ENHANCED SECURED DATA ACQUISITION FRAMEWORK FOR CLOUD SYSTEMS INTEGRATING KEY MANAGEMENT AND MULTILAYER SECURITY

I.Anandakumar[1], U.Sundhar[2], D.Kanthasamy[3], P.Chitra Devi[4]

[1]P.G student, Department of CSE, Thiruvalluvar College of Engineering and Technology, Vandavasi.
[2]Head of the Department, Department of CSE, Thiruvalluvar College of Engineering and Technology, Vandavasi.
[3]Head of the Department, Department of CSE(AI&ML),Thiruvalluvar College of Engineering and Technology Vandavasi.
[4]Assistant Professor, Department of CSE, Thiruvalluvar College of Engineering and Technology Vandavasi

ABSTRACT - *In the age of digital transformation, the demand for strong data security and effective key management has reached unprecedented levels. Organizations that manage sensitive information across various sectors, including finance, healthcare, and government, need a thorough solution to protect their data assets. This abstract presents an innovative framework aimed at tackling these issues – the Secured Data Acquisition Integrating Framework (SDAIF) for Key Management and Multilayer Security. SDAIF embodies a comprehensive strategy for data security, integrating data acquisition, encryption, key management, and multilayer security protocols. The main goal of the framework is to offer a cohesive and adaptable system for organizations to defend their data against unauthorized access, tampering, and breaches. The Secured Data Acquisition Integrating Framework (SDAIF) for Key Management and Multilayer Security serves as a complete answer to the increasingly intricate data security challenges that organizations encounter today. By implementing SDAIF, organizations can enhance their data protection strategies, minimize the likelihood of data breaches, and maintain the confidentiality, integrity, and availability of their essential data assets.*

Key words: SDAIF, Key Management, Multilayer Security

1.INTRODUCTION

The emergence of cloud Fog computing introduces a distributed computing layer that enhances cloud services like storage, processing, and networking for edge devices, thus reducing service latency. This fog layer is made up of small, independent computing units known as fog nodes, which are situated near the edge devices. These nodes are interconnected with one another as well as with centralized cloud servers. The fog nodes collaborate to pre-process data and offer short-term data storage, which minimizes the need for interaction with cloud servers and boosts overall efficiency.

Fog nodes can take the form of fog devices that store data, fog servers that process data, or fog gateways that facilitate the transfer of information between fog devices and servers. Fog computing broadens cloud services across extensive geographical regions. It encompasses features such as location awareness, mobility, geo-distribution, distributed control, and real-time interaction, all of which are essential for real-time IoT applications.

The fog layer plays a crucial role in determining processing speed and information flow. The Fog-enabled ecosystem enhances the efficiency of edge devices; however, it faces similar security and privacy challenges as the cloud infrastructure. Among these security concerns, authentication remains the most critical issue [11]. In the fog computing framework, numerous participants engage, and various trust domains are present.

Need for Study

- The growing number of IoT devices necessitates a scalable and effective authentication mechanism to guarantee secure communication among devices, fog nodes, and the cloud.
- In the absence of strong authentication, the framework becomes vulnerable to threats such as impersonation, replay attacks, and man-in-the-middle attacks, jeopardizing data integrity and user privacy.

- IoT and fog devices frequently possess limited computational and energy resources. Conventional authentication methods may be overly resource-demanding, underscoring the necessity for lightweight alternatives.
- The delicate nature of data handled within cloud-fog-device frameworks (such as healthcare or financial information) demands strong authentication measures to maintain confidentiality.
- The process of establishing and managing cryptographic keys across distributed nodes is intricate and requires innovative, efficient strategies to avert key leakage or misuse.
- Fog computing adds new layers of data processing and decision-making closer to the devices, resulting in additional vulnerability points that necessitate secure key management and authentication.

