Enhancing the Security of Cloud Data through the use of Biometrics and Encryption Technology

MSc Research Project
MSc Cybersecurity

Shashank Nagaraj
Student ID: 21202834

School of Computing
National College of Ireland

Supervisor: Michael Prior

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Shashank Nagaraj		
Student ID:	21202834		
Programme:	MSc Cybersecurity	**Year:**	2023
Module:	MSc Research Project		
Supervisor:	Michael Prior		
Submission Due Date:	14/08/2023		
Project Title:	Enhancing the security of cloud data through the use of biometrics and encryption technology		
Word Count:	5500	**Page Count**	21

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Shashank Nagaraj

Date: 14/02/2023

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Table of Contents

1 Introduction 2
2 Related Work 2
2.1 Literature Review 3
2.1.1 Storage Options for Secure File Systems 3
2.1.2 Techniques for Encryption 4
2.1.3 Security and Integration of the Cloud 4
2.1.4 Biometric authentication 4
2.1.5 Compliance and Data Privacy 4
2.1.6 Dual-Layer Encryption 4
3 Research Methodology 5
3.1 Research Strategy: 5
3.2 Dataset of Choice: 5
3.3 Model Training & Validation: 6
3.4 Choice of Programming and Technologies: 6
3.5 Evaluation: 6
3.6 Weaknesses and Strengths: 6
3.7 Encryption Implementation & Testing: 7
4 Design Specification 8
4.1 A three-tiered architecture 9
4.2 Drive HQ's integration with cloud storage: 10
4.3 System of Notification: 10
5 Implementation 11
5.1 Data Storage and Management 11
5.2 Hybrid Encryption Mechanism 11
5.3 Frontend Development 11
5.4 Role-Based Data Access 11
5.5 Data Storage and Management 12
5.6 Cloud Integration 12
5.7 Notification System 12
5.8 Backend Database 12
5.9 Synergy Between Flask and the Frontend 13
6 Evaluation 13
6.1 Comprehensive Analysis of Results 13
6.2 Implications from an Academic Perspective 13
6.3 Implications from a Practitioner Perspective 13
7 Experiment / Case Study 1 14
8 Experiment / Case Study 2 16
8.1 Discussion 17
9 Conclusion and Future Work 18
10 References 19

Enhancing the Security of Cloud Data through the use of Biometrics and Encryption Technology

Shashank Nagaraj
21202834

Abstract

Securing cloud data is still extremely significant in a time when data breaches are happening more frequently. The goal of this study is to improve the security of cloud data storage by exploring the interface between biometric authentication and encryption technologies. A robust system was created using a dataset of fingerprints obtained from Kaggle. It consists of three interactive webpages for different user roles: admin, data owner, and data user. This research inventively reduces risks related to password weaknesses, phishing attempts, and other common dangers by integrating RSA and AES encryption methods with fingerprint identification. The paper assesses how this hybrid verification strategy improves cloud login security and offers suggestions for developing more reliable systems in the cybersecurity environment.

1 Introduction

We now store and access data differently because of the growing popularity of cloud technology. Even if these platforms are flexible and convenient, fraudsters continue to make unrelenting attempts to compromise them. A common security precaution that has historically been the weakest link and vulnerable to assaults is the use of passwords. Transcending conventional password-based systems is the foundation of this investigation **(Manoj Tyagi, 2019).** The goal is to create a more robust layer of security by combining the distinctive but complementary strengths of biometrics and encryption.

A thorough cloud security mechanism was designed using the fingerprint dataset from Kaggle. This system functions as a practical example of our hybrid verification method, incorporating the responsibilities of an admin, a data owner, and a data user**.** The RSA encryption system, which safeguards all uploaded files and fingerprint data, is at the core of this method. The data is first encrypted using AES before being further secured by encrypting the AES key with RSA in situations where RSA's usefulness may be constrained by file size **(Ming Ni, 2020)**.

This study is focused on one key question: To what extent can a hybrid verification method that combines biometrics and encryption for cloud logins mitigate the complex problems of password vulnerabilities, phishing attacks, and other impending security threats? This paper explores the complex webs of cybersecurity in search of solutions, paving the path for more dependable digital systems.

2 Related Work

The study highlights data administration, data ownership, and secure data access for users while presenting a thorough investigation of a secure data sharing system implemented within the Anaconda environment. The system uses RSA and AES encryption in combination to provide strong privacy and confidentiality. The research is put into context in the following literature review by looking at related studies in the areas of secure data sharing, encryption, and biometric authentication.

The research "Cloud-based biometrics processing for privacy-preserving identification" provides important insights in the pursuit of secure data sharing and access control. To simplify secure identification operations over encrypted databases, this study suggests a successful biometric identification outsourcing scheme. Although different in scope, the approach's focus on efficiency and privacy protection is in line with the objectives of the ongoing research. Additionally, the methodology's use of biometric characteristics is consistent with the data user authentication strategies suggested in the current study **(Changhee Hahn, 2017)**.

The study by " Attribute-Based Secure Data Sharing with Hidden Policies in Smart Grid " explores attribute-based data sharing and access control and offers useful insights. The ability of the data owner to assign attributes and manage file access in the current research is consistent with the mechanisms for controlling access to data introduced in this work. The study's focus on covert policies and attribute-based encryption complements the suggested data ownership module and adds to the larger discussion of secure data sharing mechanisms **(Junbeom Hur, 2013).**

This survey thoroughly examines cryptographic methods and biometric-based authentication strategies, demonstrating the authentication mechanism built into the data user access procedure. The research's biometric authentication component is well supported by the study's discussion of various biometric traits, encryption techniques, and security issues (**Colin Soutar, 1999)**.

2.1 Literature Review

Making sure sensitive data is secure and confidential has become of utmost importance in the digital age. Innovative solutions are necessary to reduce the risks associated with unauthorized access and breaches as organizations depend more and more on cloud storage and data sharing. The research and technologies that are currently available in the fields of data security, cloud integration, and secure file system storage are examined in this literature review.

2.1.1 Storage Options for Secure File Systems

Due to their potential to protect sensitive information, secure file system storage solutions have drawn considerable attention. The importance of attribute-based access control in managing data access permissions is highlighted. This is in line with the architecture suggested in this work, where data owners assign users attributes to control file access (**Jiyi Wu, 2010)**.

