IJRAR.ORG E-ISSN: 2348-1269, P-ISSN: 2349-5138

INTERNATIONAL JOURNAL OF RESEARCH AND ANALYTICAL REVIEWS (IJRAR) | IJRAR.ORG

An International Open Access, Peer-reviewed, Refereed Journal

A Lightweight Policy Update Scheme for Outsourced Personal Health.

Dathatreya Gorantla, Bhuma Vamsi Krishna, Raju P, Biju Mathew

School of Computer Science, Presidency University, Bengaluru.

Under the guidance of,

Ms. Alina Raheen

School of Computer Science,

Presidency University, Bengaluru

ABSTRACT

With high flexibility and accessibility of data outsourcing environment such as cloud computing environment, several healthcare providers implement electronic personal health records (PHRs) to enable individual patients to manage their own health data in such resilient and scalable environment. However, PHRs contain highly sensitive information of which the security and privacy issues are the critical concern. Besides, PHRs owners should be capable to flexibly and securely define their own access policy for their outsourced data. In addition to the basic authentication feature, existing commercial cloud platforms usually provide symmetric or public key encryption as an optional feature to support data confidentiality for their tenants. However, such traditional encryption schemes are not suitable for data outsourcing environment because of high key management overhead of symmetric encryption and high maintenance cost for handling multiple copies of cipher text for public key encryption solution. In this paper, we design and develop a secure and fine-grained access control scheme with lightweight access policy update for outsourced PHRs. Our proposed scheme is based on the cipher text policy attribute-based encryption (CP-ABE) and proxy re-encryption (PRE). In addition, we introduce a policy versioning technique to support the full traceability of policy changes. Finally, we conducted the performance evaluation to demonstrate the efficiency of the proposed scheme.

KEYWORDS: PHRs, access control, CP-ABE, policy update, proxy re-encryption, police versioning, performance evaluation.

CHAPTER 1

1.1 INTRODUCTION

1.1 Aim of the Project:

In an outsourced data sharing environment such as cloud storage j system, the outsourced server must be available all the time to provide unlimited access to shared data and the services. Nowadays, many companies and individuals prefer to store their valuable data in outsourced servers such as cloud storage due to cost saving and efficient resource management provided by cloud providers. Regarding to the privacy and security issue, data owners usually encrypt their data before outsourcing it to the cloud server. Encrypting data is the most suitable way to protect the sensitive data from unauthorized access. Nevertheless, encryption alone is not adequate to support rigorous security control. Access control mechanism is another security perimeter generally required. To address this concern, attribute-based encryption (ABE) has been extensively adopted by many works. ABE provides a ‘‘one-to-many’’ encryption scheme with finegrained access control. Also, it possesses both encryption and access control capabilities. There are two types of ABE: ciphertext-policy attribute-based encryption (CP-ABE) and key-policy attribute-based encryption (KP-ABE). In CPABE, attributes are used to construct the user’s decryption key, and access policy is used to encrypt the data. For KPABE, the user key is associated with the access policy while the encryption is done by a set of attributes. In security enforcement point of view, CP-ABE is preferred as the data owner can specify his/her own policy to encrypt the data. The advantages to using CP-ABE is for group key management. One of them is the decoupling of abstract attributes from actual keys. It reduces communication overhead and provides a fine-grained data access control. Also, it achieves flexible one-to-many encryption instead of one-to-one; it’s envisioned as a promising tool for addressing the problem of secure and fine-grained data sharing and decentralized access control. Nevertheless, CP-ABE introduces expensive overheads including ciphertext re-encryption, key re-generation, and key re-distribution when there is attribute revocation or policy update. These revocation and policy update operations must be done carefully as the propagation effect to both ciphertext and user decryption key is high.

1.2 Scope of the Project

The scope of this project encompasses the development and implementation of a lightweight policy update scheme tailored for outsourced Personal Health Records (PHRs) sharing. The scheme will address the critical challenges of access control policy management, ensuring the security and privacy of sensitive health data. This project will involve the design of efficient algorithms and mechanisms to facilitate seamless policy updates, while minimizing computational overhead. The scheme will be compatible with existing PHR systems and will prioritize user- friendliness, scalability, and robust security measures. The ultimate goal is to provide individuals with a secure and efficient means of managing their health information in outsourced PHR environments.

1.3 Project Modules:

1.Authentication Module:

Ensure secure user authentication to access personal health records.

Implement multi-factor authentication for enhanced security.

2.Policy Management Module:

Create a user-friendly interface for managing access policies.

Allow users to define and update sharing preferences easily.

3.Encryption and Security Module:

Implement robust encryption techniques to safeguard sensitive health data.

Regularly update security protocols to address emerging threats.

4.Audit Trail Module:

Incorporate an audit trail system to track data access and modifications.

Enable users to review and monitor who has accessed their health records.

5.Notification System:

Develop a notification mechanism for users to be informed of policy updates.

Ensure transparency in communicating changes to sharing settings.

6.Compliance Module:

Stay compliant with relevant healthcare regulations and standards.

Conduct regular audits to ensure adherence to privacy guidelines.

7.User Education and Training:

Provide educational resources to users about the importance of privacy.