Objective of the Paper

Some of the main objectives are:

- Key Management: Develop a secure and efficient system for generating, storing, distributing, rotating, and revoking cryptographic keys utilized in encryption, decryption, and authentication processes.
- Multilayer Security: Apply multiple layers of security measures (including encryption, access controls, authentication protocols, intrusion detection, and monitoring) at various levels of the system to ensure comprehensive protection against a range of threats.
- Risk Mitigation: Recognize potential vulnerabilities and threats, evaluate the associated risks, and implement strategies to effectively mitigate these risks, thereby minimizing the likelihood and impact of security incidents.
- User Access Control: Establish detailed access controls and authentication mechanisms to guarantee that only authorized individuals or systems can access specific data based on predetermined roles, permissions, and credentials.
- Scalability and Performance: Create the framework to be scalable, adaptable, and high-performing, capable of managing increasing data volumes, various data types, and changing security requirements without sacrificing efficiency.

2.LITERATURE REVIEW

In the paper titled "A Multilayer Encryption Model to Protect Healthcare Data in Cloud Environment" from the Department of Medicine at Hayatabad Medical Complex in Peshawar, Pakistan, the 21st Century is acknowledged as the age of cloud computing, which has become essential for organizations. This technology is applicable across various sectors, including education, government, public services, and healthcare. There are two categories of patient information: protected/sensitive health information and general information. Protected information, such as phone numbers, ATM details, security numbers, and medical record numbers, necessitates a higher level of confidentiality compared to general information. Consequently, certain protected health information that does not directly identify patients, like general disease names and symptoms, can be beneficial for research purposes. Health information is safeguarded by ensuring confidentiality, integrity, and availability when data is stored in a cloud environment. Cryptographic methods offer various techniques to secure data in the cloud. In this paper, we propose a multilayer encryption technique aimed at maintaining the confidentiality of data stored in the cloud. This proposed method is expected to enhance the security of cryptographic techniques when implemented in a multilayered approach. We have established a local system for conducting the experiment.

In the paper titled "Secure Data Transmission and Trustworthiness Judgement Approaches Against Cyber-Physical Attacks in an Integrated Data-Driven Framework" from the Department of Control Science and Engineering at Harbin Institute of Technology in Harbin, China, it is noted that threats from cyberattacks have escalated, ranging from the exposure of critical user information to the destruction or manipulation of industrial control systems. The study of data security during network transmission has garnered increasing attention within the systems and control community, which is deemed both necessary and timely in the context of Industry 4.0.In most current methodologies, the safeguarding of transmitted data against eavesdropping attacks and the identification of malicious integrity threats are typically conducted separately. This study proposes a unified data-driven framework suitable for the control level to address secure transmission and attack detection concurrently. Within this framework, a secure correlation-based encryption/decryption method and a trustworthiness assessment approach are introduced. Extensive discussions are provided concerning the analysis of sensitivity to attacks, the resulting time delay, and the design degree-of-freedom. Executable algorithms are offered, for which the hardware is modularized and can operate independently from the configuration of monitoring and control systems or any external authentication agencies.

Referring to the paper, 'A Secure and Intelligent Framework for Vehicle Health Monitoring Exploiting Big-Data Analytics' from the School of Mathematics and Computer Science at the University of Wolverhampton, U.K., the reliance on vehicles is rapidly increasing due to their exceptional transport capacity, speed, efficiency, flexibility, enjoyable travel experience, minimal physical exertion, and significant economic impact. Consequently, the demand for smart and intelligent feature enhancements is rising and has become a primary concern for maximizing productivity from the current viewpoint. In this context, the Internet of Everything (IoE) emerges as a concept that can significantly influence the automotive sector by connecting stakeholders, processes, data, and objects through networked connections. However, the lack of intelligent features results in neglect regarding the proper maintenance of vulnerable vehicle components, reckless driving, severe accidents, insufficient driving instruction, and poor decision-making, which incurs additional maintenance costs and hampers national economic growth. For this, we proposed a conceptual framework for a central VHMS exploiting IoE-driven Multi-Layer Heterogeneous Networks (HetNet) and a machine learning technique to oversee individual vehicle health conditions, notify the respective owner-driver real-timely and store the information for further necessary action. This article transparently portrayed an overview of central VHMS and proposed the taxonomy to achieve such an objective.