2.1.2 Techniques for Encryption

For the confidentiality of data to be maintained, encryption is essential. The research highlights how well AES encryption protects data during storage and transmission. The proposed solution incorporates AES encryption for file content to ensure that the data is impenetrable even in the event of unauthorized access **(Taufik Hidayat, 2020)**.

2.1.3 Security and Integration of the Cloud

Data management has been revolutionized by cloud storage, but it also raises security issues. The importance of robust authentication mechanisms is highlighted investigation of secure cloud integration strategies. These results are in line with the use of multi-factor authentication and RSA encryption of fingerprint images in this work, which improves data security in cloud environments **(Md. Alamgir Hossain, 2020)**.

2.1.4 Biometric authentication

Because of its reliability, biometric authentication is becoming more popular. This trend is followed by the proposed solution, which makes sure that only authorized users with proper biometric credentials can access the system by using fingerprint images for user authentication **(Md. Alamgir Hossain, 2020)**.

2.1.5 Compliance and Data Privacy

For regulatory compliance, it is essential to ensure data privacy. These issues are directly addressed by the attribute-based access control and encryption hierarchy used in this work, which supports data privacy and regulatory compliance **(Md. Alamgir Hossain, 2020)**.

2.1.6 Dual-Layer Encryption

(Mr. Abhishek Guru, 2021) research provides support for the concept of dual-layer encryption as it is used in this solution. Their research looks at the more secure advantages of self-encrypting encryption keys. This method fits with the suggested encryption hierarchy because it encrypts AES keys with RSA encryption, adding an extra layer of security.

Author(s)	**Year**	**Key Focus**	**Key Findings/Insights**	**Relevance to Current Study**
Mr. Abhishek Guru	2021	Dual-Layer Encryption	Advantages of self-encrypting encryption keys	Encryption of AES keys with RSA, adding an extra layer of security
Taufik Hidayat	2020	Techniques for Encryption	AES encryption's importance in data protection	AES encryption use for file content
Md. Alamgir Hossain (first ref)	2020	Security and Integration of the Cloud	Importance of robust authentication mechanisms	Multi-factor authentication; RSA encryption of fingerprint images
Md. Alamgir Hossain (second ref)	2020	Biometric authentication	Rising reliability of biometric authentication	Use of fingerprint images for user authentication
Md. Alamgir Hossain (third ref)	2020	Compliance and Data Privacy	Importance of data privacy for regulatory compliance	Attribute-based access control; encryption hierarchy
Changhee Hahn	2017	Cloud-based biometrics processing for privacy-preserving identification	Secure identification over encrypted databases	Focus on efficiency and privacy; use of biometric characteristics

3 Research Methodology

3.1 Research Strategy:

The quantitative research strategy was selected because of its unambiguous nature, which enables precise measurement of the effectiveness and dependability of our hybrid verification system. This method made it easier to statistically validate our findings, guaranteeing their objectivity and reproducibility.

3.2 Dataset of Choice:

Data Source: Limited to the SOCOFing dataset from Kaggle **(ruizgara, 2018).**
The fingerprint images of various people from Kaggle were used as the dataset for fingerprint training. This dataset offers a broad range of biometric information that is perfect for creating and testing our hybrid system. This dataset's diversity and real-world nature, which makes it representative of potential application scenarios, contribute to its dependability.

3.3 Model Training & Validation:

Machine learning models require rigorous training and validation to ensure accuracy. The SOCOFing dataset was split, with a significant portion allocated for training and a separate subset reserved for validation. This validation ensured the model's predictions for fingerprint matches were reliable **(Lee, 2018).**

3.4 Choice of Programming and Technologies:

- Python: This language was favoured due to its vast library ecosystem and ease of integration with various systems.
- Flask: A micro web framework that facilitates quick and efficient web development. It’s lightweight and is known for its compatibility with Python, making it an ideal choice for this project.
- HTML, CSS, JS: Chosen for frontend development to create responsive and interactive web interfaces.
- Drive HQ & FTP: To facilitate cloud storage and secure file transfer mechanisms.
- MySQL: For data storage and easy retrieval capabilities.

3.5 Evaluation:

The effectiveness of the hybrid system is evaluated through the simulation of actual-world scenarios. The accuracy and security of the authentication system were evaluated based on the matching scores from the prediction model.

3.6 Weaknesses and Strengths:

Strengths:

- Security: The hybrid system guards against weaknesses in conventional passwords and potential phishing attacks by combining biometrics with encryption.
- Individual-centric verification is made possible by biometrics, preventing unauthorized access.

Limitations:

- Data Integrity: The integrity of the biometric data is crucial to the functioning of the system. Any corruption may present difficulties.

- Data Storage: Privacy concerns arise when biometric data is stored, even when it is encrypted. Adequate steps should be taken to stop violations.

3.7 Encryption Implementation & Testing:

In the realm of cybersecurity, especially when addressing cloud storage vulnerabilities, encryption is the linchpin that guarantees data integrity and confidentiality. Our approach adopted a dual-layer encryption mechanism, both sophisticated and efficient, to ensure the sanctity of the data.

AES (Advanced Encryption Standard), a symmetric encryption algorithm, was the primary choice for encrypting the data. Its allure stems from several pivotal factors. Firstly, its speed and efficiency are unmatched when it comes to encrypting substantial data files, making it a natural choice for a project that deals with sizeable data. AES's resilience, with key lengths ranging from 128 to 256 bits, ensures a formidable defense against brute-force attacks. Moreover, its design as a block cipher, adept at encrypting chunks of data, further solidified its position as the first line of encryption defense for our project **(Taufik Hidayat, 2020)**.

However, the symmetric nature of AES, where the same key is used for both encryption and decryption, presents a critical challenge: secure key transmission. If an adversary intercepts this key during transmission, they can decrypt the data, rendering the encryption moot.

Enter **RSA (Rivest–Shamir–Adleman)**, an asymmetric encryption algorithm. The brilliance of RSA lies in its dual-key system: a public key for encryption and a distinct private key for decryption. Integrating RSA into our encryption scheme addressed the challenge posed by AES. The process was elegant in its simplicity. After encrypting the data using AES, we encrypted the AES key itself using RSA. This approach ensured that the AES key, critical for data decryption, could be securely transmitted using the recipient's RSA public key. Only the recipient, in possession of the corresponding RSA private key, could then decrypt and access the original AES key. RSA is not only a bulwark against cryptographic attacks but also offers versatility, laying the foundation for potential system evolutions, such as the integration of digital signatures **(Manoj Tyagi, 2019)**.

