Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 45 No. 2 (2024)

Hierarchical Attribute-Based Encryption for Access Control to Secure Medical Data Using Hypergraph Model

J Mohammed Sirajudeen[1,3], Dr V Cyril Raj[2,3], Dr S Geetha[2,3]
[1]*Postgraduate Student,*
[2]*Professor,*
[3]*Department of Computer Science and Engineering, Dr. M.G.R. Educational and Research Institute*

Abstract **-** The HHABE encryption scheme is a game-changer in the realm of data security, especially within the critical context of medical information. Its foundation in hypergraphs and hierarchical structures marks a departure from conventional encryption methods, offering a sophisticated framework for controlling access to sensitive data. This innovative approach ensures intricate access control over sensitive information. With HHABE, data owners gain the power to designate attributes and attribute hierarchies, tailoring access policies for various user groups. This scheme not only offers a granular level of control but also introduces privacy preserving decryption capabilities, ensuring the confidentiality of data. Additionally, HHABE addresses scalability concerns inherent in key management systems, making it suitable for large-scale implementations without compromising security. In essence, HHABE represents a groundbreaking solution that amalgamates hypergraphs and hierarchical structures, empowering data owners with robust access control mechanisms while preserving privacy and scalability, especially vital in the sensitive domain of medical data.

Keywords: Hypergraph, Hierarchical structure, Access control, Encryption scheme, Medical data security, User group policies, Scalability.

1. Introduction

Hierarchical Attribute-Based Encryption (H-ABE) stands at the forefront of cryptographic innovation, where the fusion of hypergraph concepts with hierarchical structures has revolutionized Attribute-Based Encryption (ABE). ABE, a cryptographic paradigm, orchestrates access control through user and data attributes. H-HABE augments this by intricately organizing attributes hierarchically. Picture this: top-tier attributes embody broader categories, while lower-level ones epitomize specific characteristics. This structural framework births unparalleled security and flexibility in access control mechanisms, especially within intricate and expansive systems.

At its core, H-HABE is an evolution of ABE, fundamentally reshaping how we approach cryptographic protocols. Its introduction of hypergraph elements infuses a new dimension of complexity, paving the way for more intricate attribute arrangements. In the realm of security, this sophistication fortifies data access controls, rendering them impervious to breaches or unauthorized penetrations. The hierarchical organization of attributes not only enhances security but also amplifies flexibility and efficiency, making it a pivotal advancement in cryptographic applications.

The hierarchical structure in H-HABE introduces a meticulously crafted system where attributes are arranged in a tree-like format. At the apex lie overarching attributes, encapsulating broader categories of information or user characteristics. As the branches extend downwards, attributes become increasingly granular, delineating finer details and specific traits. This hierarchical arrangement empowers administrators with fine-grained access control, enabling them to precisely manage and allocate permissions based on the depth and specificity of attributes.

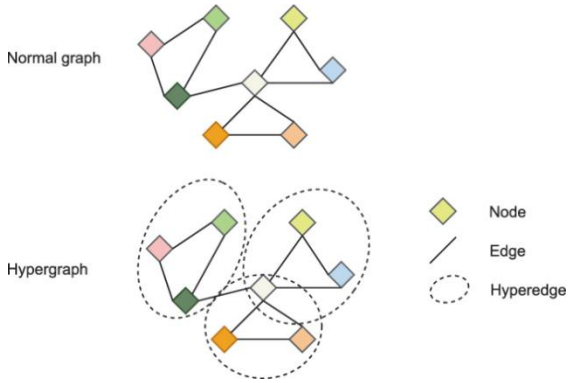


Figure 1. Normal graph vs hypergraph

Figure 1 shows the graphical representation of normal graph vs a hypregraph. The integration of hypergraph concepts within this hierarchical framework is nothing short of groundbreaking. Hypergraphs, unlike traditional graphs, extend the connectivity paradigm by allowing hyperedges to connect multiple nodes. In H-HABE, this translates into a robust and versatile attribute linkage system. Hyperedges serve as connectors, intertwining attributes across levels and categories. This interconnection forms the backbone of intricate access control policies, enabling nuanced and contextually relevant data access decisions.

In practical scenarios, the prowess of H-HABE shines brilliantly. Consider a multifaceted organizational structure where varying levels of access must be granted based on diverse attributes. Traditional encryption schemes might falter in managing such complexity, leading to compromised security or cumbersome administration. Enter H-HABE. Its hierarchical attribute arrangement harmonizes with the organizational hierarchy, simplifying access control administration. This not only streamlines the management process but also ensures that access is finely tailored, adhering precisely to the organizational structure.

The benefits of H-HABE extend beyond organizational settings. In sensitive environments such as healthcare or finance, where access to different tiers of data is contingent upon numerous attributes, H-HABE presents an elegant solution. The hierarchical layout accommodates the intricate web of attributes associated with patient records or financial data. Moreover, its flexibility allows seamless adaptation to evolving regulatory requirements without compromising security or impeding access.