Offer training sessions on utilizing and updating sharing policies.

8.Data Segmentation Module:

Implement data segmentation to restrict access based on specific criteria.

Allow users to customize sharing based on the type of health information.

9.Interoperability:

Ensure compatibility with various health record systems for seamless data sharing.

Facilitate secure data exchange with other healthcare providers.

10.Scalability and Performance Optimization:

Design the system to handle a growing volume of personal health records.

Optimize performance to provide a responsive user experience.

CHAPTER 2

2.0 LITERATURE REVIEW

A. Sahai and B. Waters,"Fuzzy identity-based encryption," in Proc.24th Annu. Int. Conf. Appl. Cryptograph. Technique (EUROCRYPT) (Lecture Notes in Computer Science). Berlin, Germany: Springer, May 2015, pp. 457–473

We introduce a new type of Identity-Based Encryption (IBE) scheme that we call Fuzzy Identity-Based Encryption. In Fuzzy IBE we view an identity as set of descriptive attributes. A Fuzzy IBE scheme allows for a private key for an identity, ω, to decrypt a ciphertext encrypted with an identity, ω 0 , if and only if the identities ω and ω 0 are close to each other as measured by the "set overlap" distance metric. A Fuzzy IBE scheme can be applied to enable encryption using biometric inputs as identities; the error-tolerance property of a Fuzzy IBE scheme is precisely what allows for the use of biometric identities, which inherently will have some noise each time they are sampled. Additionally, we show that Fuzzy-IBE can be used for a type of application that we term "attribute-based encryption". In this paper we present two constructions of Fuzzy IBE schemes. Our constructions can be viewed as an Identity-Based Encryption of a message under several attributes that compose a (fuzzy) identity. Our IBE schemes are both error-tolerant and secure against collusion attacks. Additionally, our basic construction does not use random oracles. We prove the security of our schemes under the Selective-ID security model.

J.Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in Proc. IEEE Symp. Secur. Privacy, Oakland, CA, USA, May 2007, pp. 321–334.

In several distributed systems a user should only be able to access data if a user posses a certain set of credentials or attributes. Currently, the only method for enforcing such policies is to employ a trusted server to store the data and mediate access control. However, if any server storing the data is compromised, then the confidentiality of the data will be compromised. In this paper we present a system for realizing complex access control on encrypted data that we call Cipher text-Policy Attribute-Based Encryption. By using our techniques encrypted data can be kept confidential even if the storage server is untrusted; moreover, our methods are secure against collusion attacks. Previous Attribute Based Encryption systems used attributes to describe the encrypted data and built policies into user's keys; while in our system attributes are used to describe a user's credentials, and a party encrypting data determines a policy for who can decrypt. Thus, our methods are conceptually closer to traditional access control methods such as Role-Based Access Control (RBAC). In addition, we provide an implementation of our system and give performance measurements.

Summary: John Bethencourt, Amit Sahai, Brent Waters works based on the sensitive data is shared and stored by third-party sites on the Internet.

S. Belguith, N. Kaaniche, and G. Russello, "PU-ABE: Lightweight attribute-based encryption supporting access policy update for cloud assisted IoT," in Proc. IEEE 11th Int. Conf. Cloud Comput. (CLOUD), Jul. 2018, pp. 924–927.

Cloud-assisted IoT applications are gaining an expanding interest, such that IoT devices are deployed in different distributed environments to collect and outsource sensed data to remote servers for further processing and sharing among users. On the one hand, in several applications, collected data are extremely sensitive and need to be protected before outsourcing. Generally, encryption techniques are applied at the data producer side to protect data from adversaries as well as curious cloud provider. On the other hand, sharing data among users requires fine grained access control mechanisms. To ensure both requirements, Attribute Based Encryption (ABE) has been widely applied to ensure encrypted access control to outsourced data. Although, ABE ensures fine grained access control and data confidentiality, updates of used access policies after encryption and outsourcing of data remains an open challenge. In this paper, we design PU-ABE, a new variant of key policy attribute based encryption supporting efficient access policy update that captures attributes addition and revocation to access policies. PU-ABE contributions are multifold. First, access policies involved in the encryption can be updated without requiring sharing secret keys between the cloud server and the data owners neither re-encrypting data. Second, PU-ABE ensures privacy preserving and fine grained access control to outsourced data. Third, ciphertexts received by the end-user are constant sized and independent from the number of attributes used in the access policy which affords low communication and storage costs

Summary: Sana Belguith , Nesrine Kaaniche and Giovanni Russello worked for data security.

J. Li, S. Wang, Y. Li, H. Wang, H. Wang, H. Wang, J. Chen, and Z. You, "An efficient attribute-based encryption scheme with policy update and file update in cloud computing," IEEE Trans. Ind. Informat., vol. 15, no. 12, pp. 6500– 6509, Dec. 2019.