In culmination, this hybrid encryption methodology combined the best of both algorithms. The speed and efficiency of AES ensured rapid encryption of large datasets, while the security and versatility of RSA guaranteed the safe transmission of the AES key. Post-implementation, we subjected the system to rigorous simulations of breach attempts. The objective was clear: validate the robustness of this dual encryption strategy. These tests were pivotal, affirming our confidence in the system's capability to effectively shield data from myriad threats **(Ming Ni, 2020)**.

To ensure the system was user-friendly and met real-world requirements, it was tested by potential end-users.

4 Design Specification

Designing a reliable system architecture plays an important role in the field of cybersecurity, especially when combining different technologies like biometrics and encryption.

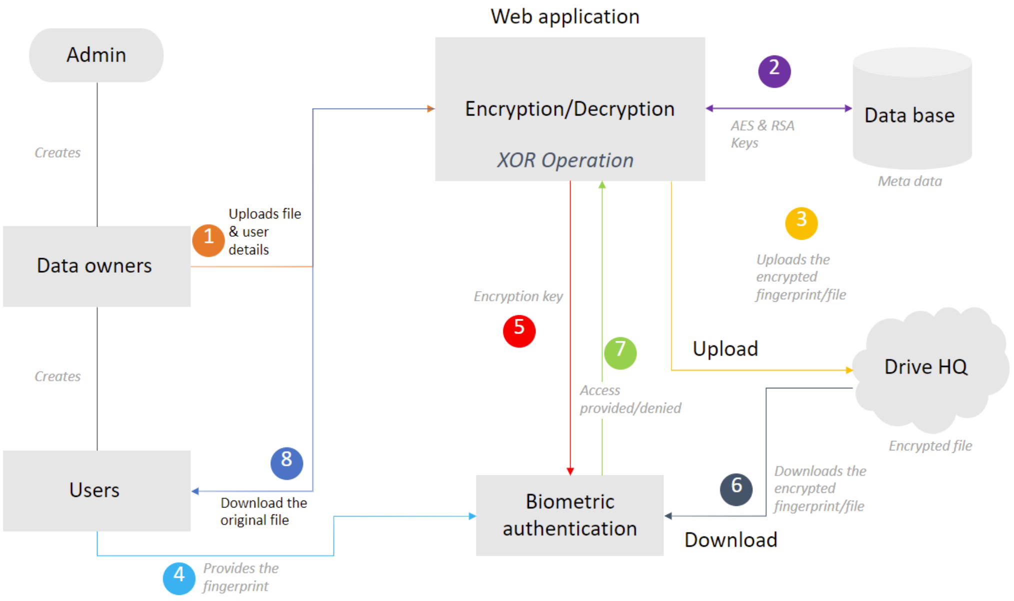


Figure 1. Proposed Architecture.

Step 1: Uploading the Data Owner's File and Fingerprints

- After entering their login information, the data owner is given the choice of uploading either a file or the fingerprint image.
- Metadata, such as file name, date, and remarks, can be added during file upload.
- The fingerprint image is first encrypted using AES for security before being uploaded to the cloud, and then it is encrypted again using RSA using the AES encryption key. This guarantees the security of the fingerprint, even on a third-party cloud platform.

Step 2: Database Key Storage and Encryption

- The data owner's uploaded file is first encrypted with AES. A second layer of security is then added by using RSA to encrypt the actual AES encryption key.
- The relevant file metadata as well as the RSA-encrypted AES key are both kept in the MySQL database.

Step 3: Upload an encrypted file to the cloud.

- The AES-encrypted file is uploaded to the Drive HQ cloud storage system using the FTP library. This guarantees that the file's original content cannot be read even if someone gains unauthorized access to Drive HQ.

Step 4: Login with User Fingerprint

- Users of the data must upload a fingerprint scan along with their provided email ID to log in. For biometric verification, this image will be used.

Step 5: Retrieve the encryption key from the database.

- The system retrieves the file's associated RSA-encrypted AES key from the MySQL database after a successful login attempt.

Step 6. Encrypted fingerprint verification.

- Downloaded from the Drive HQ cloud platform is the user's previously saved, encrypted fingerprint.
- The original AES-encrypted fingerprint is recovered by decrypting it with the RSA private key. The original fingerprint is then recovered by decrypting it with the AES key.

Step 7: Fingerprint Similarity Check

- The system compares the supplied fingerprint with the stored fingerprint using a trained prediction model. A similarity or matching score is then calculated.
- The user is granted access if their score is higher than the cutoff (for example, 80%). Otherwise, entry is prohibited.

Step 8: Accessing and Decrypting the Original File

- The user can view the list of files available for download after successfully authenticating, subject to any restrictions set by the data owner.
- The system first gets the encrypted file from Drive HQ in order to download it.
- The file is decrypted so that the user can access it in its original form using the decryption key (which is produced by performing an XOR operation between the attribute and the RSA private key).

4.1 A three-tiered architecture

Overview: To improve modularity and scalability, this design paradigm divides the system into three main layers, each of which is in charge of specific functions.

Presentation layer:

- Function: It serves as the user interface and offers a visual interface for communication.
- Technologies Used: To create user-friendly and responsive interfaces, HTML, CSS, and JavaScript are used.

Components:

- Manages data owners and views files using the admin interface.
- Manages files, users, and domain attributes through the data owner interface.
- Accesses files based on assigned attributes using the data user interface.

Logic layer:

- Function: As the system's operational hub, the logic layer processes data, communicates with storage systems, manages encryption and decryption, and directs user requests.
- Used technology: The mainstay, Flask, a Python-based micro web framework, converts front-end interactions to back-end operations.

Components:

- Files are encrypted using AES, and the AES key is then encrypted using RSA by the encryption module.
- Utilizes stored data and uploaded fingerprints to verify users using biometric verification.
- Email notifications are sent using SMTP by the notification module.

The Data Layer

- Function: It acts as the data repository, providing the security and integrity of the data.
- Technologies: MySQL manages data storage, while Anaconda provides the environment.

Components:

- Credentials, attributes, and fingerprints that have been encrypted.
- File Data: Encrypted files that data owners have uploaded.
- Configuration Data: Consists of settings like Drive HQ access information and SMTP credentials.