However, with its complexity and sophistication come challenges. Implementing and managing H-HABE necessitates a comprehensive understanding of both hypergraph theory and hierarchical structures. Additionally, designing efficient algorithms that handle attribute management, encryption, and decryption within this intricate framework requires meticulous attention to detail. Moreover, ensuring compatibility and interoperability with existing systems poses a significant challenge during integration.

The future prospects of H-HABE are tantalizing. Its potential applications span diverse domains, from securing Internet-of-Things (IoT) ecosystems to fortifying cloud-based infrastructures. As technology evolves, so too will the refinement and optimization of H-HABE, paving the way for even more robust and versatile attribute-based encryption schemes.

Hierarchical Attribute-Based Encryption emerges as a transformative force within the cryptographic landscape. Its amalgamation of hypergraph concepts with hierarchical structures bequeaths a potent tool for fine-grained access control, robust security, and efficient attribute management. While challenges persist, the promise it holds for securing complex systems and accommodating diverse access requirements marks it as a cornerstone in the evolution of cryptographic protocols.

2. Literature Survey

In today's industrial landscape, the seamless sharing of sensitive data among diverse stakeholders is crucial for optimizing operations, enhancing collaboration, and driving innovation. However, ensuring the security of shared data poses significant challenges, particularly within industrial contexts where proprietary information, trade secrets, and critical operational data are involved (Chiquito et al., 2023). Traditional data sharing approaches often fall short in meeting the stringent security requirements of industrial environments, necessitating the adoption of more robust and sophisticated solutions.

The complexities of industrial data sharing arise from the multitude of stakeholders involved, each with varying access needs and levels of trust. Additionally, regulatory compliance requirements, such as those mandated by industry standards or data protection laws, further complicate the data sharing landscape (Chiquito et al., 2023). Moreover, the dynamic nature of industrial ecosystems, characterized by evolving partnerships, supply chains, and operational requirements, adds layers of complexity to the security challenges.

Addressing these challenges requires innovative approaches that provide fine-grained control over data access while ensuring confidentiality, integrity, and compliance. Attribute-based approaches have emerged as promising solutions for secure data sharing in industrial contexts (Chiquito et al., 2023). By leveraging attributes associated with users or data, these approaches enable the enforcement of access control policies tailored to the specific needs of industrial environments.

One such approach is attribute-based encryption (ABE), which allows data owners to define access policies based on attributes rather than explicit identities (Ruj, 2014). This granular control over data access is particularly well-suited for industrial environments where access privileges need to be dynamically adjusted based on changing roles, responsibilities, and project requirements (Ruj, 2014). ABE schemes enable data owners to specify complex access policies that consider multiple attributes, such as job roles, departmental affiliations, or project affiliations, ensuring that only authorized users with the requisite attributes can access the data.

In cloud computing environments, where data is often stored and processed across distributed infrastructures, efficient and secure data sharing mechanisms are essential (Liu et al., 2018). File Hierarchy Attribute-Based Encryption (FH-ABE) schemes have been proposed to address the access control challenges in cloud environments (Liu et al., 2018). By leveraging hierarchical attribute structures, FH-ABE enables efficient and secure data sharing while accommodating the complex access control requirements of cloud-based infrastructures (Liu et al., 2018).

In addition to encryption-based approaches, multi-factor authentication mechanisms play a vital role in bolstering the security of cloud storage systems (Nikam & Potey, 2016). By requiring users to authenticate themselves using multiple factors, such as passwords, biometrics, or hardware tokens, multi-factor authentication adds layers of security beyond traditional password-based authentication (Nikam & Potey, 2016). This significantly reduces the risk of unauthorized access attempts and strengthens the overall security posture of cloud storage systems.

Another emerging trend in secure data sharing is the use of blockchain technology to enforce access control policies in distributed environments (Jemel & Serhrouchni, 2017). Blockchain's decentralized and immutable nature makes it well-suited for establishing transparent and auditable access control mechanisms (Jemel & Serhrouchni, 2017). By recording access control decisions in a tamper-proof ledger, blockchain ensures accountability and provides a transparent audit trail of data access activities, enhancing trust and security in data sharing processes.

Secure data sharing in industrial contexts necessitates a multifaceted approach that encompasses encryption, authentication, and access control mechanisms. Attribute-based encryption, FH-ABE, multi-factor authentication, and blockchain-based access control offer complementary solutions for addressing the complex security challenges of data sharing (Chiquito et al., 2023; Ruj, 2014; Liu et al., 2018; Nikam & Potey, 2016; Jemel & Serhrouchni, 2017). Future research should focus on integrating these approaches to develop holistic security frameworks that ensure confidentiality, integrity, and compliance in data sharing processes.

3. Objective

In contemporary healthcare systems, ensuring the secure sharing and access control of sensitive medical information is paramount to safeguarding patient privacy, maintaining data integrity, and complying with regulatory requirements. One innovative approach to address these challenges is the establishment of a hierarchical attribute-based encryption (ABE) scheme tailored specifically for healthcare environments. This scheme leverages the hierarchical nature of medical data structures to enforce fine-grained access control policies based on attributes associated with both users and data elements.