Recently, more and more users and enterprises have entrusted data storage and platform construction to cloud computing platform. Under this background, attribute-based encryption (ABE) mechanism is an alternative to fill the drawbacks of traditional encryption. However, there exist some security issues when access policy and file need to be updated. And the ABE has the problems of excessive computation and storage costs. In this paper, an efficient ciphertext-policy ABE (CP-ABE) scheme with policy update and file update is proposed in cloud computing. The ciphertext components generated by first encryption can be shared when the policy update and file update happens. It reduces the storage and communication costs of the client, and the computational cost of the PCSP. Moreover, the proposed scheme is proved to be secure under the decision q-parallel BDHE. Finally, experimental simulation shows that the proposed scheme is highly efficient in terms of policy update and file update.

M. Mambo and E. Okamoto, ‘‘Proxy cryptosystems: Delegation of the power to decrypt cipher texts,’’ IEICE Trans., vol. E80-A, no. 1, pp. 54–63, 1997.

Proxy cryptosystem, first proposed by Mambo and Okamoto [M.Mambo, E. Okamoto, Proxy cryptosystem: delegation of a power to decrypt ciphertexts, IEICE Trans. Fundam. Electron. Commun. Comput. Sci. E80-A/1 (1997) 54–63], allows the original decryptor to delegate his decrypting capability to the proxies. However, until now, no practical proxy cryptosystem modes are proposed. Therefore, in this paper, we present a novel proxy cryptosystem model: proxy cryptosystem based on time segmentation. Under this mode, a security analysis model will be proposed. Furthermore, a proxy cryptosystem scheme is presented as an example. We will show that the proposed scheme is proven security in the proposed security analysis model. Finally, we will give the ID-based version of this construction.

K. Liang, W. Susilo, and J. K. Liu, ‘‘Privacy-preserving cipher text multisharing control for big data storage,’’ IEEE Trans. Inf. Forensics Security, vol. 10, no. 8, pp. 1578–1589, Aug. 2015. [8] S. Fugkeaw and H. Sato, ‘‘Embedding lightweight proxy re- encryption for efficient attribute revocation in cloud computing,’’ J. High Perform. Comput. Netw., vol. 9, no. 4, pp. 299–309, 2016.

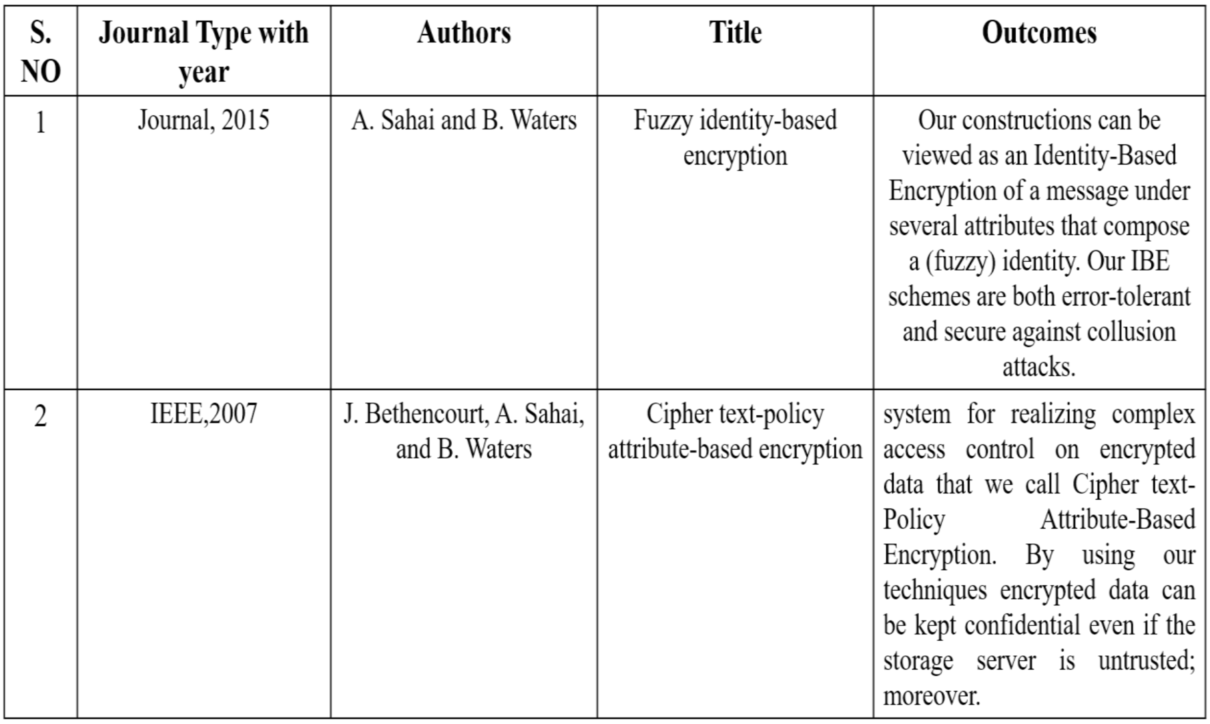
The need of secure big data storage service is more desirable than ever to date. The basic requirement of the service is to guarantee the confidentiality of the data. However, the anonymity of the service clients, one of the most essential aspects of privacy, should be considered simultaneously. Moreover, the service also should provide practical and fine-grained encrypted data sharing such that a data owner is allowed to share a ciphertext of data among others under some specified conditions. This paper, for the first time, proposes a privacy-preserving ciphertext multi-sharing mechanism to achieve the above properties. It combines the merits of proxy re-encryption with anonymous technique in which a ciphertext can be securely and conditionally shared multiple times without leaking both the knowledge of underlying message and the identity information of ciphertext senders/recipients. Furthermore, this paper shows that the new primitive is secure against chosen-ciphertext attacks in the standard model.