4.2 Drive HQ's integration with cloud storage:

- Overview: Drive HQ is used by the system for encrypted file and fingerprint storage because it recognizes the importance of remote storage solutions.

- Function: Encrypted data is safely stored and retrieved.
- Implementation: Python's FTP library makes data transfers easier.
- To ensure security even if accessed, all data that is stored is encrypted.
- Data access for authorized users is seamless thanks to integration with the Logic Layer.

4.3 System of Notification:

- Overview: It's important to communicate with users, especially when sending notifications or confirmations.

- Notify users of system updates, such as new user creation.
- Implementation: Uses SMTP through a protected Google account.
- incorporated within the Logic Layer to automatically send emails in response to certain triggers, such as the addition of a user by the data owner.

5 Implementation

5.1 Data Storage and Management

Anaconda was the project's main data management platform, offering a structured and effective method of handling datasets. The fingerprint data was one of the datasets that came from Kaggle. The data was securely stored and organized in the Anaconda environment in a way that was optimized for quick and effective retrieval.

5.2 Hybrid Encryption Mechanism

Due to its effectiveness in handling larger datasets, AES (Advanced Encryption Standard) was initially used to encrypt the files. The AES encryption keys were further protected using RSA encryption after being encrypted with AES. The data would remain inaccessible even if one encryption layer were compromised thanks to the superior security provided by this dual-layer encryption **(Ye Liu, 2018)**.

5.3 Frontend Development

- HTML, CSS, and JavaScript were used to create the user interfaces for the Administrator, Data Owner, and Data User.
- To ensure that the layout and content of the web pages were well-organized, HTML was used.
- When used to stylize the web pages, CSS provided a simple user interface across every page.
- JavaScript (JS): By enabling immediate responses and validations, this scripting language was used to create dynamic interactions on web pages, improving the user experience.

5.4 Role-Based Data Access

Three unique web-based user interfaces were developed (Rubina Ghazal, 2020):

- Admin - The platform's admin interface provided extensive control over data owners and users. The admin had complete control over everything, including the ability to monitor all users, add or edit data owner details, view all files without actually accessing their contents, and change their own access credentials.

- Data Owner - Once authenticated, data owners could manage users, assign user-specific attributes, upload files, and take care of domain settings using the data owner interface. The ability of data owners to encrypt user fingerprint data with RSA, ensuring the security of biometric data while being stored in the cloud, was an important feature.

- Data User Interface: Users can access files through this portal, which was created for them. Their authentication required a matching fingerprint and an active email. The submitted fingerprint was compared to a stored fingerprint using a machine-learning model that had been trained on the Kaggle dataset. Access was granted if a high matching score (above 80%) was obtained. Depending on the permissions set by the data owner, users could view and download files after successfully logging in.

5.5 Data Storage and Management

- Data from Kaggle was downloaded, processed, and organized using Python's extensive library ecosystem in the Anaconda environment. Python connectors allowed for quick and secure CRUD (Create, Read, Update, Delete) operations by facilitating secure interactions with the MySQL database.

5.6 Cloud Integration

- Python was used to integrate the FTP library with Drive HQ for cloud storage, speeding up the secure transfer of encrypted files and biometric information between the local servers and the cloud platform.

5.7 Notification System

- Email notifications were sent to users via an SMTP (Simple Mail Transfer Protocol) configuration that was set up. This was done by setting up a special Google account, which improved the system's ability to stay in touch with its users without human intervention.

5.8 Backend Database

- MySQL was used as the backend database to store important system information, including user information, file metadata, encrypted keys, and more. The project's data storage needs were met by this relational database system, which was also scalable.

5.9 Synergy Between Flask and the Frontend

- Flask connected the Frontend and the Backend with ease. The framework was used to serve static files like CSS and JS, render HTML templates, and route requests. Flask served as the central component in the architecture of the entire system, managing data passed between user interfaces and the backend.

6 Evaluation

6.1 Comprehensive Analysis of Results

AES and RSA encryption methods were combined to create a layered security system. AES's ability for handling larger datasets, together with RSA's contribution to adding an additional layer of encryption for the AES keys, proven to be an effective in future against online dangers. This type of multilayer encryption not only represented improvement in data security measures, but it also set the stage for other cutting-edge strategies in the future.

Structured data access systems is used, project's split into the distinct roles of administrator, data owner, and data user. Data access was optimized using this role-based authentication technique while still being hierarchical and segregated. Such a method strengthens the barriers against future data breaches by inherently lowering the risks of unauthorized access.

Integration of fingerprint-based biometric authentication was another. The research demonstrated a high success rate in fingerprint verification using a Kaggle dataset as its benchmark. This strengthened the idea that problems that have long plagued traditional password systems may be solved practically and successfully by biometrics.

6.2 Implications from an Academic Perspective

The research, improves cybersecurity using the encryption and biometrics, is viewed from an academic perspective as an important work of research.

The use of the Kaggle dataset for fingerprint verification also offers an academic analysis of the importance of freely accessible datasets, providing insights into both potential advantages and drawbacks.