In the paper titled "Security Threats and Mitigation Techniques in UAV Communications" from the Department of Electronics and Communication Engineering at the National Institute of Technology Silchar, Cachar, Assam, India, highlights the significant role of unmanned aerial vehicles (UAVs) in facilitating a variety of new applications and services. These include military and rescue operations, aerial surveillance, civilian uses, precision agriculture, and extensive wireless network access in remote regions. UAVs are also utilized in other fields such as monitoring transmission lines and oil rigs, as well as in disaster recovery efforts. With their enhanced payload capacity and extended flight times, UAVs are increasingly becoming the preferred option for numerous emerging wireless communication systems. However, due to their inherently open operational framework, UAVs are particularly susceptible to serious security threats, including cyber-attacks and eavesdropping on navigational and communication channels. Given their extensive

applications, ensuring secure UAV communications has become increasingly vital, as security breaches can result in severe repercussions. Numerous studies have explored the privacy and security challenges in UAV-assisted networks and proposed various mitigation strategies to tackle these security issues. This paper presents a thorough survey focusing on the security concerns associated with UAV-aided networks.

In the paper titled "A Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption," published in the IEEE Transactions on Parallel and Distributed Systems, it is noted that the 21st century is characterized by the rise of cloud computing, which has become essential for organizations across various sectors. This technology is applicable to all types of organizations, including education, government, public sector, and healthcare. There are two categories of patient information: protected/sensitive health information and general information. Protected information (such as phone numbers, ATM details, security numbers, medical record numbers, etc.) necessitates a higher level of confidentiality compared to general information. Consequently, certain protected health information that lacks patient association (such as general disease names and symptoms) can significantly aid research experiments. Health information is safeguarded by ensuring confidentiality, integrity, and availability when data is stored in a cloud environment. Various cryptographic methods offer different techniques to secure data within this cloud setting. In this paper, we propose a multilayer encryption technique aimed at maintaining the confidentiality of data stored in the cloud. This proposed method is expected to enhance the security of cryptographic techniques when implemented in a multilayered structure. We have established a local system for conducting the experiment.

In the paper titled "Achieving secure, scalable, and fine-grained data access control in cloud computing," presented at Proc. IEEE INFOCOM, pp. 1-9, 2019, it is noted that threats from cyberattacks range from exposing critical user information to the destruction or manipulation of industrial control systems. The study of data security during network transmission has garnered increasing attention within the systems and control community, which is deemed essential and timely in the context of Industry 4.0. In most current methodologies, the safeguarding of transmitted data against eavesdropping attacks and the detection of malicious integrity attacks are typically addressed separately. This study proposes an integrated data-driven framework that can be applied at the control level to manage secure transmission and attack detection concurrently. Within this framework, a secure correlation-based encryption/decryption method and a trustworthiness assessment approach are introduced. Detailed discussions are provided regarding the sensitivity analysis to attacks, the time delays introduced, and the design degree-of-freedom. Executable algorithms are presented, and the corresponding hardware is modularized, allowing it to function independently from the configuration of monitoring and control systems or any third-party authentication entities.

Referring to the paper by M. Li, S. Yu, and Y. Zheng titled "Scalable and secure sharing of personal health records in cloud computing using Attribute-Based Encryption," published in IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 1, pp. 131-143, 2019. The reliance on vehicles is significantly increasing due to their remarkable transport capacity, speed, efficiency, flexibility, comfortable travel experience, minimal physical exertion, and considerable economic influence. Consequently, the need for enhancements in smart and intelligent features is rising and has become a primary concern for maximizing productivity from the current viewpoint. In this context, the Internet of

Everything (IoE) emerges as a concept that can significantly impact the automotive sector by connecting stakeholders, processes, data, and objects through networked links. However, the lack of intelligent features results in neglect regarding the proper maintenance of vulnerable vehicle components, reckless driving, severe accidents, insufficient driving instruction, and poor decision-making, which leads to additional maintenance costs and hampers national economic development. To address this issue, we have proposed a conceptual framework for a central Vehicle Health Management System (VHMS) that utilizes IoE-driven Multi-Layer Heterogeneous Networks (HetNet) and machine learning techniques to monitor the health conditions of individual vehicles, provide real-time notifications to the respective owner-drivers, and store the information for necessary future actions. This article provides a clear overview of the central VHMS and introduces a taxonomy aimed at achieving this objective.