Y. Kawai, ‘‘Outsourcing the re-encryption key generation: Flexible ciphertext-policy attribute-based proxy re-encryption,’’ in Proc. Int. Conf. Inf. Secur. Pract. Exper. (ISPEC), Beijing, China, 2015, pp. 301–315.

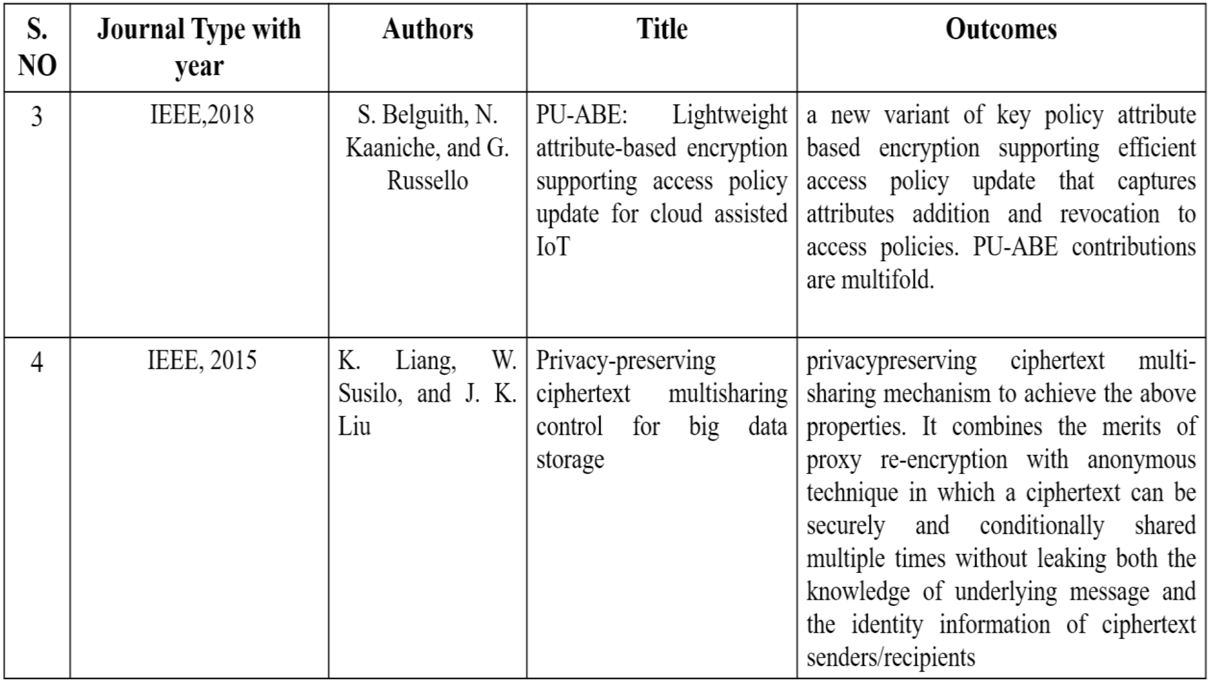
With high flexibility and accessibility of data outsourcing environment such as cloud computing environment, several healthcare providers implement electronic personal health records (PHRs) to enable individual patients to manage their own health data in such resilient and scalable environment. However, PHRs contain highly sensitive information of which the security and privacy issues are the critical concern. Besides, PHRs owners should be capable to flexibly and securely define their own access policy for their outsourced data. In addition to the basic authentication feature, existing commercial cloud platforms usually provide symmetric or public key encryption as an optional feature to support data confidentiality for their tenants. However, such traditional encryption schemes are not suitable for data outsourcing environment because of high key management overhead of symmetric encryption and high maintenance cost for handling multiple copies of ciphertext for public key encryption solution. In this paper, we design and develop a secure and fine-grained access control scheme with lightweight access policy update for outsourced PHRs. Our proposed scheme is based on the ciphertext policy attribute-based encryption (CP-ABE) and proxy re-encryption (PRE). In addition, we introduce a policy versioning technique to support the full traceability of policy changes. Finally, we conducted the performance evaluation to demonstrate the efficiency of the proposed scheme.L.

Touati and Y. Challal, ‘‘Instantaneous proxy-based key update for CPABE,’’ in Proc. IEEE 41st Conf. Local Comput. Netw. (LCN), Dubai, United Arab Emirates, Nov. 2016, pp. 591–594. [12] K. Yang, X. Jia, K. Ren, R. Xie, and L. Huang, ‘‘Enabling efficient access control with dynamic policy updating for big data in the cloud,’’ in Proc. IEEE Conf. Comput. Commun. (INFOCOM), Apr. 2014, pp. 2013–2021.