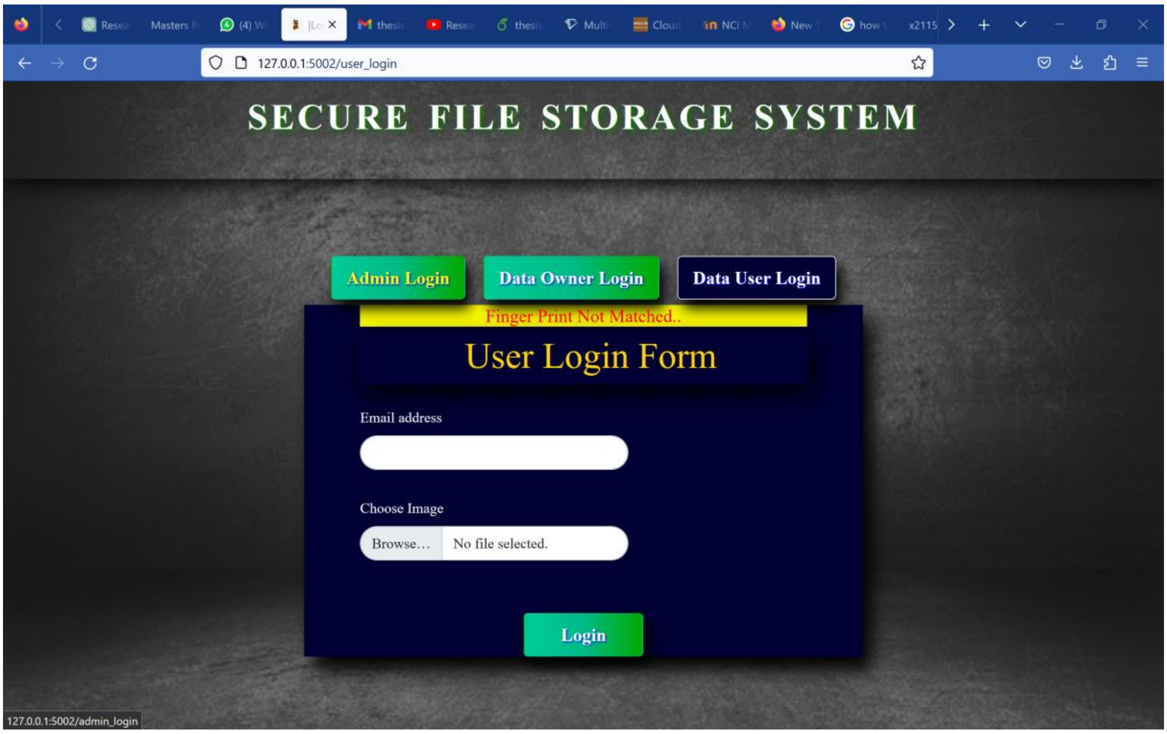
6.3 Implications from a Practitioner Perspective

The project's hybrid encryption framework encourages businesses to reconsider their data encryption methods. Such a technique provides improved security as well as potential solutions for encrypting large datasets.

The initial expenses needed for biometrics deployment may seem high in terms of costs. However, the long-term financial outcome looks positive when compared to the anticipated decline in losses caused by data breaches.

Furthermore, including modern security measures like these can improve an organization's market reputation in a time when data privacy is no longer a luxury but a need. It can encourage the development of user trust by developing a connection based on an assurance of security.

7 Experiment / Case Study 1


127.0.0.1:5002/user_login

SECURE FILE STORAGE SYSTEM

Finger Print Not Matched..

User Login Form

Email address

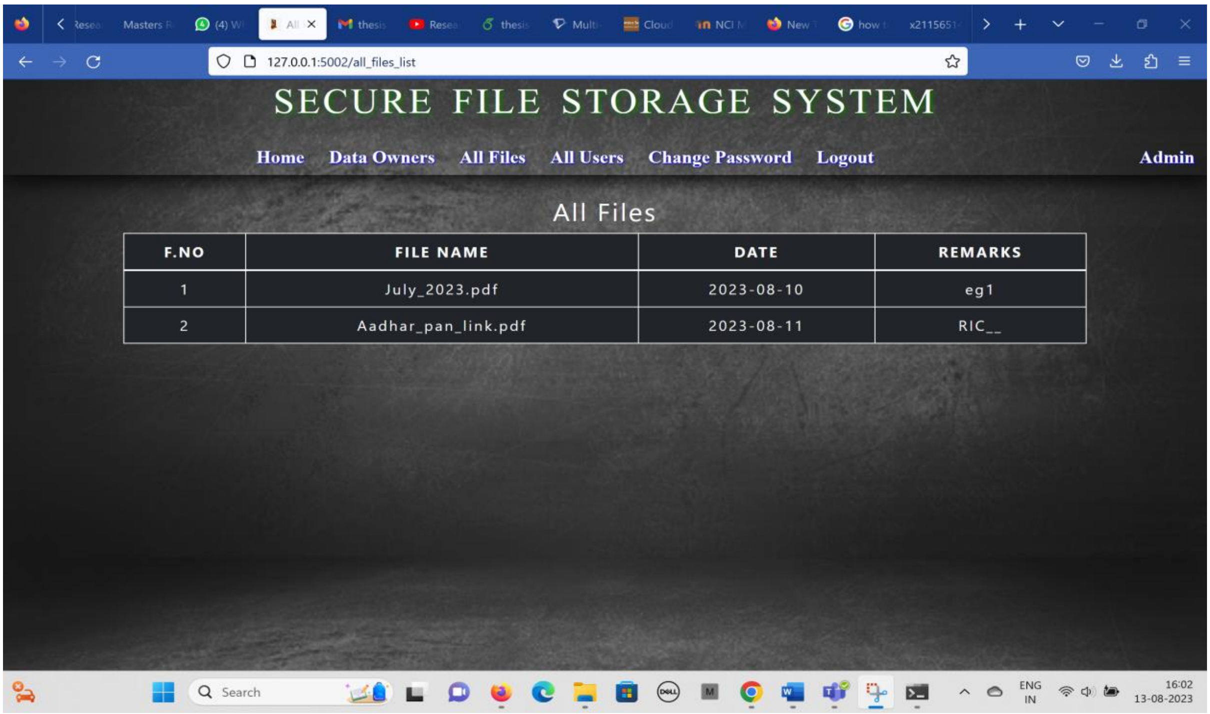
Choose Image

Browse… No file selected.

127.0.0.1:5002/admin_login

Figure 2. Access denied for fingerprint mismatch.

In this experiment, if wrong password or login ID is given by the admin, data Owner, for the cloud login or wrong finger print is given by the user then, access is denied.