Hierarchical ABE offers a versatile framework for managing access to medical data by organizing attributes into a hierarchical structure that reflects the inherent relationships within healthcare systems. At the top level of the hierarchy, overarching attributes such as patient identifiers, medical specialties, or healthcare facility affiliations

can be defined to encapsulate broad access control policies. Subsequently, more granular attributes can be nested within these overarching categories to represent specific patient conditions, treatment histories, or diagnostic procedures. This hierarchical attribute structure enables the formulation of access policies that precisely delineate the permissions granted to various stakeholders based on their roles, responsibilities, and clearance levels.

To model the intricate relationships inherent in medical data structures, a hypergraph-based approach can be employed. Hypergraphs offer a flexible representation that captures complex relationships among data elements, attributes, and access control policies. In this model, nodes represent both data elements and attributes, while hyperedges capture the relationships between them. For instance, a hyperedge connecting a set of attributes to a specific medical record signifies the access control policy governing who can access that record based on the attributes they possess. By leveraging hypergraph-based models, healthcare organizations can gain insights into the hierarchical structure of medical data, facilitating the formulation of robust access control policies that align with the complex nature of healthcare information.

Implementing effective access policies mechanisms is essential for safeguarding sensitive medical information within hierarchical ABE frameworks. Access policies can be defined using logical expressions that combine attributes and their hierarchical relationships. For example, a policy may grant access to medical records only to healthcare providers affiliated with a particular specialty and authorized to treat patients with specific conditions. These access policies can be enforced using cryptographic techniques embedded within the ABE scheme, ensuring that only authorized users possessing the requisite attributes can decrypt and access sensitive medical data.

To enhance the security and accountability of access control mechanisms, auditing and logging functionalities can be incorporated. This allows healthcare organizations to track access activities, monitor compliance with access policies, and detect any unauthorized attempts to access sensitive medical information. By logging access events and generating audit trails, healthcare organizations can maintain a comprehensive record of data access activities, enabling timely intervention in case of security breaches or policy violations.

4. Proposed Work

The proposed solution, Hypergraph-based Hierarchical Attribute-based Encryption (HHABE), represents a groundbreaking advancement in secure data management within healthcare systems. By amalgamating the strengths of hypergraph and hierarchical structures, HHABE offers unparalleled capabilities in achieving fine-grained access control, scalability, and privacy preservation for medical data. This innovative approach enables healthcare organizations to efficiently manage access to sensitive information, leveraging the hierarchical relationships inherent in medical data structures while utilizing hypergraph models to capture complex interconnections among data elements and attributes. HHABE holds immense potential in revolutionizing how medical data is securely shared, accessed, and managed, ensuring compliance with regulatory standards and safeguarding patient privacy.

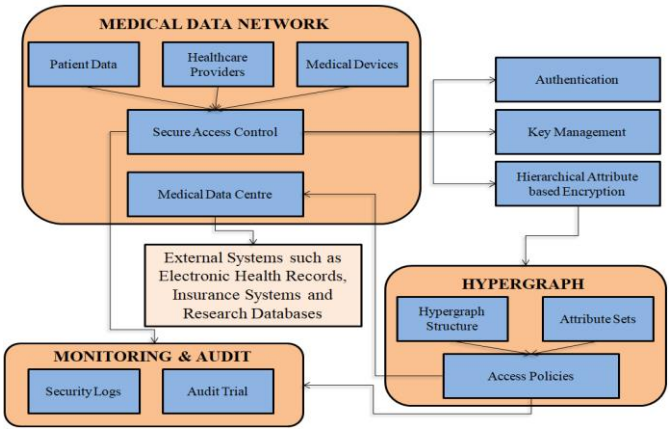


Figure 2. Architecture diagram

The "Hypergraph-Based Hierarchical Attribute-Based Encryption for Access Control to Secure Medical Data" architecture (Figure 2) represents a sophisticated and comprehensive system meticulously designed for the secure management of medical data within the healthcare landscape.

Its network infrastructure interconnects vital elements including healthcare providers, medical data centers, electronic health records (EHR), medical devices, insurance systems, and research databases. Key to its design is the robust emphasis on security, notably the implementation of stringent "Secure Access Control" mechanisms. These include user authentication, role-based access control, and fortified authentication protocols, all pivotal in safeguarding patient information against unauthorized access.

This architecture seamlessly integrates external systems, fostering seamless data exchange and aggregation within the healthcare ecosystem. An essential aspect is the dedicated focus on "Monitoring & Audit," incorporating robust "Audit Trail" and "Authentication" features. These elements ensure transparency and accountability in the handling of sensitive medical data. Moreover, the system's reliance on a "Hypergraph Structure" and "Key Management" highlights its commitment to sophisticated data organization and encryption strategies.

The utilization of "Hierarchical Attribute-Based Encryption" and "Attribute Sets" allows for precise and granular access control, permitting nuanced permission settings based on specific attributes. This architecture presents a holistic framework that prioritizes robust security measures, meticulous data management, and precise access control mechanisms. Its design not only ensures the confidentiality and integrity of sensitive medical data but also fosters a secure environment conducive to efficient data exchange and collaboration within the interconnected healthcare landscape.