The document titled 'Deep Learning Based Homomorphic Secure Searchable Encryption for Keyword Search in Blockchain Healthcare System: A Novel Approach to Cryptography' is published in Sensors, 22(2), 528. Unmanned Aerial Vehicles (UAVs) have played a crucial role in facilitating numerous new applications and services, which encompass military and rescue operations, aerial surveillance, civilian uses, precision agriculture, and the provision of extensive wireless network access in remote locations. Additionally, they have been utilized in various other fields such as monitoring transmission lines and oil rigs, as well as disaster recovery efforts. With their enhanced payload capacity and extended flight durations, UAVs are increasingly becoming the preferred option for a wide range of emerging wireless communication systems. Nevertheless, due to their inherently open operational framework, UAVs are particularly susceptible to significant security threats stemming from cyber-attacks, eavesdropping on navigational and communication channels, among other vulnerabilities. In light of their extensive applications, the necessity for secure UAV communications has grown increasingly urgent, as security breaches can result in severe repercussions. Numerous studies have explored the scope of privacy and security challenges within UAV-assisted networks and have proposed various mitigation strategies to tackle different security issues. This paper presents a thorough survey focusing on the security concerns associated with UAV-aided operations.

3.IMPLEMENTATION

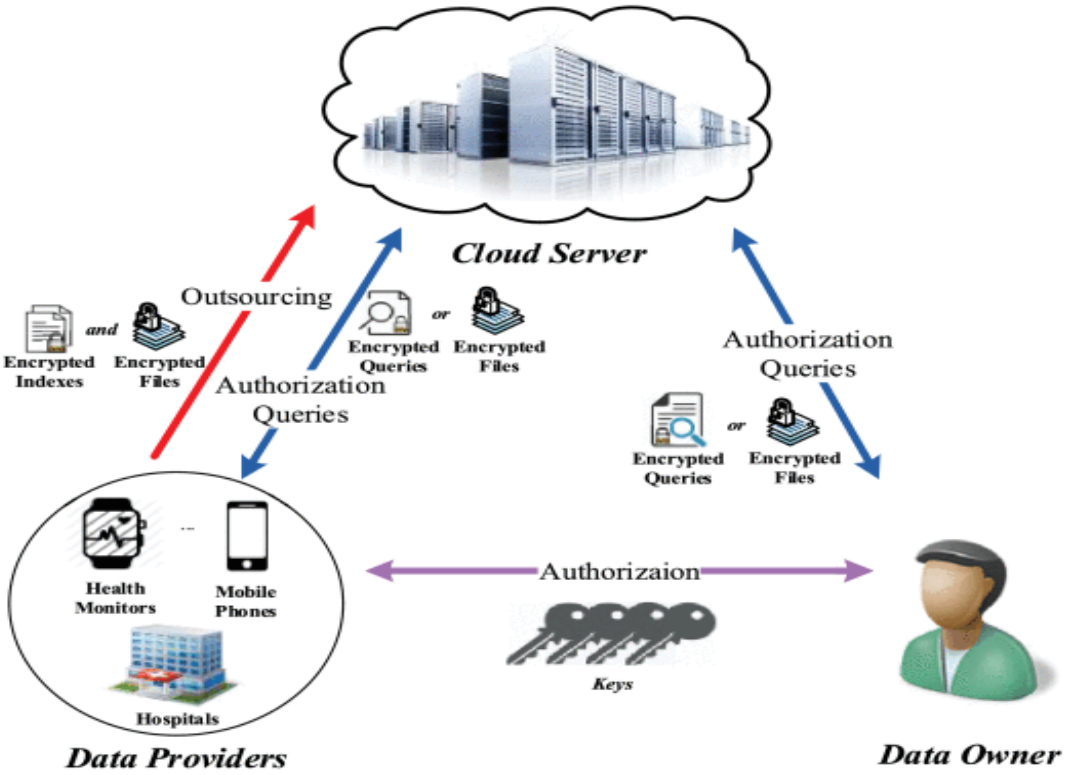
Creating an algorithm for the Secured Data Acquisition Integrating Framework focused on Key Management and Multilayer Security entails various intricate elements. Below is a proposed algorithm outline that takes into account the complex characteristics of the security framework:

Key Generation and Management:

Step 1: Key Generation: Generate cryptographic keys using a secure random key generator, creating both symmetric and asymmetric keys.

Step 2: Key Distribution: Establish a secure method for distributing keys to authorized entities; ensuring encryption keys are securely shared.

Step 3: Key Rotation and Revocation: Implement routines for periodic key rotation to enhance security and mechanisms for key revocation in case of compromise or unauthorized access.



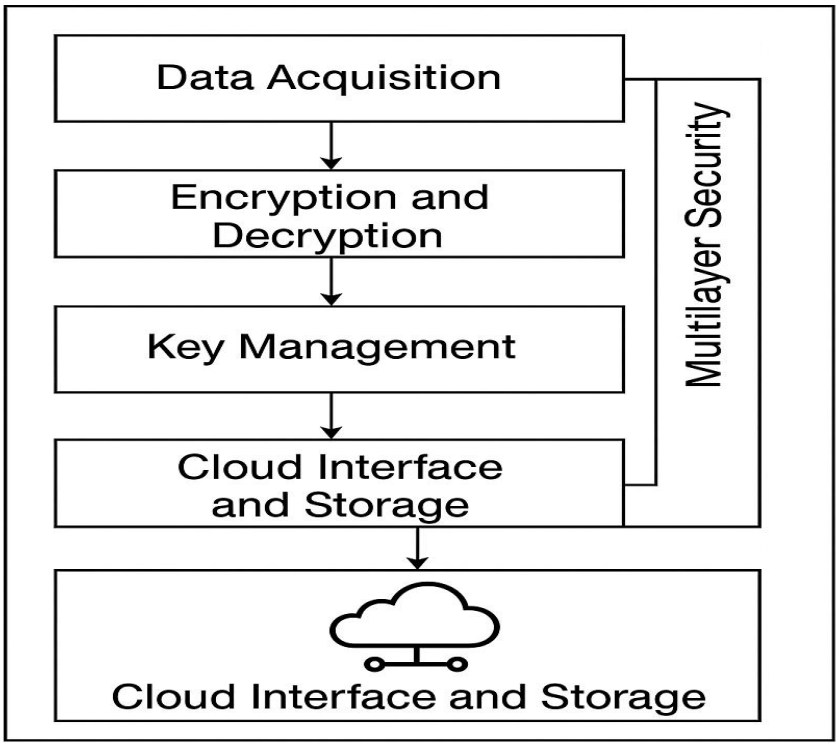


Fig 3.1 System Cloud Architecture

Multilayer Security:

Step 1: Data Encryption/Decryption: Utilize AES (Advanced Encryption Standard) for symmetric encryption and RSA (Rivest-Shamir-Adleman) for asymmetric encryption to protect data in transit and at rest.

Step 2: Access Control: Apply Role-Based Access Control (RBAC) or Attribute-Based Access Control (ABAC) to manage user access permissions and regulate data access.
Step 3: Authentication Mechanisms: Implement Multi-Factor Authentication (MFA) or Biometric Authentication for enhanced user identity verification.

Data Lifecycle Protection:
Step 1: Data Acquisition: Employ secure data acquisition protocols ensuring encrypted transmission channels for data collection.
Step 2: Data Storage: Store encrypted data in secure databases or repositories with access controls and encryption mechanisms.
Step 3: Data Access: Implement decryption and access controls at the point of data retrieval, ensuring only authorized users can access decrypted data.