127.0.0.1:5002/all_files_list

SECURE FILE STORAGE SYSTEM

Home Data Owners All Files All Users Change Password Logout Admin

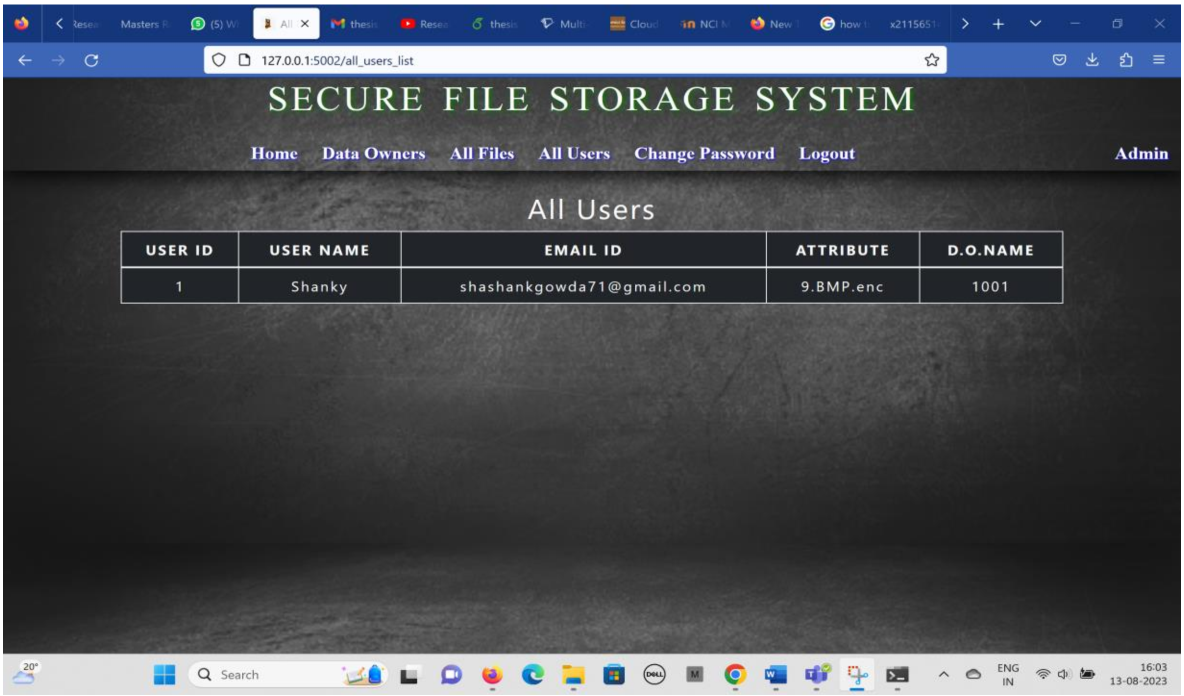
All Files

F.NO	FILE NAME	DATE	REMARKS
1	July_2023.pdf	2023-08-10	eg1
2	Aadhar_pan_link.pdf	2023-08-11	RIC__

16:02 13-08-2023

Figure 3. Files viewed by the administrator.

The admin can only view the files data and users' data but cannot access the files or edit the users.



127.0.0.1:5002/all_users_list

SECURE FILE STORAGE SYSTEM

Home Data Owners All Files All Users Change Password Logout Admin

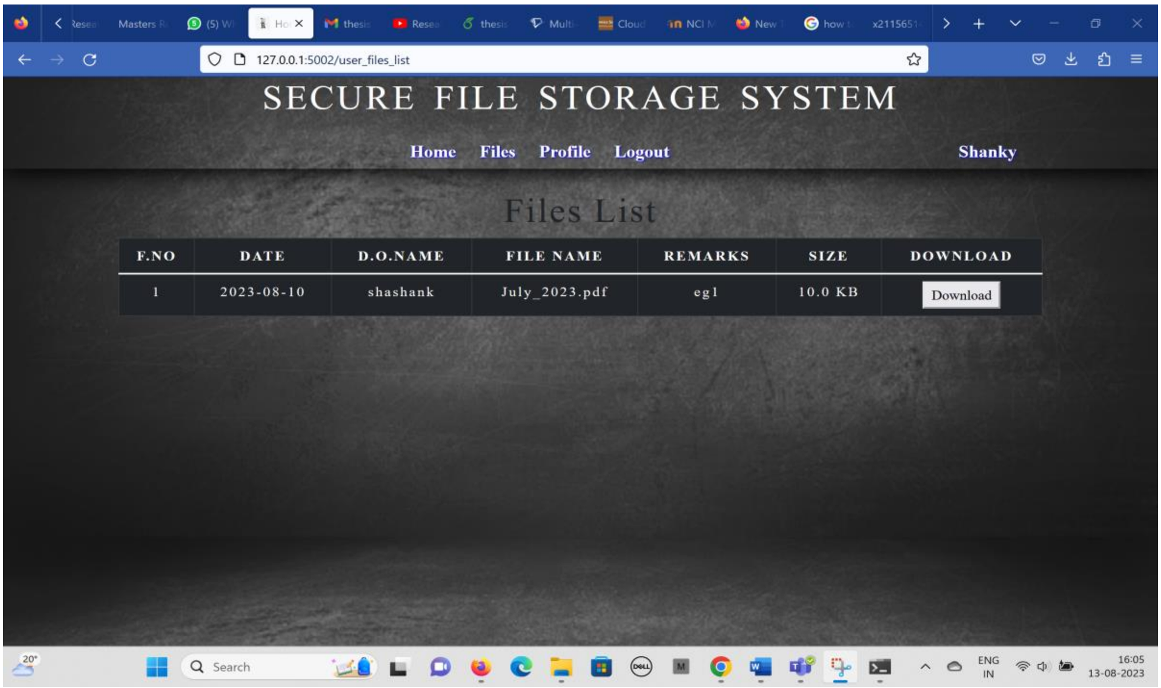
All Users

USER ID	USER NAME	EMAIL ID	ATTRIBUTE	D.O.NAME
1	Shanky	shashankgowda71@gmail.com	9.BMP.enc	1001

16:03 13-08-2023

Figure 4. All users page for admin.

The admin can only view the files details uploaded by the data owner and cannot view the file or alter the files.



