WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Container-Based File Encryption and Retrieval System Approach Using RSA algorithm

[1].Mallikharjuna Rao. Y, [2.] Dr. M.Bhuvaneswari

1.PG Student ,**malliymr1435@gmail.com**
2. Associate Professor bhuvaneswari.mca@drmgrdu.ac.in
Department of Computer Applications
Dr. M.G.R. Educational and Research Institute, Chennai - 95

ABSTRACT:

This paper proposes a container-based file encryption and retrieval system leveraging the RSA (Rivest–Shamir–Adleman) algorithm for enhanced data security. The system comprises key modules for RSA key generation, file encryption, container management, and file retrieval. By encrypting files with RSA public keys and securely managing RSA private keys, the system ensures data confidentiality and integrity. This approach offers a robust and scalable solution for secure storage and access to sensitive files.

Keywords: RSA algorithm, file encryption, container-based storage, data security, key management, access control, public-key cryptosystem, secure retrieval, confidentiality, integrity.

I.INTRODUCTION:

This makes APFS a valuable target for digital forensics, since systems using RSA are widely used. APFS is a relativel file system that has not been fully analyzed and studied. Additionally, since it is a proprietary file system, the source code is not freely available, which hides the file system. Reverse engineering of the partial file system definition and architecture published. Because of its novelty and obscurity, it is an interesting topic for digital forensics. Data hidden in APFS has been studied, but so far no research involves detection of hidden data. investigating the possibility of automating the detection of changed data structures[1].

A study to understand the APFS file system was done in a pre-release of macOS 10.12 Sierra.This version is not compatible with the current version, but the underlying data structures have not changed significantly. Recovering lost or deleted files.The file system is an important part of computer forensics. This is calledcarving. There are tools for creating internal.data structures in file systems[2].
A partition consists of a single container, which can contain several partitions, such as logical volumes ,and this container contains the corresponding superblock (NXSB). One container contains multiple volumes with their matching superblocks (APSB). Both the container and the ewcontainer superblock refer to an object map (OMAP), which does not contain references to objects. A simplified overview made by encryption[3].

Stores the small end of the data and is essentially split into two layers, namely the container layer and the file system layer. The container layer has 64-bit aligned boundaries and stores volume metadata, snapshots, and encryption state.The container layer has a one-to-many relationship with the file system layer. These are container and volumes in Apple nomenclature. Each container contains multiple volumes and there is only one container per partition. The file system layer
is built with, for example, directory data structures, metadata and file contents[4].

Recovering lost or deleted files from the file system is an important part of computer forensics. this is called carving. there are tools to create the internal data structures of file systems, e.g. sleuthkit is incomplete or apfs carving. dewald researched different ways to detect and recover files in rsa. the result of their work is an implemented proof of concept called afro, named after apfs file recovery[5].

II.LITERATURE SURVEY:

According to **Kamil Malinka**.et al., 2020 Data is the most valuable part of most modern systems. Many hackers and criminals try to steal this information all the time. Therefore, data must also be the most protected part of any company's systems. We would like our systems to be impenetrable, but that is not possible. If we want to protect data, if our system[6].

According to **Michał Leszczynski**.et al., 2020 open source blackbox binary analysis system DRAKVUF. This project uses Xen's virtual machine introspection and altp2m to accomplish its goal very carefully. We describe our recent contributions to the project, including Windows API monitoring and heuristic malware extraction[7].

According to **Nihad A Hassan**. et al., 2019 The main task of a computer forensics investigator is to acquire and analyze computing devices' memory images. In a nutshell, a memory image—widely known as a forensic image—is a static snapshot of all or part of the data on a computing devices' secondary storage (e.g., HDD, SSD), attached storage device (e.g., USB thumb drive, external hard drive, magnetic tape), or RAM memory (when performing live acquisition on running systems)[8]..