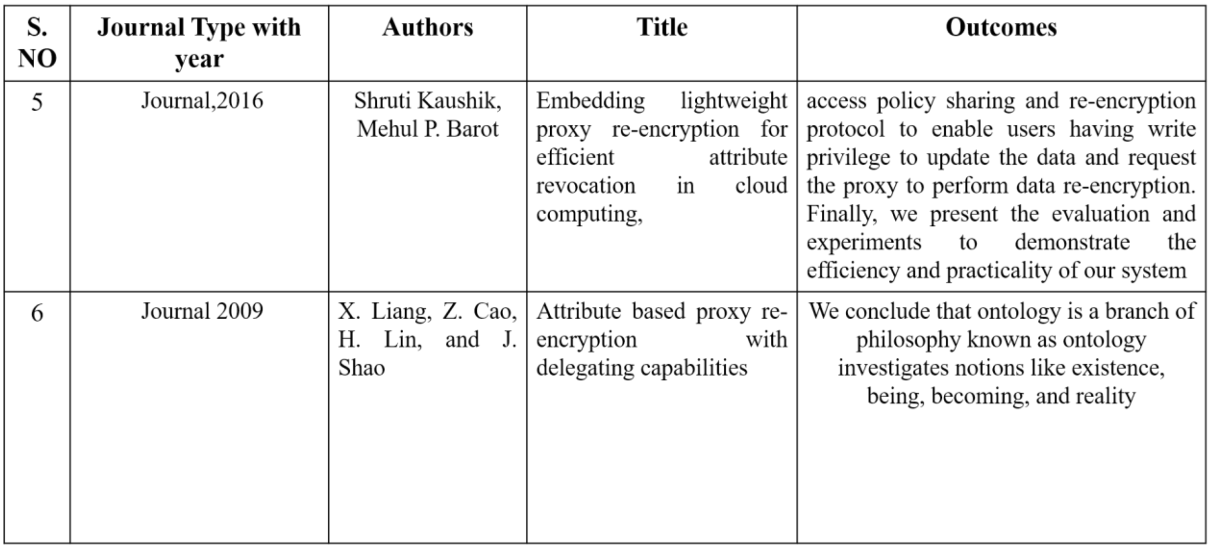
Attribute Based Encryption (ABE) scheme has been proposed to implement cryptographic fine grained access control to shared information. It allows to share information of type one-to-many users, without considering the number of users and their identities. However, original ABE systems suffer from the non-efficiency of their attribute revocation mechanisms. Based on Ciphertext-Policy ABE (CP-ABE) scheme, we propose an efficient proxy-based immediate private key update which does require neither re-encrypting ciphertexts, nor affect other users' secret keys. The semi-trusted proxy assists nodes during the decryption process without having ability to decrypt users' data. Finally, we analyze the security of our scheme and demonstrate that the proposed solution outperforms existing ones in terms of generated overheard.



S. NO	Journal Type with year	Authors	Title	Outcomes
1	Journal, 2015	A. Sahai and B. Waters	Fuzzy identity-based encryption	Our constructions can be viewed as an Identity-Based Encryption of a message under several attributes that compose a (fuzzy) identity. Our IBE schemes are both error-tolerant and secure against collusion attacks.
2	IEEE,2007	J. Bethencourt, A. Sahai, and B. Waters	Cipher text-policy attribute-based encryption	system for realizing complex access control on encrypted data that we call Cipher text-Policy Attribute-Based Encryption. By using our techniques encrypted data can be kept confidential even if the storage server is untrusted; moreover.



S. NO	Journal Type with year	Authors	Title	Outcomes
3	IEEE,2018	S. Belguith, N. Kaaniche, and G. Russello	PU-ABE: Lightweight attribute-based encryption supporting access policy update for cloud assisted IoT	a new variant of key policy attribute based encryption supporting efficient access policy update that captures attributes addition and revocation to access policies. PU-ABE contributions are multifold.
4	IEEE, 2015	K. Liang, W. Susilo, and J. K. Liu	Privacy-preserving ciphertext multisharing control for big data storage	privacypreserving ciphertext multi-sharing mechanism to achieve the above properties. It combines the merits of proxy re-encryption with anonymous technique in which a ciphertext can be securely and conditionally shared multiple times without leaking both the knowledge of underlying message and the identity information of ciphertext senders/recipients



S. NO	Journal Type with year	Authors	Title	Outcomes
5	Journal,2016	Shruti Kaushik, Mehul P. Barot	Embedding lightweight proxy re-encryption for efficient attribute revocation in cloud computing,	access policy sharing and re-encryption protocol to enable users having write privilege to update the data and request the proxy to perform data re-encryption. Finally, we present the evaluation and experiments to demonstrate the efficiency and practicality of our system
6	Journal 2009	X. Liang, Z. Cao, H. Lin, and J. Shao	Attribute based proxy re-encryption with delegating capabilities	We conclude that ontology is a branch of philosophy known as ontology investigates notions like existence, being, becoming, and reality

CHAPTER 3

3.0 EXISTING METHODS AND DRAWBACKS

Attribute-Based Encryption (ABE):

- **Description:** ABE is a cryptographic approach that allows data owners to define access policies based on attributes. This can include patient attributes, such as age or medical condition.