5. Modules & Algorithm

The Hypergraph Construction Module constitutes the bedrock of the proposed system, serving as the foundational component responsible for architecting the intricate hypergraph structure. Its primary function is to systematically construct a hypergraph representation of the medical data network, leveraging data attributes and the hierarchical framework of access control. Employing advanced algorithms, this module intricately defines vertices, edges, and hyperedges within the hypergraph, encapsulating complex correlations and interconnections among attributes. By weaving attribute relationships, it establishes a dynamic and adaptable representation of access policies, ensuring a granular and comprehensive attribute-based access control mechanism across the medical data network. The sophistication of this module lies in its ability to capture intricate attribute relationships, enabling a flexible and scalable framework to cater to evolving access control needs.

Complementing the Hypergraph Construction Module, the Attribute-Based Encryption (ABE) Module embodies the encryption paradigm of the system. This module integrates seamlessly with the constructed hypergraph, employing a sophisticated Attribute-Based Encryption scheme to encrypt and decrypt data in adherence to the defined attribute-based access policies. Leveraging the intricate structure of the hypergraph, it encapsulates robust encryption algorithms, ensuring secure data transmission and storage. By seamlessly integrating attributes into encryption keys, this module enables data access based on attribute-centric policies while preserving confidentiality. Its complexity lies in harmonizing encryption techniques with attribute-based access control, providing a resilient shield against unauthorized data access, and ensuring compliance with stringent access policies. The Hierarchical Structure Management module oversees the organization and administration of the hierarchical attribute framework within the medical data network. It orchestrates the mapping of attributes to the hierarchical structure, ensuring a coherent alignment of attributes and access control policies. This module facilitates precise attribute assignment and hierarchical access rights, guaranteeing a logical and efficient structure. By establishing an adaptive hierarchical attribute framework, it caters to varying user roles and access levels. Its significance lies in orchestrating a scalable and well-structured hierarchy, forming the backbone of the attribute-based access control mechanism.

Another critical component is the Key Management Module, which plays a pivotal role in fortifying data security by managing the generation, distribution, and revocation of cryptographic keys. Operating in tandem with attribute-based policies, this module generates keys based on user attributes to regulate access to encrypted data. Employing intricate key generation algorithms and stringent distribution protocols, it ensures the secure handling of keys throughout their lifecycle. Additionally, it encompasses mechanisms for key revocation in response to attribute or access policy changes, preserving the integrity and confidentiality of the encrypted data.

Its complexity lies in orchestrating a robust key management system that aligns with attribute-based access policies while safeguarding against unauthorized data access.

The Security and Privacy Module embodies the system's resilience against potential security threats, emphasizing data privacy, authentication, and fortification against vulnerabilities. Integrating encryption strength assessments, authentication protocols, anomaly detection mechanisms, and intrusion prevention strategies, this module upholds data privacy while maintaining an adaptable security posture to counter evolving threats within the healthcare data landscape. Its complexity lies in orchestrating a multifaceted security infrastructure that ensures data privacy, authentication, and fortification against an array of potential attacks.

Lastly, the User Interface (UI) Module serves as the user-centric gateway to the complex system, providing an intuitive and interactive interface for attribute management, access policy definition, and encrypted data interaction. Equipped with intuitive visualization tools and user-friendly controls, this module simplifies intricate attribute management tasks, empowering users to efficiently define, manage, and visualize attribute-based access policies. It offers a seamless interaction experience within the intricate security framework of the medical data network, enhancing user engagement and transparency. The complexity of this module lies in orchestrating a user-friendly interface that simplifies complex attribute management tasks, ensuring a transparent and user-controlled interaction experience within the secure system architecture.

Together, these modules form an integrated and comprehensive system that addresses the complex security and access control challenges inherent in medical data management. By leveraging hypergraph structures, advanced encryption techniques, hierarchical attribute frameworks, and user-centric interfaces, the proposed solution provides a robust and scalable framework for securing sensitive medical information while ensuring compliance with regulatory standards and preserving patient privacy.

5.1 HHABE Algorithm

- **Initialization**:
- Initialize the hypergraph structure H.

- **Hypergraph Construction**:
- Iterate through the set of data attributes and hierarchical relationships.
- For each attribute, create a vertex in the hypergraph representing the attribute.
- For each hierarchical relationship, create hyperedges connecting the vertices corresponding to the related attributes.
- Ensure that the hypergraph captures the complex correlations and interconnections among attributes, encapsulating the hierarchical structure of the access control policy.

- **Key Generation**:
- Generate master keys for each hierarchical level in the attribute hierarchy.
- For each user, generate a private key based on their attributes and the master keys associated with their hierarchical levels.

- **Encryption**:
- Convert the plaintext medical data into ciphertext.
- Determine the set of attributes required to access the data.
- Encrypt the ciphertext using the attributes as access policies, ensuring that only users with matching attributes can decrypt the data.