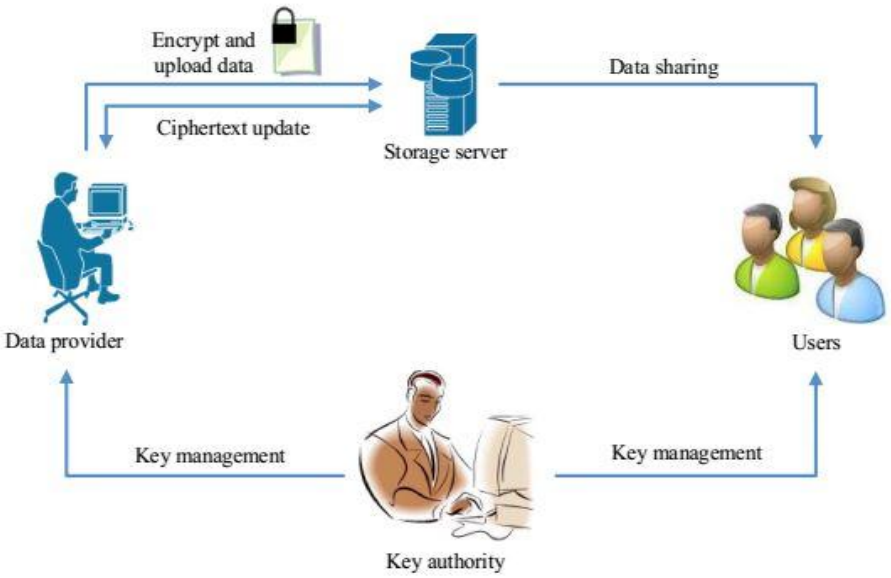
According to **O Nolasco-Jauregui**.et al., 2022 The purpose of this study is to create a web application from the edited methodology with a set of instructions that show the coding in a flowchart. The main purpose of this method is to help non-profits spread the word about the COVID-19 pandemic so that users can share important and timely information. This is a working design and below is a series of screenshots that show how it behaves[9].

According to **Scott Belshaw**.et al., 2023 Although known for both legitimate and illegitimate purposes, the dark web remains notorious for facilitating illegal and deviant activities ranging from drug trafficking to child pornography, human trafficking, arms trafficking and extremist recruitment. Thus, researching and understanding the dark web is a critical and important step in fighting and preventing cybercrime. However, exploring the dark web presents unique challenges[10].

III.PROPOSED SYSTEM:

The proposed system aims to securely store and retrieve files by employing a container-based architecture combined with RSA encryption. The RSA algorithm, known for its strong cryptographic properties, will be utilized to safeguard the data.

ARCHITECTURE DIAGRAM:



Explanation:

RSA Key Generation Module:

This module is responsible for generating RSA public and private key pairs.
Representation: Show this as a standalone component or module connected to the main system, indicating its role in key generation.

File Encryption Module:

This module handles the encryption of files using the RSA public key.
Representation: Depict this module connected to both the RSA Key Generation Module (for obtaining the public key) and the Container Management Module (for storing encrypted files).

Container Management Module:

This module manages the storage and retrieval of encrypted files in containers.
Representation: Show this as a central component or database-like structure where encrypted files are stored. Connect it to the File Encryption Module (for storing encrypted files) and the File Retrieval Module (for retrieving files).

File Retrieval Module:

This module handles the retrieval and decryption of files using the RSA private key.
Representation: Depict this module connected to the Container Management Module (for accessing encrypted files) and possibly to an authentication/authorization component to ensure secure access.

Authentication/Authorization Component:

This component verifies the identity and permissions of users or systems accessing the encrypted files.
Representation: Show this component connected to the File Retrieval Module and possibly to external systems or user interfaces for authentication and authorization processes.

IV.RESULT AND DISCUSSION:

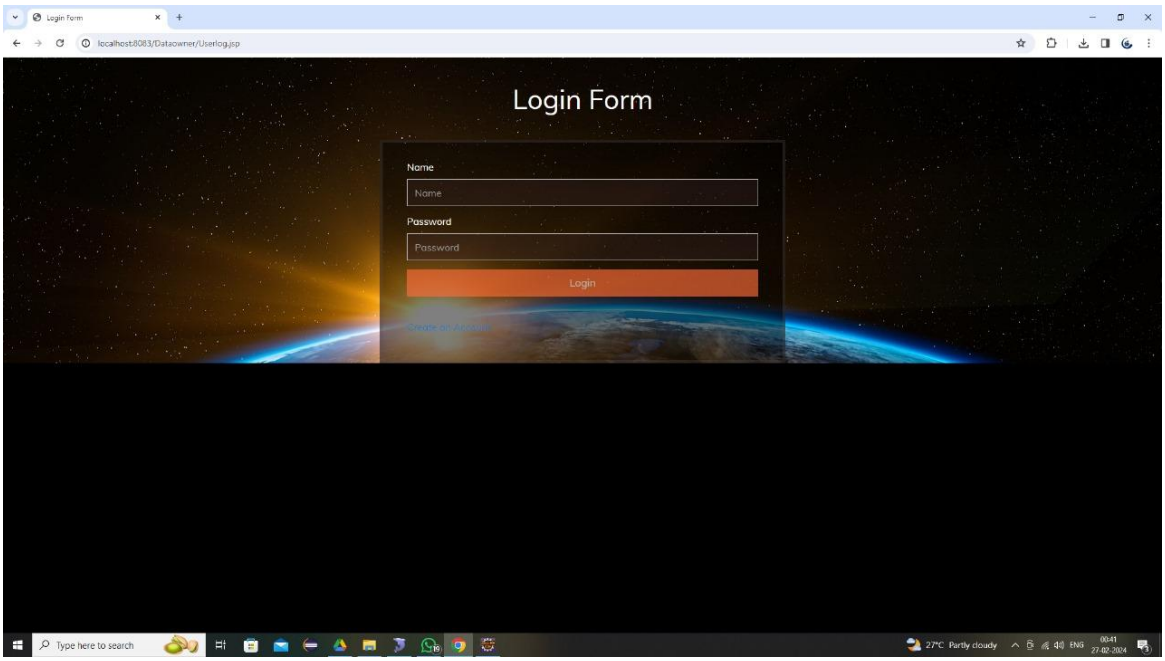


FIG.1 Admin Login Page

The Admin Login Page is designed exclusively for system administrators to access the backend administration panel securely. Administrators are required to enter their unique credentials, including username and password, to authenticate and gain access to the admin dashboard.

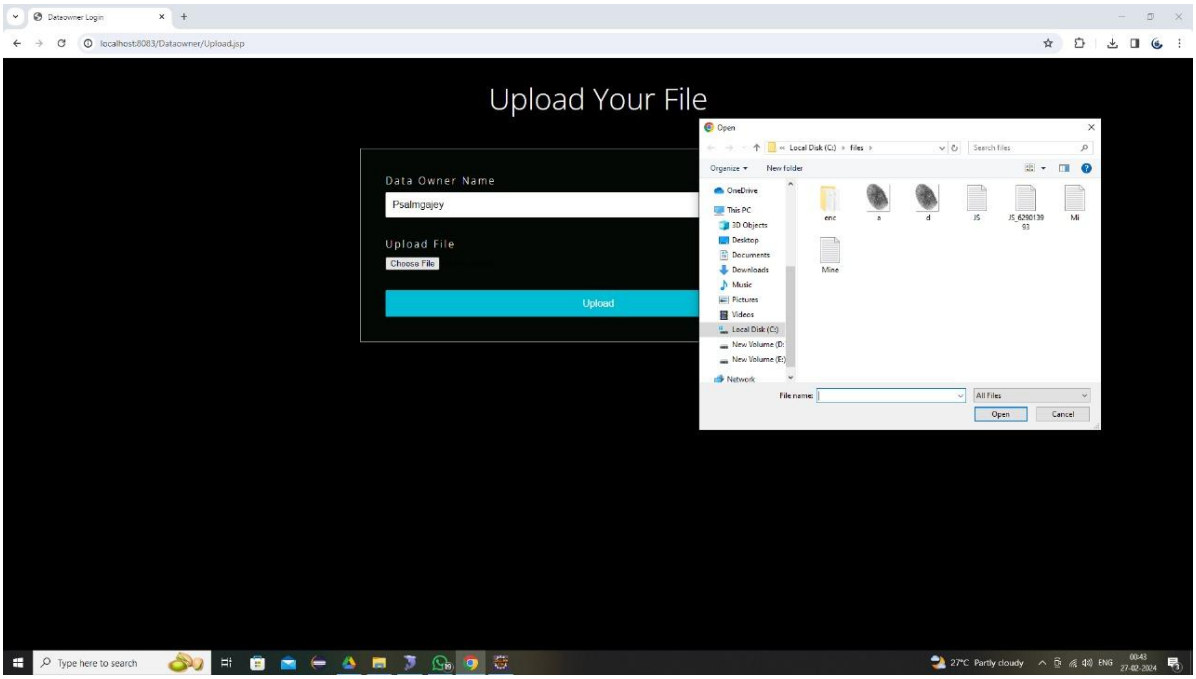


FIG.2Data Owner Home Page

The Data Owner Home Page serves as the central hub for data owners to manage and oversee their data assets securely. Upon logging in, data owners are presented with a comprehensive dashboard that provides insights into their data storage, access logs, and user activity.