- **Advantages:** ABE provides fine-grained access control, allowing for flexible and dynamic policy updates without revealing the underlying data.

- **Challenges:** Computational overhead and key management complexity could be concerns, but lightweight variants of ABE aim to address these challenges.

Proxy Re-Encryption (PRE):

- **Description:** PRE allows a proxy entity to transform ciphertext encrypted under one key into ciphertext encrypted under another key, without accessing the plaintext. This could be employed to update access policies.

- **Advantages:** Enables policy updates without requiring the involvement of the data owner, providing a flexible and efficient approach.

- **Challenges:** Key management, computational overhead, and ensuring secure proxy operations are considerations.

Differential Privacy Techniques:

- **Description:** Differential privacy aims to provide a mathematical framework for quantifying the privacy guarantees in statistical databases. It can be applied to ensure privacy during policy updates

- **Advantages:** Enhances privacy by adding noise to the query results, making it difficult to determine the contribution of any specific record.

Challenges: Balancing privacy and utility, and potential impacts on data accuracy.

Secure Multi-Party Computation (SMPC):

1. **Description:** SMPC allows multiple parties to jointly compute a function over their inputs while keeping those inputs private. It can be used for collaborative policy updates.

2. **Advantages:** Enables computation on encrypted data without revealing the data to any single party.

3. **Challenges:** Communication overhead and ensuring the security of the computation in a distributed environment.

Role-Based Access Control (RBAC) with Encryption:

1. **Description:** RBAC is a well-established access control model. When combined with encryption, it allows for the enforcement of policies based on roles and attributes.

2. **Advantages:** Simplicity of RBAC combined with the security of encryption for sensitive data.

3. **Challenges:** Ensuring efficient policy updates and maintaining access control lists.

CHAPTER 4

4.0 PROPOSED METHOD

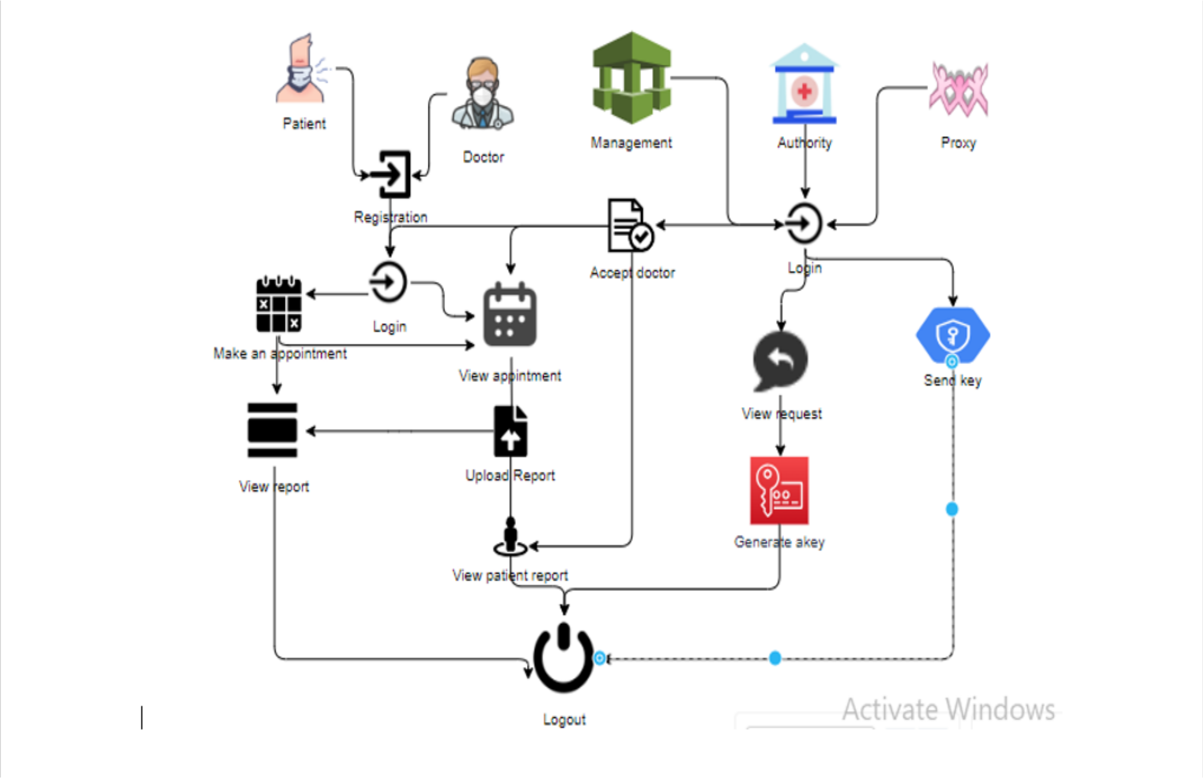
- Our proposed scheme is based on the cipher text policy attribute-based encryption (CP-ABE) and proxy re-encryption (PRE).

- In addition, we introduce a policy versioning technique to support the full traceability of policy changes.