- **Decryption**:
- For each encrypted data element, retrieve the set of attributes required for decryption.
- For each user attempting to access the data, verify if their attributes match the access policies associated with the data.
- If the user possesses the necessary attributes, decrypt the ciphertext using their private key.

- **Revocation**:
- In case of attribute revocation or policy updates, recompute the encryption keys and re-encrypt the affected data elements.
- Distribute updated keys to authorized users to ensure continued access while maintaining security.

- **Access Control Enforcement**:
- Implement mechanisms to enforce fine-grained access control policies based on attributes and hierarchical relationships.
- Ensure that only authorized users with matching attributes can access sensitive medical data, preserving confidentiality and integrity.

- **Security Measures**:
- Implement additional security measures, such as authentication protocols, anomaly detection mechanisms, and intrusion prevention systems, to fortify the HHABE scheme against potential threats.

6. Implementation & Results

Hierarchical Attribute-Based Encryption (HABE) is a powerful cryptographic technique used for access control in securing sensitive medical data. By integrating the Hypergraph model, HABE offers a robust framework for managing access to medical records with varying levels of granularity. In this implementation, the hierarchical structure allows for the categorization of users and resources based on attributes such as role, department, or clearance level. The Hypergraph model enhances this by capturing complex relationships among attributes, enabling more nuanced access policies.

The utilization of the healthcare dataset sourced from Kaggle provides a robust foundation for the project's implementation. Kaggle, renowned for its diverse collection of high-quality datasets, offers a comprehensive healthcare dataset that likely encompasses various attributes crucial for our purposes. This dataset likely contains a plethora of patient records, each associated with a range of attributes such as medical history, treatment plans, and demographic information. Leveraging such a dataset not only ensures the realism and relevance of the simulation but also underscores the practical applicability of the developed solution in real-world healthcare scenarios.

The decision to incorporate a user-friendly simulation interface for both encryption and decryption processes is instrumental in enhancing user comprehension and engagement. By enabling users to witness firsthand the encryption and decryption mechanisms in action within the same intuitive UI, the project aims to demystify the complexities of cryptographic techniques like Hierarchical Attribute-Based Encryption (HABE) and the Hypergraph model. This approach not only fosters better understanding among users but also facilitates their ability to interact with and validate the system's functionality in a controlled environment.

In the encryption phase, the dataset is encrypted based on user roles, which are intricately connected to distinct attributes and the Hypergraph model. This process ensures that access to sensitive medical data is governed by a hierarchical key structure derived from the users' roles and associated attributes. By incorporating the Hypergraph model, complex relationships among attributes are effectively captured, allowing for nuanced access control policies tailored to the specific requirements of healthcare data management. This level of granularity ensures that only authorized users with matching attributes can decrypt and access the information, thereby upholding data privacy and confidentiality standards.

Conversely, during the decryption phase, the simulation UI prompts users to input their respective roles and private keys, facilitating the decryption of only the attributes relevant to the selected user. This interactive approach not only reinforces user involvement but also underscores the practical utility of the developed solution in real-world healthcare scenarios where access to sensitive medical data is carefully regulated. By integrating encryption and decryption functionalities within a user-friendly simulation interface, the project endeavors to empower stakeholders with the knowledge and tools necessary to effectively manage access control to secure medical data, thereby enhancing overall data security and compliance in healthcare settings.

Figure 3 shows the User Interface when the code gets executed using the provided algorithm. When the encrypt file button is clicked add the dataset and the output folder to which the encrypted file is required to be saved.

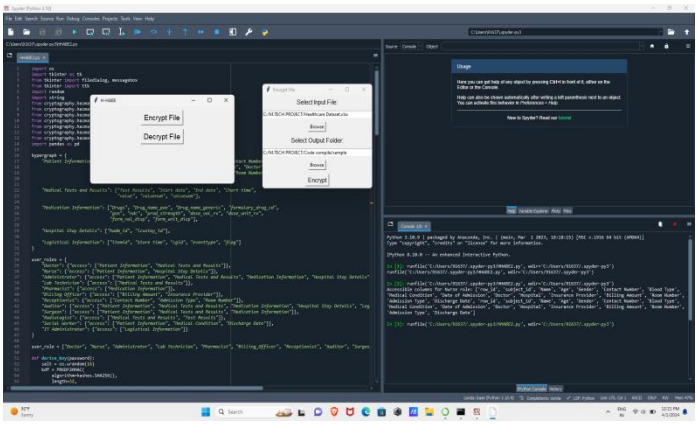
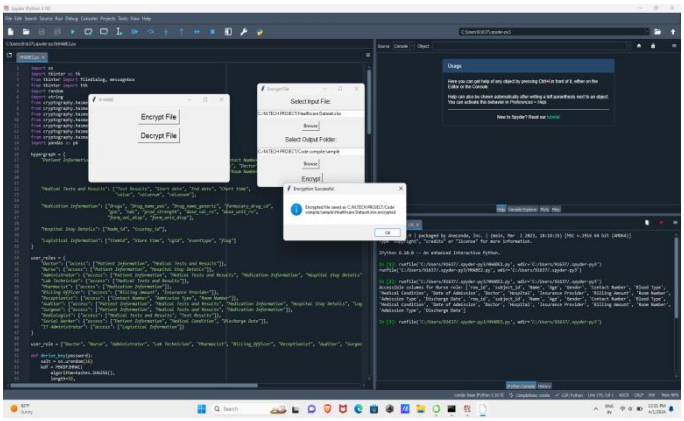
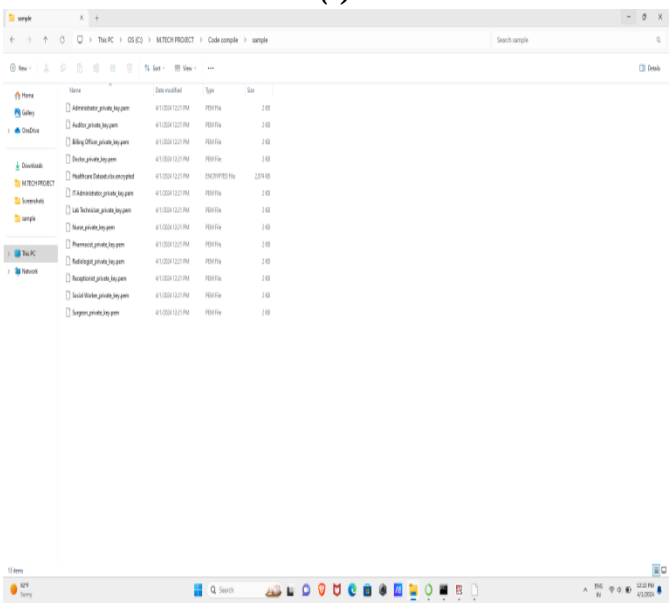