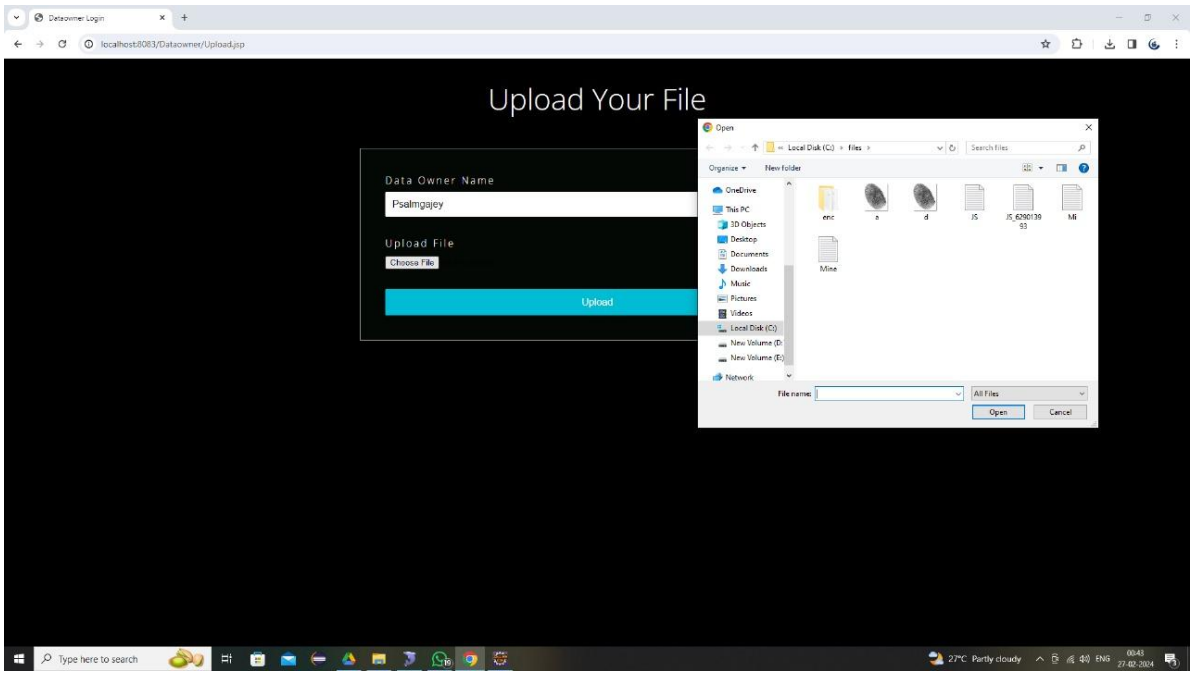


FIG.3 Upload File

The file upload feature facilitates users to securely upload their files to the system. Upon successful upload, the file is encrypted using the RSA algorithm and stored in a containerized format. Users are provided with feedback confirming the successful upload of their files.