127.0.0.1:5002/user_files_list

SECURE FILE STORAGE SYSTEM

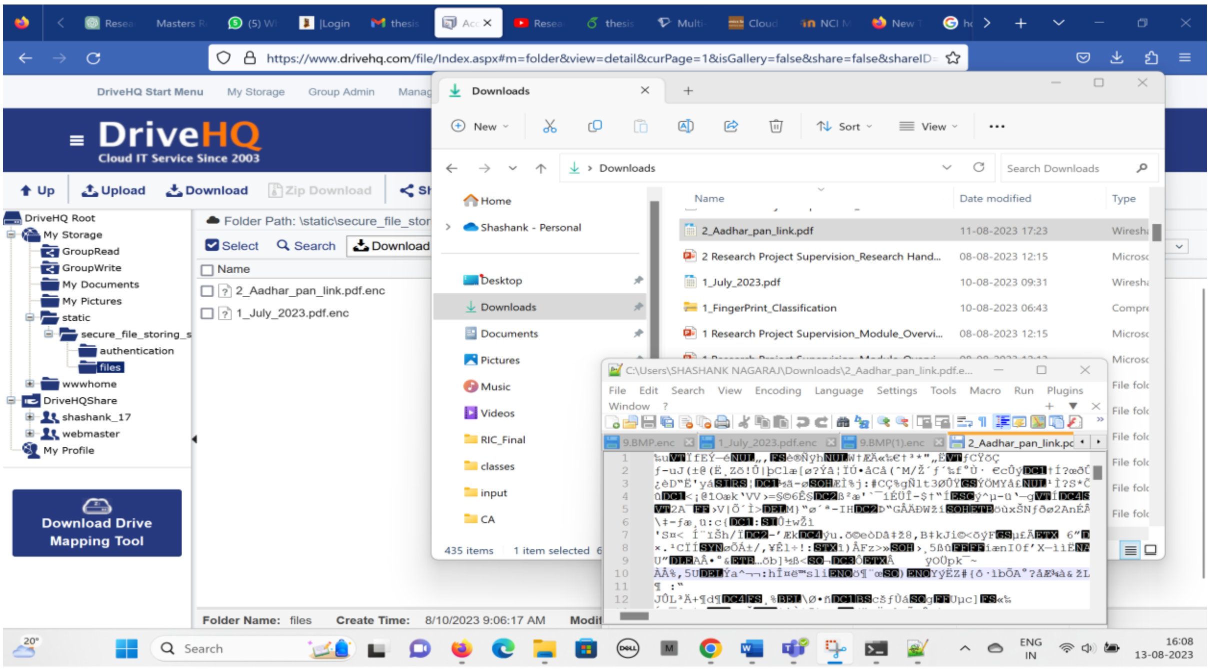
Files List

F.NO	DATE	D.O.NAME	FILE NAME	REMARKS	SIZE	DOWNLOAD
1	2023-08-10	shashank	July_2023.pdf	eg1	10.0 KB	Download

Figure 5. The file list view for user

The user can only download the file that are from the assigned domain and uploaded by the data owner.

8 Experiment / Case Study 2



https://www.drivehq.com/file/Index.aspx#m=folder&view=detail&curPage=1&isGallery=false&share=false&shareID=

Folder Path: \static\secure_file_stor

Name
2_Aadhar_pan_link.pdf.enc
1_July_2023.pdf.enc

Folder Name: files Create Time: 8/10/2023 9:06:17 AM

Name	Date modified	Type
2_Aadhar_pan_link.pdf	11-08-2023 17:23	Wiresh
2 Research Project Supervision_Research Hand...	08-08-2023 12:15	Microsc
1_July_2023.pdf	10-08-2023 09:31	Wiresh
1_FingerPrint_Classification	10-08-2023 06:43	Compre
1 Research Project Supervision_Module_Overvi...	08-08-2023 12:15	Microsc

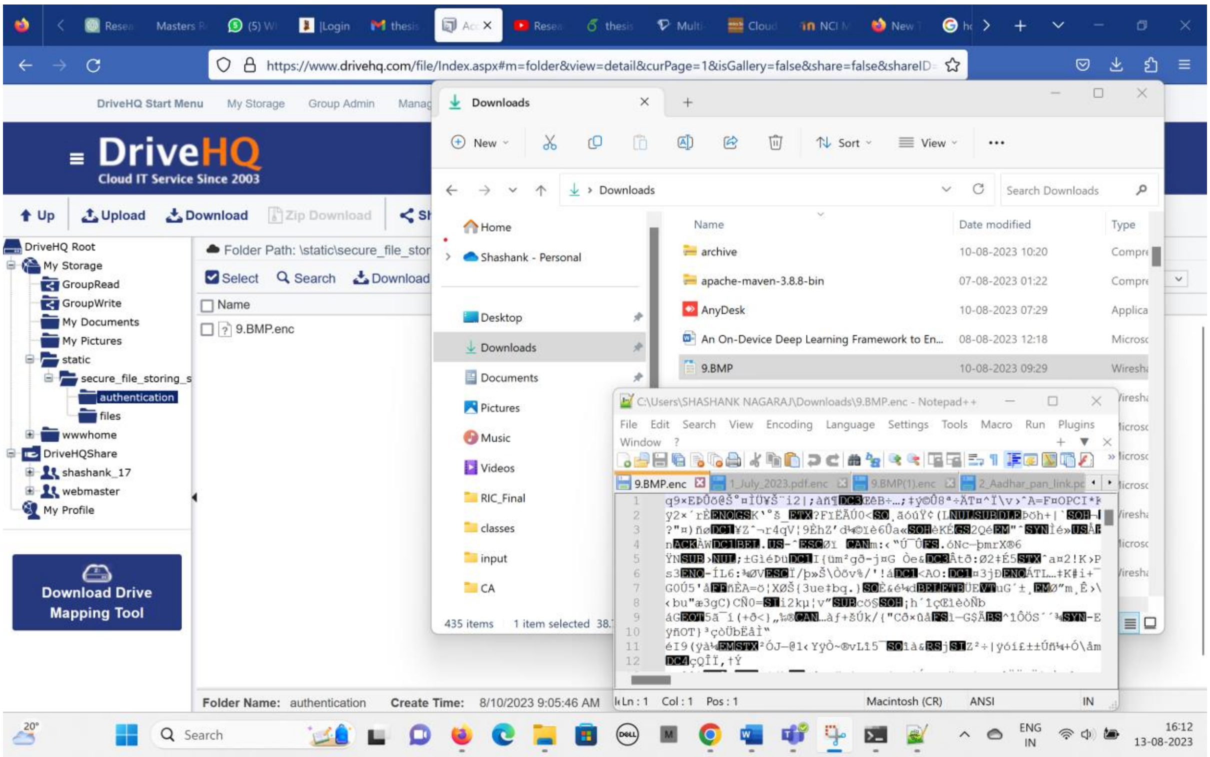
435 items 1 item selected

C:\Users\SHASHANK NAGARAJ\Downloads\2_Aadhar_pan_link.pdf.e...

File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
9.BMP.enc
1_July_2023.pdf.enc
9.BMP(1).enc
2_Aadhar_pan_link.pc

Figure 6. Encrypted file stored in the cloud.

The file stored on the cloud storage is an encryptd file therefore, cannot be accessed by anybody else.