Continuous Monitoring and Threat Detection:
Step 1: Real-time Monitoring: Deploy monitoring tools for continuous surveillance of system logs, network traffic, and user activities.
Step 2: Anomaly Detection: Utilize machine learning algorithms or anomaly detection techniques to identify suspicious activities or deviations from normal.Step 3: Incident Response: Implement automated or manual response mechanisms to address identified threats, including isolation, notification, and resolution procedures.

*Compliance Integration***:**
Step 1: Regulatory Mapping: Establish mapping between regulatory requirements (e.g., GDPR, HIPAA) and corresponding security measures within the framework.
Step 2: Compliance Auditing: Develop routines for periodic compliance audits to ensure adherence to regulatory standards and guidelines.

*User Education and Awareness***:**
Step 1: Training Programs: Schedule regular training sessions and awareness programs to educate users about security policies, best practices, and the importance of compliance.
Step 2: Phishing Awareness: Conduct simulated phishing exercises to enhance user awareness and readiness against potential threats.

Adaptive Security Measures:
Step 1: Threat Intelligence Integration: Incorporate threat intelligence feeds or databases to stay updated with evolving cyber threats and vulnerabilities.
Step 2: Patch Management: Establish procedures for timely application of security patches and updates to address known vulnerabilities.

Work Description

- User Authentication
- Profile Management
- File Upload and Encryption
- Static Information Pages
- Session & Security Management.

User Authentication (Sign Up & Sign In)
Authentication is the cornerstone of any secure web application. This module enables secure user registration and login functionality, forming the first layer of access control in the system.

Features:

- *Sign Up Functionality*:
  - Users can register by submitting a username and password via a form powered by WTForms.
  - Input data is validated before account creation.
  - Although basic in the current design, this module is scalable to include advanced checks such as email verification, password strength, and CAPTCHA integration.

- *Sign in Functionality*:
  - Allows returning users to authenticate using their registered credentials.
  - Upon successful login, users are redirected to a profile page, and session variables are initialized to maintain the user's login state.

- *Session Management:*
  - Flask's session mechanism ensures user data is retained securely across requests using signed cookies.
  - Logged-in users can access restricted routes like the profile and upload pages.

Profile Management

This module enables each authenticated user to view their profile and personalized content.

Features:

- Upon login, users are redirected to a dedicated profile page.
- This page displays session-specific data such as the username, offering a personalized view.
- Acts as a control center for navigating to other secure parts of the application such as file upload.

Security Considerations:

- Access to the profile page is restricted via session checks to prevent unauthorized access.
- Session tokens are monitored to ensure user authenticity across activities.

File Upload and Encryption

This module manages the core functionality of the system: secure file acquisition and storage.

Subcomponents:

File Upload Interface:

- Users can select a local file and upload it via a web interface.
- Upload routes are protected to ensure only authenticated users can use this feature.

Encryption Process:

- AES CBC Mode encryption is used to protect the file content before it is uploaded.
- A new random AES key and IV (Initialization Vector) are generated per file upload.
- The file is padded to fit the block size required by AES and then encrypted.
- The IV is prepended to the encrypted content for future decryption.

Advantages:

- Strong symmetric encryption ensures confidentiality of sensitive user files.
- Each file gets a unique key and IV, preventing pattern recognition.