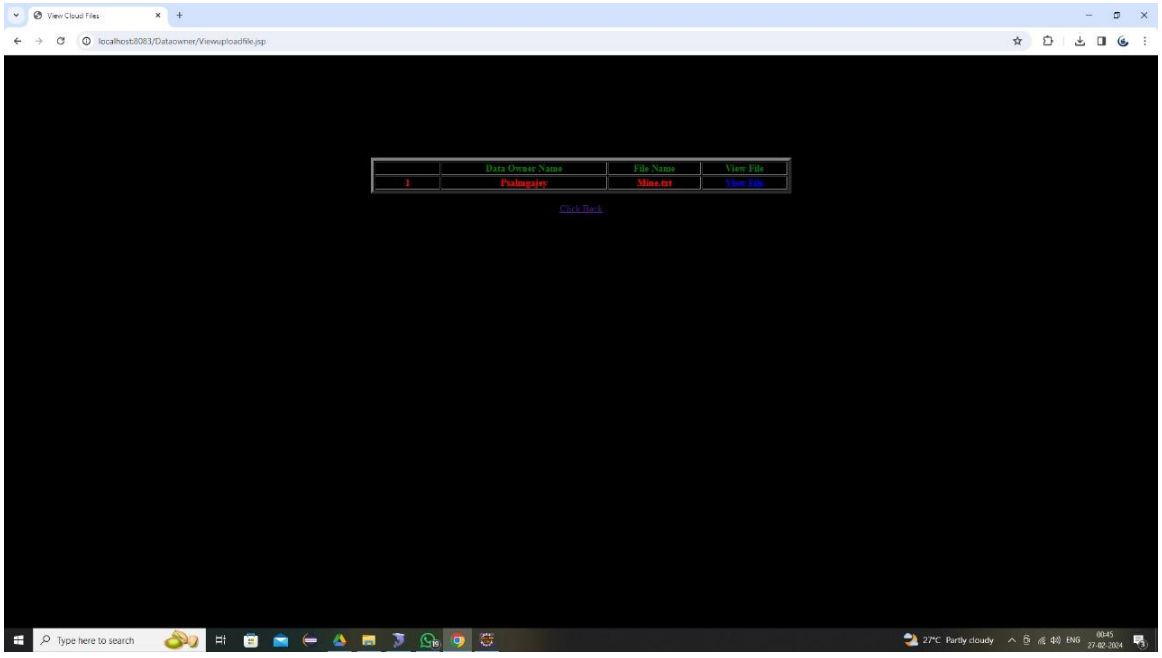


FIG.4 View File List

The view file list functionality enables users to see a list of their uploaded files. Each file entry includes metadata such as filename, file size, and upload date. Users can select a file from the list to perform various actions like downloading, viewing, or deleting the file.

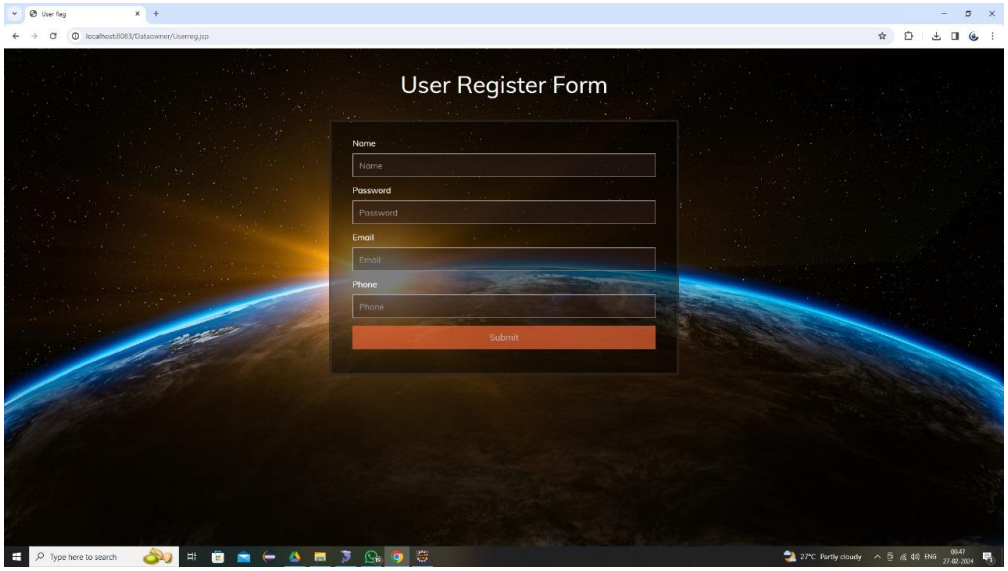


FIG.5 User register Page

The user registration page allows new users to create an account by providing necessary information such as username, email address, and password. The registration process includes validation checks to ensure the uniqueness of the username and the strength of the password. Upon successful registration, users receive a confirmation message and can proceed to log in to their account.