- Finally, we conducted the performance evaluation to demonstrate the efficiency of the proposed scheme

CHAPTER 5

5.0 ARCHITECTURAL DIAGRAM



CHAPTER 6

6.0 PYTHON MODULES

6.0.1 PySerial: This library provides a cross-platform serial communication library for Python. It is used to communicate with sensors and other hardware devices that provide data for golf ball tracking.

-PySerial's features include:

Serial Port Management: PySerial allows for opening, configuring, and closing serial ports, enabling communication with various hardware devices.

Data Transmission and Reception: PySerial facilitates sending and receiving data over serial ports, allowing for the exchange of information between the golf ball tracking system and connected devices.

Error Handling: PySerial provides error handling mechanisms to detect and deal with communication errors, ensuring the reliability and robustness of data transfer.

6.0.2. PyQt: This library provides a cross-platform GUI framework for Python. It is used to develop a graphical user interface for the golf ball tracking system, allowing users to view sensor data and interact with the application without relying on image processing.

-PyQt's features include:

GUI Design and Layout: PyQt offers various widgets and layout management tools for creating user-friendly and visually appealing interfaces.

Data Visualization: PyQt supports data visualization through widgets like charts, graphs, and gauges, enabling users to view sensor data in a meaningful way.

User Interaction Handling: PyQt provides mechanisms for handling user interactions, such as button clicks, keyboard input, and menu selections, allowing users to control the application and interact with the tracking data.

6.0.3. Pandas: This library provides data analysis and manipulation tools for Python. It is used to organize, clean, and analyse sensor data collected for golf ball tracking.

- Pandas' features include:

Data Structures: pandas offer data structures like Data Frames and Series for efficient storage and manipulation of sensor data.

Data Cleaning: pandas provide tools for cleaning and pre-processing sensor data, such as handling missing values, detecting outliers, and correcting data inconsistencies.

Data Analysis: pandas support statistical analysis, data filtering, and aggregation tasks, allowing for extracting meaningful insights from sensor data related to golf ball tracking.

6.0.4. Stats models: This library provides tools for statistical modelling and econometrics in Python. It can be used to develop statistical models for predicting golf ball trajectory and analysing sensor data patterns.

Stats models' features include:

Statistical Models: stats models offer a variety of statistical models, such as linear regression, time series analysis, and generalized linear models, which can be applied to golf ball tracking data.

Model Estimation and Evaluation: stats models provide functions for estimating model parameters, evaluating model performance, and performing hypothesis tests, allowing for rigorous statistical analysis of golf ball tracking data.

Statistical Inference: stats models support statistical inference techniques, such as confidence intervals and p-values, enabling the interpretation of statistical results and drawing conclusions about golf ball tracking behaviour.

6.0.5. Filterpy: This library provides efficient filtering algorithms for Python. It is used to smooth and filter sensor data to remove noise and improve the accuracy of golf ball tracking.

-filterpy's features include:

Kalman Filtering: filterpy offers implementations of the Kalman filter, a powerful algorithm for state estimation that can effectively filter sensor data and predict golf ball trajectory.

Particle Filtering: filterpy provides particle filter algorithms, which are well-suited for tracking objects in dynamic environments like golf ball tracking.

Smoothing Algorithms: filterpy offers various smoothing algorithms, such as moving average filters and exponential smoothing, which can be used to smooth out sensor data and reduce noise. These Python modules can be effectively combined to develop a robust golf ball tracking system without relying on image processing. PySerial enables communication with sensors, PyQt provides a user-friendly interface, pandas facilitate data analysis, stats modelssupports statistical modelling, and filterpy allows for data filtering and smoothing.