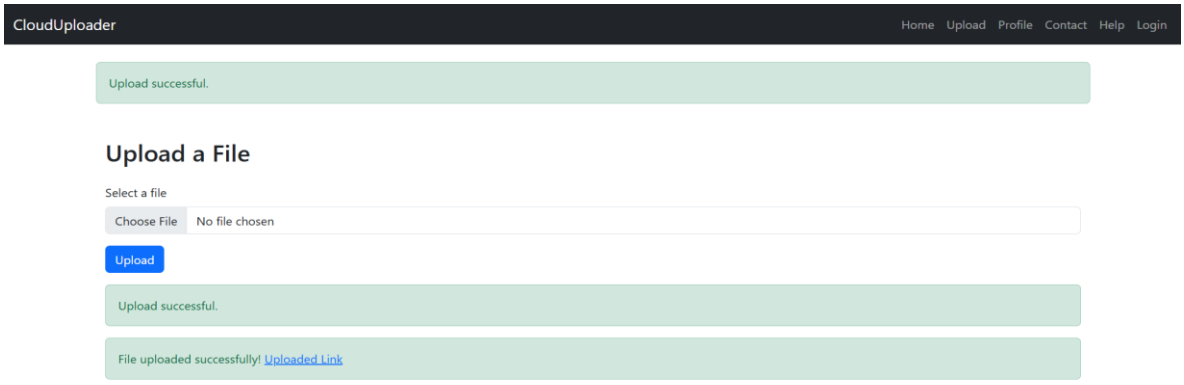


Fig 3.2: File Upload Interface

Fig 3.3.File encrypted text& upload process

Files stack Integration:

- The encrypted file is uploaded to Filestack using its Python SDK.
- A secure URL is generated and shared with the user after a successful upload.
- This approach offloads storage concerns and leverages Filestack's scalable infrastructure.

Security Highlights:

- Encryption is done before the file leaves the local server.
- Uploaded files are unreadable to external parties, including the storage provider.
- Ensures confidentiality even if the cloud infrastructure is compromised.

Static Information Pages

These pages offer navigational support and helpful information for the users.

Home Page:

- Serves as the landing page with general application information and navigation links.

Contact Page:

- Displays contact information or a form for users to reach administrators.

Help Page:

- Provides instructions and support for using various functionalities of the application.
- These pages are publicly accessible and contain no sensitive user-specific content.

Session & Security Management

Beyond user credentials and file encryption, this module ensures secure state management and controlled access.

Key Functions:

- User session management using Flask sessions.
- Cookies are signed and stored securely.
- Restriction of sensitive routes (/profile, /upload) to only logged-in users.
- Prevents session hijacking by ensuring only authenticated users can access resources.

Planned Enhancements:

- Logout functionality to clear sessions explicitly.
- Inactivity timeout for automatic session expiration.
- CSRF token integration for form submissions.

CONCLUSION AND FUTURE ENHANCEMENT

This paper outlines a method known as cloud-assisted access, highlighting its advantages and drawbacks. The project focuses on safeguarding medical information and ensuring its anonymity within the cloud. The suggested system incorporates privacy into healthcare frameworks through the use of a private cloud, offering a solution for secure data storage that employs an encryption algorithm-based key management system to ensure unlinkability. Additionally, the system explores methods for access control in both standard and emergency situations, as well as the auditing of authorized users to deter misconduct, by merging anonymity-controlled threshold signing with advanced encryption standard encryption. Looking ahead, we aim to develop mechanisms capable of detecting any illegal distribution of users' health data and pinpointing potential sources of leakage.

In the future, this system could be further improved by incorporating intelligent tracking and forensic tools that not only identify unauthorized access but also trace the precise origin of any possible data breaches. By utilizing advanced watermarking or fingerprinting methods, it would be feasible to uniquely label each instance of access or data duplication, facilitating accurate identification in cases of data misuse.

REFERENCES

[1] Manjunath Hedge, Rohini R. Rao, and Radhakrishnan Bhat, “Design of an Efficient and Secure Authentication Scheme for Cloud-Fog-Device Framework Using Key Agreement and Management,” Proc. IEEE INFOCOM, pp. 10-07, 2024.

[2] Al S. Yu, C. Wang, K. Ren, “Achieving secure, scalable, and fine-grained data access control in cloud computing,” Proc. IEEE INFOCOM, pp. 1-9, 2019.

[3] J. Bethencourt, A. Sahai, B. Waters, "Ciphertext-policy attribute-based encryption," Proc. Security and Privacy, pp. 321-334, 2019

[4] J. Hur, D.K. Noh, "Attribute-based access control with efficient revocation in data outsourcing systems," IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 7 pp. 1214-1221, 2019.