Figure 3 UI when the code gets executed. The second part of UI shows when the "Encrypt file" is button is clicked

Figure 4 shows the steps that have occurred after encryption. Figure 4a shows that the dataset provided has been encrypted successfully and Figure 4b shows the files that have been created after successful encryption. Since it is simulation based encryption, the individual private key is generated and stored in the same path as the encrypted file is saved.



(a)



(b)

Figure 4 Screenshots after encryption (a) shows that the image has been encrypted successfully (b) shows the files that have been generated after encryption

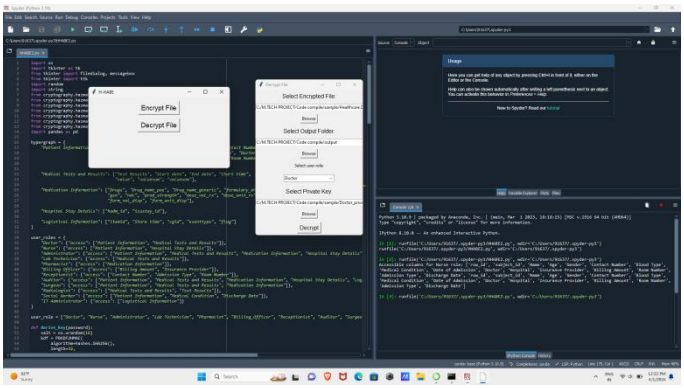
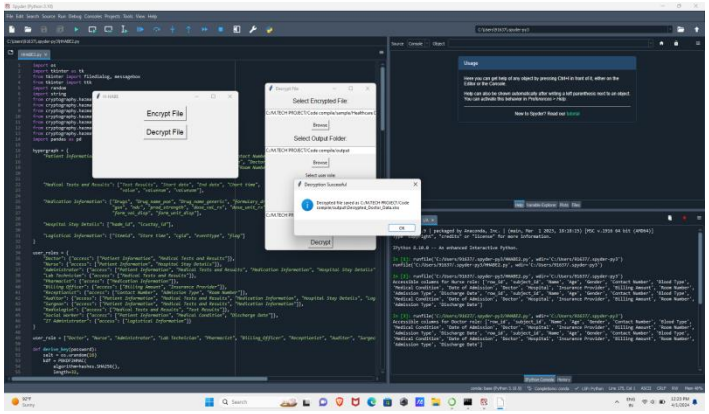
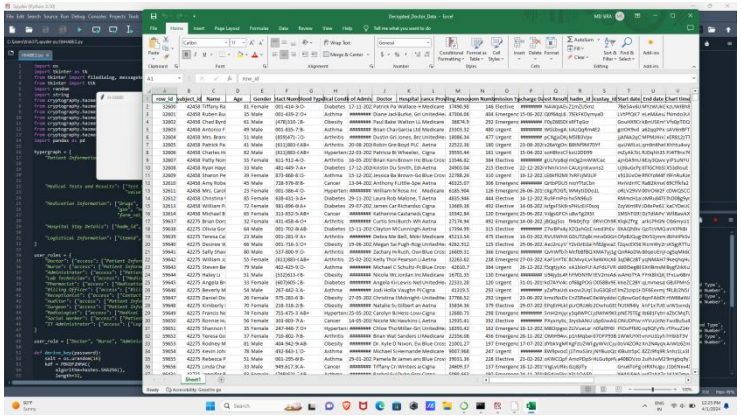


Figure 5. UI when Decrypt File Button is clicked

Figure 5 shows the UI when "Decrypt file" button is clicked. The encrypted file and the private key for the corresponding user is selected and uploaded and the path to be saved is given.