CHAPTER 7

7.0. HARDWARE AND SOFTWARE COMPONENTS

SOFTWARE REQUIREMENS

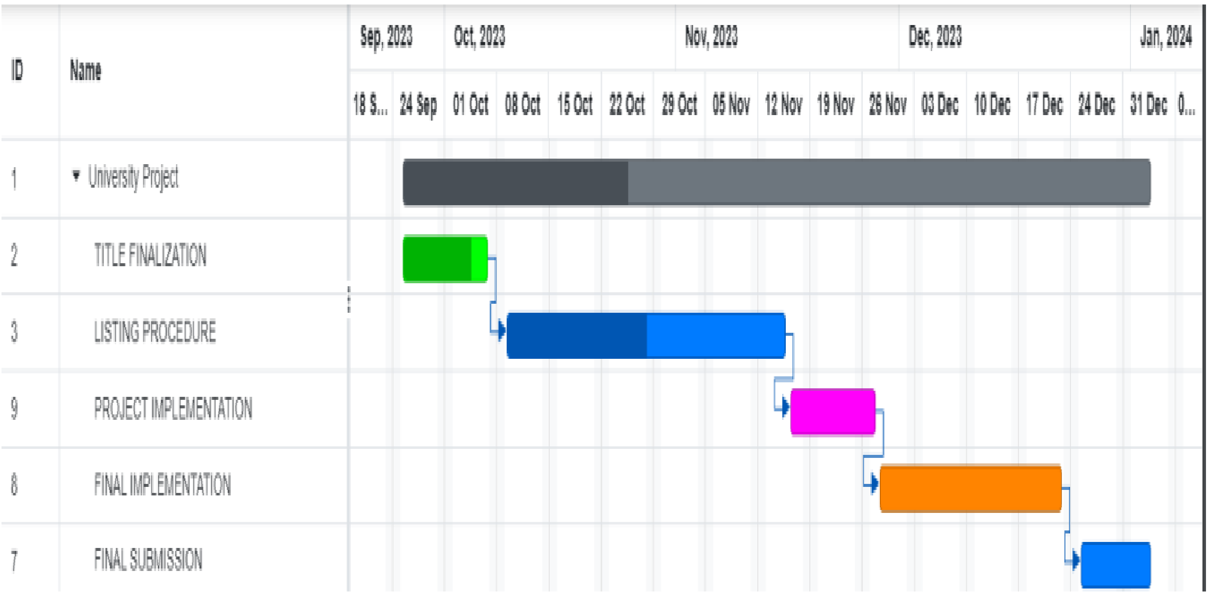
- Operating System : Windows 7/8/10
- Server side Script : HTML, CSS, Bootstrap & JS
- Programming Language : Python
- Libraries : Flask, Pandas, Mysql.connector , Os , Smtplib, Numpy
- IDE/Workbench : PyCharm
- Server side Script :Python 3.6
- Framework :Flask

HARDWARE REQUIREMENTS

- Processor - I3/Intel Processor
- RAM - 8GB (min)
- Hard Disk - 128 GB
- Key Board - Standard Windows Keyboard
- Mouse - Two or Three Button Mouse
- Monitor - Any

CHAPTER 8

8.0 TIME LINE BY GANTT CHART



ID	Name
1	▾ University Project
2	TITLE FINALIZATION
3	LISTING PROCEDURE
9	PROJECT IMPLEMENTATION
8	FINAL IMPLEMENTATION
7	FINAL SUBMISSION

CHAPTER 9

9.0 REFERENCES

- [1] A. Sahai and B. Waters, “Fuzzy identity-based encryption,” in Proc. 24th Annu. Int. Conf. Appl. Cryptograph. Technique (EUROCRYPT) (Lecture Notes in Computer Science). Berlin, Germany: Springer, May 2015, pp. 457– 473.

- [2] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-policy attribute-based encryption,” in Proc. IEEE Symp. Secur. Privacy, Oakland, CA, USA, May 2007, pp. 321–334.

- [3] S. Belguith, N. Kaaniche, and G. Russello, “PU-ABE: Lightweight attribute-based encryption supporting access policy update for cloud assisted IoT,” in Proc. IEEE 11th Int. Conf. Cloud Comput. (CLOUD), Jul. 2018, pp. 924–927.

- [4] J. Li, S. Wang, Y. Li, H. Wang, H. Wang, H. Wang, J. Chen, and Z. You, “An efficient attribute-based encryption scheme with policy update and file update in cloud computing,” IEEE Trans. Ind. Informat., vol. 15, no. 12, pp. 6500– 6509, Dec. 2019.

- [5] M. Mambo and E. Okamoto, “Proxy cryptosystems: Delegation of the power to decrypt cipher texts,” IEICE Trans., vol. E80-A, no. 1, pp. 54–63, 1997.

- [6] K. Liang, W. Susilo, and J. K. Liu, “Privacy-preserving cipher text multisharing control for big data storage,” IEEE Trans. Inf. Forensics Security, vol. 10, no. 8, pp. 1578–1589, Aug. 2015.

- [7] S. Fugkeaw and H. Sato, ‘‘Embedding lightweight proxy re- encryption for efficient attribute revocation in cloud computing,’’ J. High Perform. Comput. Netw., vol. 9, no. 4, pp. 299–309, 2016.

- [8] Y. Kawai, ‘‘Outsourcing the re-encryption key generation: Flexible ciphertext- policy attribute-based proxy re-encryption,’’ in Proc. Int. Conf. Inf. Secur. Pract. Exper. (ISPEC), Beijing, China, 2015, pp. 301–315.

- [9] L. Touati and Y. Challal, ‘‘Instantaneous proxy-based key update for CPABE,’’ in Proc. IEEE 41st Conf. Local Comput. Netw. (LCN), Dubai, United Arab Emirates, Nov. 2016, pp. 591–594.

- [10] K. Yang, X. Jia, K. Ren, R. Xie, and L. Huang, ‘‘Enabling efficient access control with dynamic policy updating for big data in the cloud,’’ in Proc. IEEE Conf. Comput. Commun. (INFOCOM), Apr. 2014, pp. 2013–2021.

- [11] K. Yang, X. Jia, and K. Ren, ‘‘Secure and verifiable policy update outsourcing for big data access control in the cloud,’’ IEEE Trans. Parallel Distrib. Syst., vol. 26, no. 12, pp. 3461–3470, Dec. 2015.

- [12] S. Fugkeaw and H. Sato, ‘‘Scalable and secure access control policy update for outsourced big data,’’ Future Gener. Comput. Syst., vol. 79, pp. 364–373, Feb. 2018.