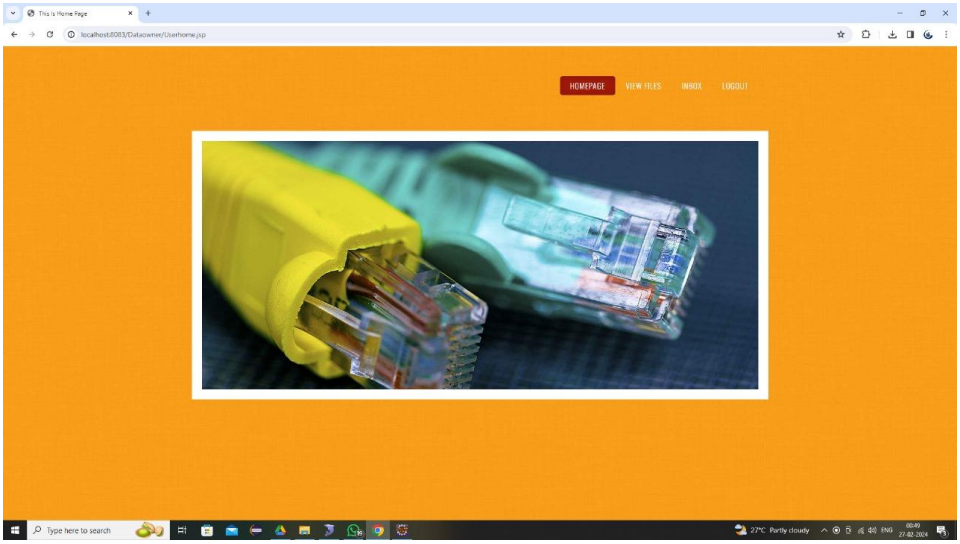


FIG.6 User Home Page

The home page displays the user's uploaded file list, along with options to upload new files, view file details, and perform other file-related actions. Additionally, users can access their profile settings, change password, and log out from the home page.

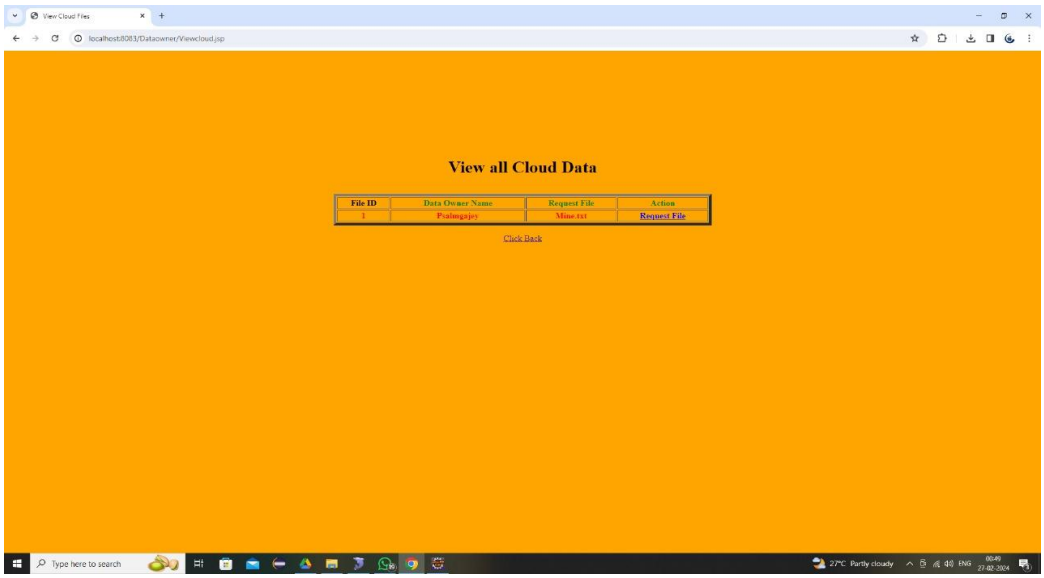


FIG.7 User View File

The view file feature allows users to access and view the contents of their uploaded files. When a user selects a file from the file list, the system retrieves the encrypted file data from the container, decrypts it using the RSA algorithm, and displays the plaintext file content to the user. Users can also download the decrypted file or choose to re-encrypt and store the file with modifications.