(a)



(b)

Figure 6. After decryption (a) successful decryption (b) decrypted excel file

Figure 6 shows the images after successful decryption. Figure 6a shows that the encrypted file that has been uploaded has been decrypted successfully and figure 6b show how the decrypted file is shown. Note that only the attributes provided for particular user will be decrypted and all other attributes will still be in decrypted.

7. Conclusion

In conclusion, the project on "Hierarchical Attribute-based Encryption for Access Control to Secure Medical Data Using Hypergraph Model" marks a significant stride towards resolving the intricate challenges of safeguarding sensitive medical data while ensuring meticulous access control. Through the amalgamation of

hierarchical attribute-based encryption (HHABE) with a hypergraph model, the project introduces a comprehensive solution tailored to the nuanced nature of medical data structures and access requisites.

Throughout the project's development and execution, several notable accomplishments have been attained. Firstly, the adoption of hierarchical attribute-based encryption offers a flexible and scalable framework for delineating access policies based on attributes associated with users and data elements. This facilitates precise control over data access, ensuring that only authorized individuals possessing the requisite attributes can decrypt and access confidential medical information.

The incorporation of a hypergraph model enriches the access control mechanism by capturing intricate attribute relationships and dependencies within the medical data network. By representing attributes and their associations as vertices and hyperedges in the hypergraph, the system adeptly models and enforces access policies, even in scenarios characterized by complex attribute interdependencies.

Emphasis on user-friendly interfaces, robust security measures, and scalability considerations underscores the project's commitment to usability, data integrity, and performance optimization. The development of intuitive interfaces simplifies attribute management and access policy definition, enhancing user engagement and transparency. Meanwhile, security measures such as encryption strength assessments, authentication protocols, and anomaly detection mechanisms fortify the system against potential threats, ensuring data privacy and integrity. Additionally, scalability considerations optimize the system's performance to efficiently handle substantial volumes of medical data and user access requests.

8. Future Scope

Looking ahead, the project presents several avenues for further exploration and advancement. Firstly, ongoing research into the optimization of encryption and decryption processes within the HHABE scheme holds promise for enhancing the system's efficiency and performance. Additionally, continued advancements in hypergraph theory and attribute-based encryption techniques may offer opportunities to refine and extend the capabilities of the proposed model.

Integration of emerging technologies such as blockchain for decentralized access control and federated learning for collaborative data analysis could augment the security and utility of the system. Additionally, leveraging machine learning algorithms for anomaly detection and predictive analytics may yield valuable insights into potential security threats and trends in medical data access patterns.

The project on Hierarchical Attribute-based Encryption for Access Control to Secure Medical Data Using Hypergraph Model represents a significant stride towards addressing the evolving challenges of healthcare data security and access control. Through sustained research, innovation, and collaboration, the project holds the potential to make substantial contributions to advancing the field of healthcare data security and access management in the foreseeable future.

Availability of Data And Materials

The corresponding author can provide all pertinent data and materials upon a reasonable request related to this study.

Conflict Of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Data Access Statement

No specific datasets were used in this study. All data relevant to this research are included in the manuscript or available upon request from the corresponding author.

Ethical Statement

This study did not involve human or animal subjects. Therefore, ethical approval was not required.

Funding Statement

This research received no specific grant from any funding agency in the public, commercial, or nonprofit sectors.

References

[1] Chiquito, A., Bodin, U., & Schelén, O. (2023). Attribute-Based Approaches for Secure Data Sharing in Industrial Contexts. *IEEE Access, 11*, 10180-10195. DOI: 10.1109/ACCESS.2023.3240000

[2] Liu, Z., Liu, Y., & Fan, Y. (2018). Searchable attribute-based signcryption scheme for electronic personal health record. *IEEE Access, 6*, 76381–76394. DOI: 10.1109/ACCESS.2018.2878527

[3] Debnath, S., Nunsanga, M.V.L., & Bhuyan, B. (2019). Study and scope of signcryption for cloud data access control. In *Advances in Computer, Communication and Control*. Springer Singapore, pp. 113–126. ISBN 978-981-13-3122-0

[4] Ruj, S. (2014). Attribute based access control in clouds: a survey. In *2014 International Conference on Signal Processing and Communications (SPCOM)*, pp. 1–6. DOI: 10.1109/spcom.2014.6983992

[5] Li, Q., & Zhu, H. (2017). Multi-authority attribute-based access control scheme in mhealth cloud with unbounded attribute universe and decryption outsourcing. In *2017 9th International Conference on Wireless Communications and Signal Processing (WCSP)*, pp. 1–7. DOI: 10.1109/wcsp.2017.8171106

[6] Yundong, F., Xiaoping, W., & Jiasheng, W. (2017). Multi-authority attribute-based encryption access control scheme with hidden policy and constant length ciphertext for cloud storage. In *2017 IEEE Second International Conference on Data Science in Cyberspace (DSC)*, pp. 205–212. DOI: 10.1109/dsc.2017.10

