IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 12, Special Issue 2, April 2023

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | SJIF: 8.423|| Volume 12, Special Issue 2, April 2023 ||

8th National Conference on Advanced Computing Technologies (NCACT'23)

Organized by

Department of CSE, Velammal Engineering College, Chennnai, India

A Lightweight Policy Update Scheme For Outsourced Personal Health Records Sharing

Charan Sai [1], Sai Sasi Vamsi [2], Amandeep Singh [3]

U.G. Student, Department of Computer Engineering, Sathyabama University, Chennai, Tamil Nadu, India[1]

U.G. Student, Department of Computer Engineering, Sathyabama University, Chennai, Tamil Nadu, India[2]

Associate Professor, Department of Computer Engineering, Sathyabama University, Chennai, Tamil Nadu, India[2]

ABSTRACT: Due to the extreme flexibility and availability of facts environments including cloud computing, many fitness vendors are enforcing electronic non-public fitness records (PHR) to allow person sufferers to manipulate their clinical information in a flexible and scalable surrounding. However, PHRs contain touchy information wherein security and privacy troubles are vital. In addition, PHR holders can extra easily and securely outline their get entry to coverage to their outside statistics. In addition to primary authentication features, existing cloud companies typically provide symmetric or public key encryption to similarly make sure statistics privacy for his or her tenants. However, such traditional encryption technology is not suitable for records outsourcing environments due to the large overhead of wearing symmetric encryption keys and the excessive renovation costs of processing more than one copies of ciphertexts for the solution of public key encryption. In this article, we design and develop a comfy and granular manipulate approach with lightweight get admission to policy updates for outsourced PHRs. The proposed scheme is primarily based on the rules of Ciphertext Encryption (CP-ABE) and Proxy Re-Encryption (PRE). In addition, we introduce a technical trade approach for a complete alternate strategy. Finally, we perform an implementation evaluation to illustrate the effectiveness of the proposed scheme.

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

Objective: The motive of this plan is to keep touchy affected person information within the cloud using an encryption approach. This securely transfers facts from affected person to affected person. Patient minute facts using the important thing.

I. INTRODUCTION

In excellent statistics-sharing surroundings which include cloud storage, the server should be without problems available at all times to provide unfastened access to shared records and offerings. Today, many corporations and individuals pick to keep their precious information on third-party servers which includes cloud garage due to the price savings and efficient useful resource control that cloud provider companies provide. As far as privateness and protection are concerned, records proprietors generally encrypt their records earlier than moving it to a cloud server. Data encryption is the maximum appropriate manner to shield sensitive facts from unauthorized access. However, encryption by myself is adequately robust to make certain security. Access manipulate mechanism is any other area of acting protection. To remedy this hassle, many works broadly attribute encryption (ABE). ABE presents a one-to-many encryption scheme with high-quality-grained get admission to manage. In addition, it has encryption and gets admission to manipulate features. There are forms of ABE: Ciphertext Policy Attribute Based Encryption (CP-ABE) and Key Policy Based Encryption (KP-ABE). In CPABE, attributes are used to create a custom decryption key and an get right of entry to policy to encrypt records. For KPABE, the user's key's related to the get admission to policy,

|| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | SJIF: 8.423|| Volume 12, Special Issue 2, April 2023 ||

8th National Conference on Advanced Computing Technologies (NCACT'23)

Organized by

Department of CSE, Velammal Engineering College, Chennnai, India

and encryption is performed through predefined attributes. From the safety factor of view, CP-ABE is most effective due to the fact the information owner can specify his policy for facts encryption. An advantage of the usage of CPABE is the control of organization keys. One is to separate abstract attributes from real keys. This reduces communication overhead and offers great-grained manipulate over get entry to records. In addition, it gives bendy one-to-many encryption rather than one-to-one; it's far seen as a promising device to remedy the problem of dependable granular statistics trade and a decent access manipulate device. However, CP-ABE introduces expensive overheads, consisting of regenerating the key, regenerating the key, and redistributing the key when the gadget is revoked or up to date.