[5] Lewko, B. Waters, "Decentralizing Attribute-Based encryption," Proc. Advances in Cryptology-EUROCRYPT, pp. 568-588, 2019.

[6] M. Li, S. Yu, Y. Zheng, "Scalable and secure sharing of personal health records in cloud computing using attribute-Based Encryption," IEEE Transactions on Parallel and Distributed System, vol. 24, no. 1, pp. 131- 143, 2019.

[7] Jiang, Y., Wu, S., Yang, H., Luo, H., Chen, Z., Yin, S., & Kaynak, O. (2022). Secure data transmission and trustworthiness judgement approaches against cyber-physical attacks in an integrated data-driven framework. *IEEE* Transactions on Systems, Man, and Cybernetics: Systems, 52(12), 7799-7809.

[8] Hu, J., Liang, W., Hosam, O., Hsieh, M. Y., & Su, X. (2022). 5GSS: a framework for 5G-secure-smart healthcare monitoring. Connection Science, *34*(1), 139- 161.

[9] GARIGIPATI, N., & REDDY, D. V. K. (2023). an integrated quantum and biometric key generation-based cloud data security framework for structured and unstructured electronic health records. Journal of Theoreticaland AppliedInformation Technology, 101(5).

[10] Poongodi, M., Bourouis, S., Ahmed, A. N., Vijayaragavan, M., Venkatesan, K. G. S., Alhakami, W., & Hamdi, M. (2022). A novel secured multi-access edge computing based vanet with neuro fuzzy systems based blockchain framework. Computer Communications, 192, 48-56.

[11] Ansari, D. B., & Khaliq, M. A. (2022). A Proposed Multilayered Framework for Security and Privacy in Big Data. International Journal of Computer Applications, *975*, 8887.

[12] Jadav, N. K., Kakkar, R., Mankodiya, H., Gupta, R., Tanwar, S., Agrawal, S., &Sharma, R. (2023). GRADE: Deep learning and garlic routing-based secure data sharing framework for IIoT beyond 5G. Digital Communications and Networks, *9*(2), 422-435.

[13] Rahman, M. A., Rahim, M. A., Rahman, M. M., Moustafa, N., Razzak, I., Ahmad, & Patwary, M. N. (2022). A secure and intelligent framework for vehicle health monitoring exploiting big-data analytics. IEEE Transactions on Intelligent Transportation Systems, *23*(10), 19727-19742.

[14] Kumar, R., Kumar, P., Aljuhani, A., Islam, A. N., Jolfaei, A., & Garg, S. (2022). Deep learning and smart contract-assisted secure data sharing for IoT-based intelligent agriculture. IEEE Intelligent Systems.

[15] Ali, A., Pasha, M. F., Ali, J., Fang, O. H., Masud, M., Jurcut, A. D., & Alzain, M. A. (2022). Deep learning based homomorphic secure search-able encryption for keyword search in blockchain healthcare system: A novel approach to cryptography. Sensors, *22*(2), 528.

[16] Leng, J., Chen, Z., Huang, Z., Zhu, X., Su, H., Lin, Z., & Zhang, D. (2022). Secure blockchain middleware for decentralized iiot towards industry 5.0: A review of architecture, enablers, challenges, and directions. Machines, *10*(10), 858.

[17] Thuraisingham, B., Kantarcioglu, M., & Khan, L. (2022). Secure Data Science: Integrating Cyber Security and Data Science. CRC Press.

[18] Chaudhary, S., Kakkar, R., Jadav, N. K., Nair, A., Gupta, R., Tanwar, S., ... &Davidson, I. E. (2022). A taxonomy on smart healthcare technologies: Security framework, case study, and future directions. Journal of Sensors, *2022*.

[19] Attkan, A., & Ranga, V. (2022). Cyber-physical security for IoT networks: a comprehensive review on traditional, blockchain and artificial intelligence-basedkey-security. Complex & Intelligent Systems, *8*(4), 3559-3591.