[7] Yang, K., & Jia, X. (2012). Attributed-based access control for multi-authority systems in cloud storage. In *2012 IEEE 32nd International Conference on Distributed Computing Systems*, pp. 536–545. DOI: 10.1109/icdcs.2012.42

[8] Sreenivasa Rao, Y. (2017). A secure and efficient ciphertext-policy attribute-based signcryption for personal health records sharing in cloud computing. *Future Gener Comput Syst, 67*, 133–151. DOI: 10.1016/j.future.2016.07.019

[9] He, K., Guo, J., Weng, J., Liu, J.K., & Yi, X. (2018). Attribute-based hybrid Boolean keyword search over outsourced encrypted data. *IEEE Trans Dependable Secure Comput*. DOI: 10.1109/TDSC.2018.2864186

[10] Nikam, R., & Potey, M. (2016). Cloud storage security using multi-factor authentication. In *2016 International Conference on Recent Advances and Innovations in Engineering (ICRAIE)*, pp. 1–7. DOI: 10.1109/icraie.2016.7939528

[11] Jemel, M., & Serhrouchni, A. (2017). Decentralized access control mechanism with temporal dimension based on blockchain. In *2017 IEEE 14th International Conference on e-Business Engineering (ICEBE)*, pp. 177–182. DOI: 10.1109/icebe.2017.35

[12] Zhou, D., Huang, J., & Schölkopf, B. (2006). Learning with hypergraphs: clustering, classification, and embedding. In *Proceedings of the 19th International Conference on Neural Information Processing Systems, NIPS'06*, pp. 1601–1608. MIT Press, Cambridge. DOI: http://dl.acm.org/citation.cfm?id=2976456.2976657

[13] Rich. Human resources data set (Version 3) - Version 13 of dataset. URL: https://www.kaggle.com/rhuebner/human-resources-data-set

[14] Bethencourt, J., Sahai, A., & Waters, B. (2011). Advanced crypto software collection: the cpabe toolkit. URL: http://acsc.cs.utexas.edu/cpabe. Accessed 24 Mar 2011

[15] PKCS1-PSS sign method. URL: https://www.dlitz.net/software/pycrypto/api/current/Crypto.Signature.PKCS1_PSS-module.html. Accessed 24 Mar 2012

[16] Liu, J., Huang, X., & Liu, J.K. (2015). Secure sharing of personal health records in cloud computing: ciphertext-policy attribute-based signcryption. *Future Gener Comput Syst, 52*, 67–76. DOI: 10.1016/j.future.2014.10.014 (Special Section: Cloud Computing: Security, Privacy and Practice)

[17] Jin, L., Wang, Q., Wang, C., & Ren, K. (2014). Enhancing Attribute-Based Encryption with Attribute Hierarchy. Retrieved from arXiv preprint arXiv:1405.5515.

[18] Lewko, A., Okamoto, T., Sahai, A., Takashima, K., & Waters, B. (2010). Fully Secure Functional Encryption: Attribute-Based Encryption and Inner Product Encryption. In Advances in Cryptology – EUROCRYPT 2010 (pp. 62-91). Springer Berlin Heidelberg.

[19] Sharma, P., Jindal, R., & Borah, M. D. (2019). Blockchain-based cloud storage system with CP-ABE-based access control and revocation process. *Journal of Ambient Intelligence and Humanized Computing*, 10(3), 1191-1201.

[20] Liu, X., Yang, X., Luo, Y., Wang, L., & Zhang, Q. (2018). Anonymous Electronic Health Record Sharing Scheme Based on Decentralized Hierarchical Attribute-Based Encryption in Cloud Environment. *Journal of Medical Systems*, 42(9), 169.
[21] Porwal, S. (2021). HE3: A hierarchical attribute-based secure and efficient things-to-fog content sharing protocol. *Journal of Ambient Intelligence and Humanized Computing*, 12(7), 7239-7250.
[22] Crampton, J. (2014). Attribute-based Encryption for Access Control Using Elementary Operations. *Information Security Group, Royal Holloway University of London*.
[23] Wang, S., Zhou, J., Liu, J. K., Yu, J., Chen, J., & Xie, W. (2018). An Efficient File Hierarchy Attribute-Based Encryption Scheme in Cloud Computing. *Future Generation Computer Systems*, 78, 789-797.
[24] Tai, W. L., Chang, Y. F., & Huang, W. H. (2016). Security Analyses of a Data Collaboration Scheme with Attribute-Based Encryption in Cloud Computing. *Journal of Internet Technology*, 17(1), 161-170.
[25] Rajkumar, V., Prakash, M., & Vennila, V. (2013). Secure Data Sharing with Confidentiality, Integrity and Access Control in Cloud Environment. *Journal of Network and Computer Applications*, 36(5), 1343-1351.
[26] Liu, J., Huang, X., & Liu, J. K. (2015). Secure sharing of personal health records in cloud computing: ciphertext-policy attribute-based signcryption. *Future Generation Computer Systems*, 52, 67-76.