II. LITERATURE SURVEY

Title 1:A. Sahay and B. Waters, "Fuzzy Identification Encryption", in Proc. 24th year International conference Dec. Cryptograph. Art (EUROCRYPT) (Computer Science Lecture Notes). Berlin, Germany: Springer, May 2015, pp.

We introduce a new type of identity-based encryption scheme (IBE), which we call identification-primarily based encryption. In Fuzzy IBE, we remember the identification of descriptive attributes. Any IBE scheme lets in the personal key for identifier ω for use to decrypt statistics with identifier ω zero if and most effective if identifiers ω and ω zero are near each different, as measured by way of the "overlap set". Metric distance. Fuzzy IBE scheme may be used to provide encryption using biometric identifying inputs; the error-tolerance of factors although the IBE scheme is exactly what permits the use of biometric identification, which by way of its nature always takes some noise. In addition, we show that Fuzzy-IBE may be used for an application that we call "attributed encryption". This article suggests two plans for a smoky MBP circle. Our production may be notion of as a message-based identification encryption with multiple identity ingredients (although). Our IBE devices are fault tolerant and immune to tampering attacks. Also, our employer no longer uses random oracles. We take a look at the safety of our technology and the usage of the Selective-ID security version.

Summary: Amit Sahay and the Brent Water crew in this text describe IBE schemes which might be fault tolerant and resistant to breaching assaults.

Title 2: J. Betancourt, A. Sahay, and B. Waters, "Ciphertext Policy Attribute-Based Encryption," in Proc. IEEE Symp. Secret Security, Oakland, CA, USA, May 2007, pp. 321–334.

In some disbursed structures, a consumer will only be able to get entry to information if they have a sure set of credentials or attributes. Currently, the best manner to put in force such policies is to use a relied-on server for information storage and get right of entry to manipulate. However, if a person compromises the server wherein the records are saved, the confidentiality of the data can be compromised. In this newsletter, we present a gadget for quit-to-give up access to govern encrypted statistics, which we name encryption based on cryptographic attributes. Using our techniques, encrypted facts can continue to be nonpublic even if the server isn't relied on; furthermore, our methods are covered in opposition to collusive assaults. Earlier characteristic-based totally encryption structures used attributes to explain encrypted facts and built into person-keyed money owed; even as in our gadget, they usually describe the attributes of the person's credentials, and the side that encrypts the information defines the coverage of folks that can be compromised. Thus, our method is towards the conventional method to get right of entry to manage based on proximity as position-based totally access manipulate (RBAC). In addition, we provide the implementation of our machine and give overall performance measurements.

Summary: John Betancourt, Amit Sahai, Brent Water based totally on confidential records this is transmitted and stored on the Internet by means of third parties.

Title 3:S. Belguit, N. Kaaniche, and G. Russell, "PUABE: Lightweight Attribute-Substructing Encryption Supporting Access Policy Update for Cloud IoT," in Proc. IEEE eleventh International Conf. Cloud computing (CLOUD), July 2018, pp. 924–927.

Cloud-based IoT packages are growing as IoT gadgets dispensed in various environments are deployed to gather and transmit the obtained records to faraway servers for similarly processing and alternate between customers. On the alternative hand, in some applications, the records gathered are extraordinarily touchy and need to be protected earlier

|| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | SJIF: 8.423|| Volume 12, Special Issue 2, April 2023 ||

8th National Conference on Advanced Computing Technologies (NCACT'23)

Organized by

Department of CSE, Velammal Engineering College, Chennnai, India

than it's miles transferred. As a rule, encryption strategies are applied at a part of the statistics operator to shield the information from intruders, as well as a few curious clouds. On the other hand, the change of facts among customers calls for state-of-the-art get entry to control mechanisms. With both requirements as legitimate, attribute encryption (ABE) is extensively used to offer get right of entry to encrypted outside energy. While ABE presents unambiguous access control and privacy of facts, the authentication of get right of entry to to the structures used after data encryption and go out remains open. In this paper, we expand PU-ABE, a brandnew encryption alternative based on key attributes that helps an efficient approach to policy updating that captures the addition and elimination of attributes inside the get admission to method. The contribution of PUABE is improved. First, the techniques used for encryption can be updated without the want to percentage the secret keys between the cloud server and the information proprietors and reencrypt the statistics. Second, PUABE gives nonpublic get admission to and thin manage to outside records. Third, the traits obtained with the aid of the give up consumer are of steady length and do no longer rely on the quantity of attributes used in the layout approach, which enables low transmission and garage prices.
Summary*:* Sana Belguit, NesrinKaaniche and IohannesRussello worked on information security.

