalra, “A lightweight biometrics based remote user authentication scheme for IoT services,” Journal of Information Security and Applications, vol. 34, pp. 255 – 270, 2017.

[19] S. D. Kaul and A. K. Awasthi, “Security Enhancement of an Improved Remote User Authentication Scheme with Key Agreement,” Wireless Personal Communications, vol. 89, no. 2, pp. 621–637, 2016.

[20] D. Kang, J. Jung, H. Kim, Y. Lee, and D. Won, “Efficient and Secure Biometric-Based User Authenticated Key Agreement Scheme with Anonymity,” Security and Communication

Networks, vol. 2018, pp. 1–14, 2018, Article ID 9046064, https://doi.org/10.1155/2018/9046064.

[21] D. Dolev and A. C. Yao, "On the security of public key protocols," IEEE Transactions on Information Theory, vol. 29, no. 2, pp. 198–208, 1983.

[22] A. K. Das, "A secure and robust temporal credential-based three-factor user authentication scheme for wireless sensor networks," Peer-to-Peer Networking and Applications, vol. 9, no. 1,
pp. 223–244, 2016.

[23] "A secure and effective biometric-based user authentication scheme for wireless sensor networks using smart card and fuzzy extractor," International Journal of Communication Systems, vol. 30, no. 1, pp. 1–25, 2017.

57

[24] C. T. Li, C. Y. Weng, and C. C. Lee, "An advanced temporal credentialbased security scheme with mutual authentication and key agreement for wireless sensor networks," Sensors, vol. 13, no. 8, pp. 9589–9603, 2013.

[25] D. He, N. Kumar, and N. Chilamkurti, "A secure temporal-credentialbased mutual authentication and key agreement scheme for wireless sensor networks," in International Symposium on Wireless and pervasive Computing (ISWPC), Taipei, Taiwan, 2013, pp. 1–6.

[26] M. Turkanovic and M. Holbl, "An improved dynamic password-based user authentication scheme for hierarchical wireless sensor networks," ELEKTRONIKA IR ELEKTROTECHNIKA, vol. 19, no. 6, pp. 109 – 116, 2013. [27] R. Amin and G. P. Biswas, "A secure light weight scheme for user authentication and key agreement in multi-gateway based wireless sensor networks," Ad Hoc Networks, vol. 36, pp. 58–80, 2016.

[28] C.-C. Chang and N.-T. Nguyen, "An Untraceable Biometric-Based Multi-server Authenticated Key Agreement Protocol with Revocation," Wireless Personal Communications, vol. 90, no. 4, pp. 1695–1715, 2016.

[29] Z. Xia, C. Yuan, R. Lv, X. Sun, N. N. Xiong, and Y. Shi, "A Novel Weber Local Binary Descriptor for Fingerprint Liveness Detection," IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2018, doi: 10.1109/TSMC.2018.2874281.

[30] C. Yuan, X. Sun, and Q. M. J. Wu, "Difference co-occurrence matrix using BP neural network for fingerprint liveness detection," Soft Computing, vol. 23, no. 13, pp. 5157–5169, 2019.

[31] W. Yang, S. Wang, J. Hu, G. Zheng, and C. Valli, "Security and Accuracy of Fingerprint- Based Biometrics: A Review," Symmetry, vol. 11, no. 2, 2019. [Online]. Available: https://www.mdpi.com/2073-8994/11/2/141

[32] X. Huang, X. Chen, J. Li, Y. Xiang, and L. Xu, "Further Observations on Smart-Card-Based Password-Authenticated Key Agreement in Distributed Systems," IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 7, pp. 1767–1775, 2014.