Name	Date modified	Type
archive	10-08-2023 10:20	Compre
apache-maven-3.8.8-bin	07-08-2023 01:22	Compre
AnyDesk	10-08-2023 07:29	Applica
An On-Device Deep Learning Framework to En...	08-08-2023 12:18	Micros
9.BMP	10-08-2023 09:29	Wiresha

Figure 7. Encrypted fingerprint stored in the cloud.

The encrypted fingerprint stored inside the cloud.

8.1 Discussion

The main goal of this study was to investigate how biometrics, primarily fingerprint verification, and encryption technology, which includes both RSA and AES encryption methods, could be used to improve cloud data security.

1. Key observations

Hybrid Security: The hybrid model's multi-tiered security layer was made possible by design. This is clear from the encryption method, which involved first RSA-encrypting the AES key before using AES to encrypt larger information. A strategy with two layers raises the bar automatically against potential cyber threats.

User Role Segmentation: The separation of users into the categories of Administrator, Data Owner, and Data User enabled role-based access while establishing an inherent hierarchy and additional layers of protection. The distinct rights assigned to each role ensured data compartmentalization and minimized exposure.

Biometric authentication: The vulnerability typically associated with password-only systems was mitigated by adding fingerprints as an additional layer of authentication. This integration is a significant step towards a more secure system because biometrics are distinctive and more difficult to copy or fake.

2. Critical Evaluation

Dataset Restrictions: Although the Kaggle dataset served as a foundation for fingerprint recognition, its diversity and thoroughness would not have adequately captured a world population's variation. More varied datasets may be useful in later iterations to assure greater accuracy.

Encryption Overhead: Using both AES and RSA to handle various data quantities may result in computational costs. There is a chance of system latency or delayed replies in settings with real-time, high-frequency data access.

3. Improvements and Suggestions:

Expanded Biometrics: As biometrics become more widely used, combining several biometric modalities (like facial or iris recognition) can provide even more reliable verification procedures.

Optimized Encryption: Researching lightweight encryption techniques that are especially suited for cloud situations may be able to help improve system performance even more.

User activity Analytics (UBA): In addition to using biometrics, implementing UBA capabilities could aid in spotting unusual activities and add an additional layer of protection by continuously monitoring user activity.

Backups & Redundancy: To enhance data resilience, future iterations can also take automated encrypted backups into consideration.

The architecture of the system undoubtedly advanced cloud data security, but there is always opportunity for improvement due to the constantly changing cyber threat landscape and quickening technological progress. The proposed architecture has laid a promising foundation, but continual iteration, considering feedback loops and newly emerging threats, is essential to preserve its resilience.

9 Conclusion and Future Work

This study demonstrated the effectiveness of combining encryption and biometric verification techniques to strengthen cloud data security. Our hybrid solution successfully countered phishing attempts and other threats while mitigating common password-based security flaws. The study created a more robust security paradigm by using fingerprint data in conjunction with dual AES and RSA encryption layers. To increase system robustness going forward, it would be wise to investigate the incorporation of additional biometric modalities, including facial or voice recognition. It will also be extremely helpful to evaluate the scalability and effectiveness of this strategy in actual, high-traffic settings. This research has paved a promising road toward more secure cloud storage solutions, which is necessary given the swift growth of cyber threats.

10 References

Ashish Singh, K. C., n.d. *Cloud security issues and challenges: A survey.* India, Science Direct.
Byun, K. B. a. H., NA. *Combination of Fingerprint and Password system.* Korea, Sangmyung Universit.

Changhee Hahn, H. S. J. H., 2017. *Cloud-based biometrics processing for privacy-preserving identification.* CHINA, IEEE.

Colin Soutar, D. R. A. S. R. G. B. V. K., 1999. *Biometric Encryption.* USA, Bioscrypt Inc. (formerly Mytec Technologies Inc.).

Dinesh, A. & Bijoy, K. E., 2017. *Privacy preserving speech, face and fingerprint based biometrie authentication system using secure signal processing.* Mumbai, IEEE.

Jiyi Wu, L. P. X. G. Y. W. J. F., 2010. *Cloud Storage as the Infrastructure of Cloud Computing.* CHINA, IEEE.

Junbeom Hur, 2013. *Attribute-Based Secure Data Sharing with Hidden Policies in Smart Grid.* CHINA, IEEE.

Keiron O'Shea, R. N., 2015. *An Introduction to Convolutional Neural Networks.* NA, cornell university.

Khanezaei, N. & Hanapi, Z. M., 2014. *A framework based on RSA and AES encryption algorithms for cloud computing services.* NA, IEEE.

Lee, B., 2018. *Fingerprint Recognition.* [Online]
Available at: https://www.kaggle.com/code/kairess/fingerprint-recognition
[Accessed 29 july 2023].

Manoj Tyagi, M. M. B. M., 2019. Analysis and Implementation of AES and RSA for cloud. *International Journal of Applied Engineering Research.*

Md. Alamgir Hossain, M. A. A. H., 2020. *Improving cloud data security through hybrid verification technique based on biometrics and encryption system.* s.l., International Journal of Computers and Applications.

Ming Ni, Y. H. W. S. X. L., 2020. *Hybrid Encryption Algorithm Based on AES and RSA in File Encryption.* CHINA, International Conference on Frontier Computing .

Mr. Abhishek Guru, D. A. A., 2021. *AES AND RSA-BASED HYBRID ALGORITHMS FOR MESSAGE ENCRYPTION & DECRYPTION.* INDIA, Journal of Information Technology in Industry.

Rubina Ghazal, A. K. M. N. Q. B. R. A. R. S., 2020. *Intelligent Role-Based Access Control Model and Framework Using Semantic Business Roles in Multi-Domain Environments.* Hawaii, IEEE.

ruizgara, 2018. *Sokoto Coventry Fingerprint Dataset (SOCOFing).* [Online] Available at: https://www.kaggle.com/datasets/ruizgara/socofing [Accessed 28 July 2023].

Samar Zaineldeen, A. A., 2020. *Improved cloud data transfer security using hybrid encryption algorithm.* NA, Indonesian Journal of Electrical Engineering and Computer Science.

Taufik Hidayat, R. M., 2020. *A Systematic Literature Review Method On AES Algorithm for Data Sharing Encryption On Cloud Computing.* Indonesia, International Journal of Artificial Intelligence Research.

Ye Liu, W. G. W. F., 2018. *Application of AES and RSA Hybrid Algorithm in E-mail.* CHINA, IEEE.