Title 4: K. Liang, V. Susilo, and J. K. Liu,
"Confidentiality, Privacy Preservation, and Multiple Ciphertext Exchange Management for Big Data Storage," IEEE Trans. Inf. Forensic Security Vol. 10, no. 8, pp
The want for dependable excessive-value information garage is needed nowadays extra than ever. The most important requirement of the workplace is to guarantee the confidentiality of statistics. However, the account have to be saved nameless by means of customer service, one of the most crucial aspects of privacy. In addition, the service must also provide a realistic and granular change of encrypted records in order that the owner of the statistics can share textual content facts with others beneath positive situations. This paper first proposes a privacykeeping ciphertext sharing mechanism to reap the above residences. It combines the powers of proxy re-encryption with an nameless technique wherein ciphertext can be transmitted securely and beneath the circumstance that each the message transport statistics and the identity of senders/receivers are broadcast. In addition, the paper suggests that the new primitive is cozy in opposition to selected ciphertext attacks on the same old model.
Summary: This article discusses the improvement of structures that can save large data and massive volumes of user get right of entry to requests. Attribute-primarily based encryption (ABE) is a technique of promoting give upto-stop safety of large records inside the cloud.

Title 5 :S. Fugkeo and H. Sato, "Implementation of Lightweight Proxy Re-Encryption for Efficient Attribute Revocation in Cloud Computing," J. High Perform. Account Network, vol. Nine, no. 2016. V. 4. S. 299-309.

With the velocity of cloud computing and the improvement of modern cellular computing, it is vital to apply cell gadgets to get hold of and send information through the cell cloud platform. This increases the benefit and versatility of facts access through cloud computing, as facts customers can get right of entry to shared statistics anytime, everywhere using cellular gadgets. However, the use of cell devices to get right of entry to public statistics inside the cloud where touchy facts is encrypted isn't always practical, due to the fact mobile gadgets have constrained computing skills to perform heavy cryptographic operations. In this article, we recommend a simplified thing-primarily based cryptographic layout attribute totally based encryption scheme (LW-C-CP-ARBE) to guide thin and lightweight access manipulate for cellular cloud. We adopt the CP-ABE method as the primary cryptographic access manager and a new proxy re-encryption (PRE) protocol to reduce the reencryption and decryption fees of cell users. To this cease, the overhead of appearing a cryptographic operation at the give up of the consumer's system is low. In addition, we develop a protocol for sharing a secure get admission to coverage and reencryption so that users can write through get admission to replace the statistics and request the manager to reencrypt the records. Finally, we present assessments and experiments to demonstrate the effectiveness and practicality of our machine.
Summary: This article discusses the development of structures wherein the encryption device is computed with attribute-primarily based seek and don't forget.

Title 6: X. Liang, Z. Cao, H. Lin, and J. Shao, "A reencryption proxy with attribute delegation capability," in Proc. 4th International Symp. With inf., comp., general. Security (ASIACCS), 2009, pp. 276-286.