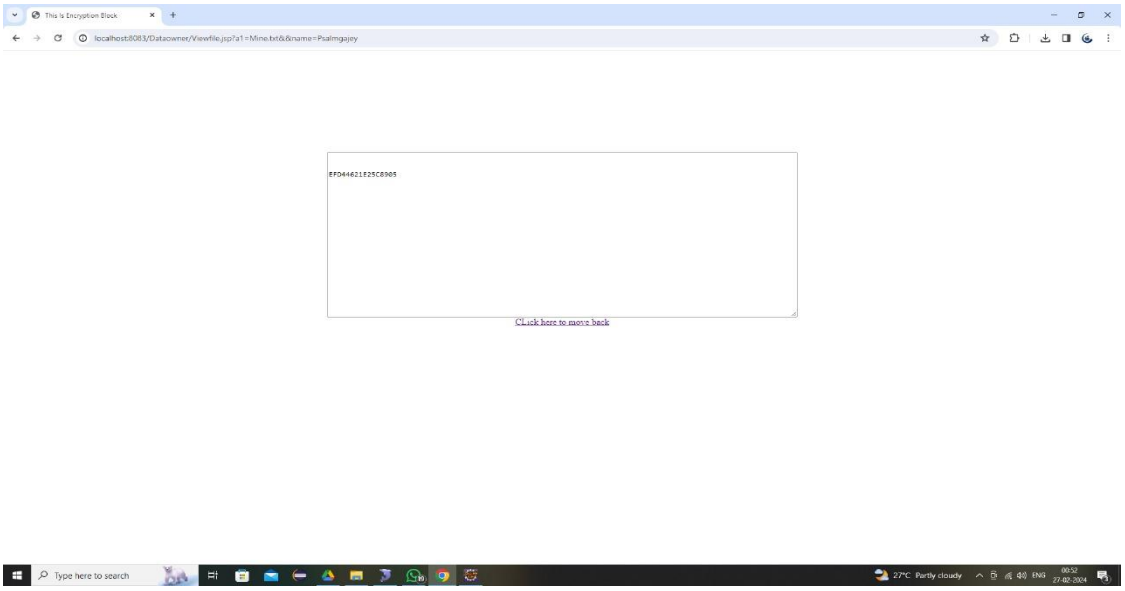


FIG.8 Encrypted Format

The encrypted format used for storing files in the container combines RSA encryption for key management and a symmetric encryption algorithm (e.g., AES) for encrypting the file data. The encrypted container file includes structured metadata and encrypted data segments. The RSA public key is used to encrypt the symmetric key, ensuring that only the intended recipient with the corresponding private key can decrypt and access the file data securely.

V.CONCLUSION:

In summary, building a container-based file encryption and retrieval system with the RSA algorithm requires careful planning and execution. It involves creating modules for key generation, file encryption, container management, and file retrieval. Ensuring secure key storage, robust access control, data integrity, and secure communication are essential aspects to focus on. By adhering to these principles and best practices, the system can offer a reliable and secure way to store and access sensitive data.

REFERENCE:

[1].Thomas Gobel, Jan Turr, and Harald Baier. Revisiting data hiding techniques for apple file system. In Proceedings of the 14th International Conference on Availability, Reliability and Security, page 41. ACM, 2019.

[2].Kurt H Hansen and Fergus Toolan. Decoding the apfs file system Digital Investigation, 22:107–132, 2017.

[3].Leon Daniel Baranovsky, Luis Felipe Cabrera, Chiehshow Chin, and Robert Rees. Logical volume manager and method having enhanced update capability with dynamic allocation of storage and minimal storage of metadata information, April 27 2018. US Patent 5,897,661.

[4].Andreas Dewald Ernw whitepaper 65 apfs internals for forensic analysis https://static.ernw.de/whitepaper/ERNW Whitepaper65 APFS-forensics signed.pdf, 2018.

[5].Jonas Plum and Andreas Dewald. Forensic apfs file recovery. In Proceedings of the 13th International Conference on Availability, Reliability and Security, pages 1–10, 2018.

[6].Martin Ocenas, Ivan Homoliak, Petr Hanacek, Kamil Malinka 2020, Security and encryption at modern databases, Proceedings of the 2020 4th International Conference on Cryptography, Security and Privacy, 19-23.

[7].Michał Leszczyński, Krzysztof Stopczański 2020,A new open-source hypervisor-level malware monitoring and extraction system-current state and further challenges, VB2020 localhost. Virus Bull...

[8].Nihad A Hassan, Nihad A Hassan 2019,Acquiring Digital Evidence, Digital Forensics Basics: A Practical Guide Using Windows OS, 111-139, 2019.

[9].O Nolasco-Jáuregui, LA Quezada-Téllez 2022, Pandemic Information Dissemination Web Application: A Manual Design for Everyone, The International Journal of Computational Science, Information Technology and Control Engineering (IJCSITCE) 9 (1), 1-19, 2022.

[10].Fawn T Ngo, Catherine Marcum, Scott Belshaw 2023,The dark web: What is it, how to access it, and why we need to study.Journal of Contemporary Criminal Justice 39 (2), 160-166, 2023.