Attribute-Based Proxy Re-encryption (ABPRE) permits a semi-trusted proxy server to convert and get entry to encryption coverage to a new access encryption coverage without revealing any facts about the message service. Such primitives facilitate small scale at ease alternate of encrypted information inside the cloud. In its primary layout, the re-encryption secret is associated with an access structure that specifies which kinds of information may be reencrypted.

|| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | SJIF: 8.423|| Volume 12, Special Issue 2, April 2023 ||

8th National Conference on Advanced Computing Technologies (NCACT'23)

Organized by

Department of CSE, Velammal Engineering College, Chennnai, India

Only two tries have been made to put into effect the key-scheme ABPRE (KP-ABPRE), one of which calls for the security of a reproducible selected ciphertext (RCCA security) and the opposite requires the safety of a delegated ciphertext (CCA security). We have proven that each RCCA and CCA systems are incredibly liable to attack. Furthermore, in these paintings we advise a selective CCA-secure KPABPRE scheme. Since we demonstrate the assaults of only two protection schemes within the literature, RCCA and CCA, our idea becomes the first KPABPRE thought that satisfies the selective safety of CCA. In addition, our layout processes an appealing property, specifically resistance to tampering. A supervisor re-encryption scheme usually consists of three elements: a delegate who delegates decryption rights, a manager who plays re-encryption, and a delegate who's delegated decryption. When a delegate wants to share his facts with a delegate that satisfies the admission to policy, the agent can collude with the malicious delegate to try and reap the delegate's non-public keys throughout the delegation period. If the non-public keys are exposed, the safety of the delegated facts is completely compromised. The delegate or delegate can attain all exclusive facts of the delegate at any time, even after the cease of the delegation length. Therefore, breakdown resistance is crucial for actual-international packages. In this text we display that our production is inconsistent with transgression. Our design proved its breach resistance and selective protection of CCA primarily based on a random oracle version, assuming a bilinear Diffie Hellman exponent.

Summary: In idea, the scheme can convey an arbitrary wide variety of corrupt government.

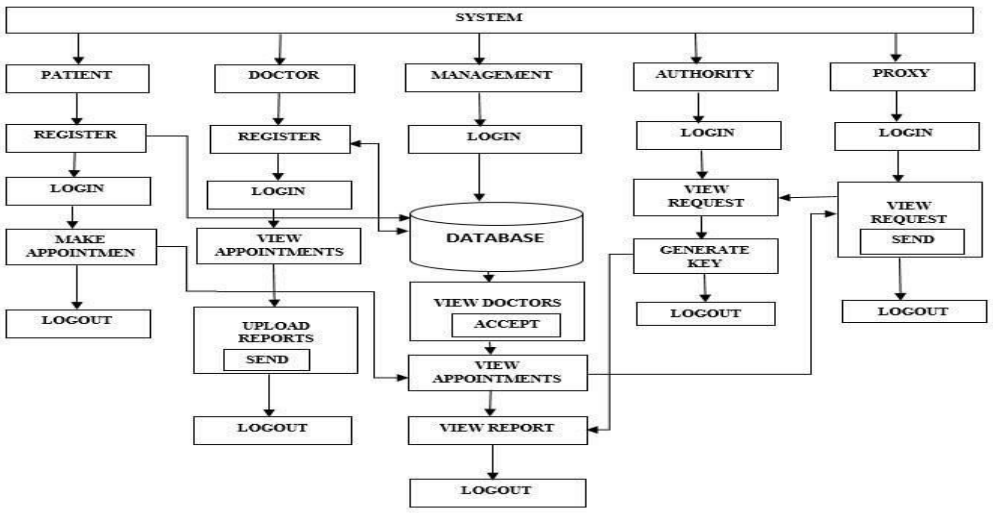
II. SYSTEM ANALYSIS & FEASIBILITY STUDY Existing

Method:

Existing commercial databases commonly offer symmetric or public key encryption as an brought feature to ensure data privacy for their holders. However, such conventional encryption schemes are not suitable for the records outsourcing environment due to the massive overhead of managing symmetric encryption keys and the excessive upkeep expenses of processing a couple of ciphertext copies for the answer of public key encryption.

Disadvantages:

- High complexity.
- Low Computation.
- Requires skilled persons.



2 (a)

|| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | SJIF: 8.423|| Volume 12, Special Issue 2, April 2023 ||

8th National Conference on Advanced Computing Technologies (NCACT'23)

Organized by

Department of CSE, Velammal Engineering College, Chennnai, India

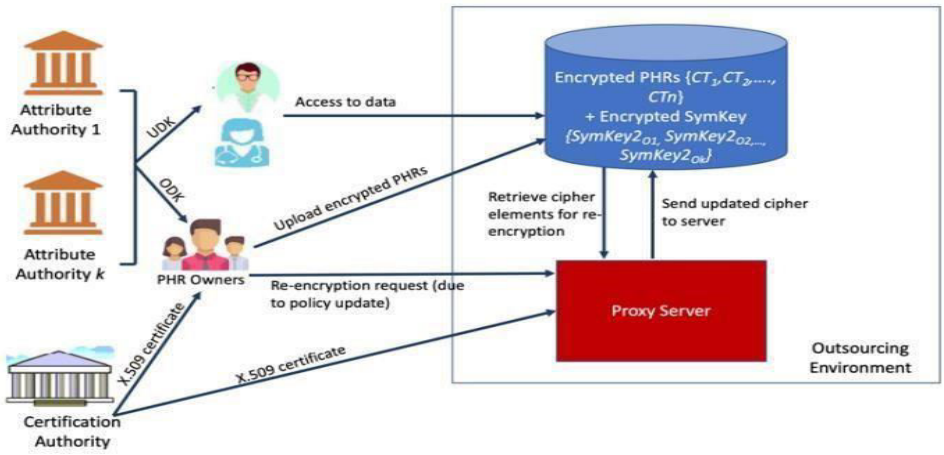
2.2 Proposed System:

The proposed scheme is based totally on the guidelines of Ciphertext Encryption (CP-ABE) and Proxy ReEncryption (PRE). In addition, we introduce a technical model plan to achieve full task changeability. Finally, we carried out an implementation evaluation to illustrate the effectiveness of the proposed scheme.

Advantages:

- Accuracy is good.
- Low complexity.
- High Computation.
- No need of skilled persons

2.3 ARCHITECTURE



2 (b)

III.METHODOLOGY AND ALGORITHMS

CLOUD:

The cloud includes three main offerings:

- Infrastructure as a Service (IaaS); • Platform as a Service (PaaS) and • Software as a Service (SaaS).

Software as a Service (SaaS) includes licensing utility software to clients. Licenses are typically supplied underneath a pay-as-you-move or on-call model. This form of gadget can be observed in Microsoft Office 365.

Infrastructure as a Service (IaaS) consists of the method of turning in everything from running systems to servers and garage over an IP-based connection as part of an on-call for carrier. Customers can keep away from having to buy software programs or servers and alternatively can buy those assets from the workplace's outstanding studies tool. Examples of popular IaaS structures consist of IBM Cloud and Microsoft Azure.

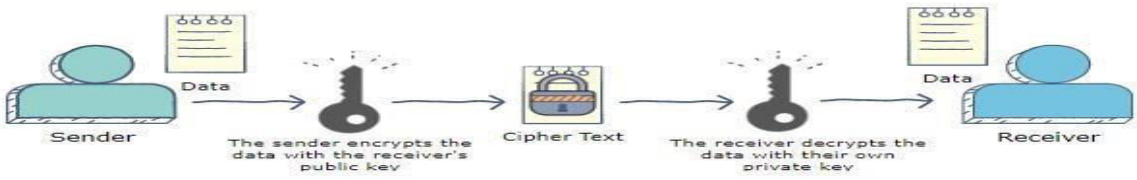
|| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | SJIF: 8.423|| Volume 12, Special Issue 2, April 2023 ||

8th National Conference on Advanced Computing Technologies (NCACT'23)

Organized by

Department of CSE, Velammal Engineering College, Chennnai, India

Platform as a Service (PaaS) is considered the most complicated of the three ranges of cloud computing. PaaS has some similarities with SaaS, the main distinction being that rather than turning in software program over the Internet, it's miles really a platform for constructing software program delivered over the Internet. This model consists of platforms including Salesforce.Com and Heroku.



3

(a)

3.1DATA ENCRYPTION:

Data encryption converts data into another shape or code so that handiest human beings with access to the secret key (officially known as the decryption key) or password can examine it. Encrypted information is typically known as ciphertext, even as unencrypted records is known as plaintext. Encryption is one of the most popular and effective statistical safety techniques utilized by organizations these days. There are forms of encryption - uneven encryption, called public key encryption, and symmetric encryption.

IV.PURPOSE

The motive of records encryption is to protect the privacy of digital information as it is saved in pc

systems and transmitted over the Internet or other laptop networks. The Data Encryption Standard (DES) has been changed by means of cutting-edge encryption algorithms that play a crucial function in securing IT structures and communications.

4.1 DATA DECRYPTION:

Decryption is the manner of converting records that has been encrypted into its unencrypted form. Through decryption, the device extracts and converts the wrong information into texts and snap shots which can be understandable not best to the reader however additionally to the machine.

4.2 Implementation:

PHR owners record files which include treatment records, patient profiles, and so on. In the encrypted form of the cloud server, users inclusive of doctors can access the shared file if they have the potential (for example, the decryption key) that satisfies. Technique the control plan.

4.3 SOFTWARE DEVELOPMENT LIFE CYCLE – SDLC:

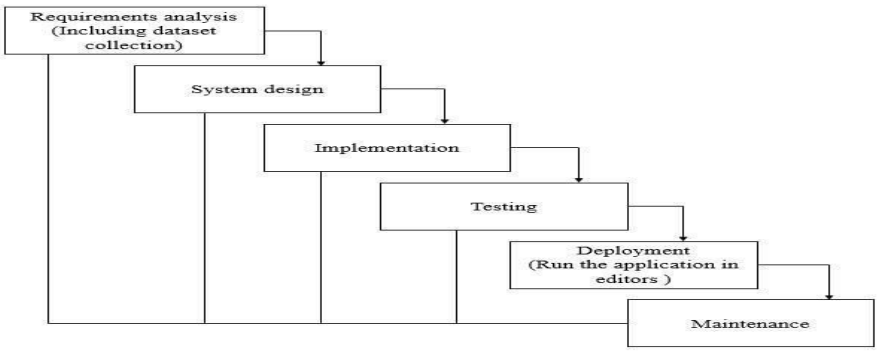
In our assignment, we use the waterfall model as a software program improvement cycle because of the step-by means of-step implementation procedure.

|| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | SJIF: 8.423|| Volume 12, Special Issue 2, April 2023 ||

8th National Conference on Advanced Computing Technologies (NCACT'23)

Organized by

Department of CSE, Velammal Engineering College, Chennnai, India



Waterfall Model 4(a)

4.4 SYSTEM REQUIREMENTS SPECIFICATION

Functional and non-functional requirements:

Requirements analysis is a totally crucial procedure that lets in you to evaluate the achievement of an intermediate machine or application. Requirements are typically divided into two classes: useful and nonuseful necessities.

4.5 Functional necessities: These are the requirements that the end person has for the principle features that the machine has to offer. All those capabilities should be protected inside the device inside the scope of the contract. They are supplied or fashioned in the form of input to the device, the operation to be completed, and the anticipated output. Generally, those are person-defined requirements that can be without delay contemplated within the final product, as opposed to non-practical requirements.

4.6 Non-useful necessities: These are essentially high quality constraints that want to be met in step with the task agreement. The precedence or degree of implementation of those factors varies from one challenge to every other. They are also referred to as non-motion necessities.

They mainly challenge troubles inclusive of:

- Portability
- Security
- Maintainability
- Reliability
- Scalability
- Show
- Reuse
- Flexibility

4.7 SYSTEM SPECIFICATIONS: H/W SPECIFICATIONS:

- Processor - I3/Intel Processor
- RAM - 8GB (min)
- Hard Disk - 128 GB

|| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | SJIF: 8.423|| Volume 12, Special Issue 2, April 2023 ||

8th National Conference on Advanced Computing Technologies (NCACT'23)

Organized by

Department of CSE, Velammal Engineering College, Chennnai, India

- Keyboard - Standard Windows Keyboard
- Mouse - Two or Three Button Mouse
- Monitor - Any

S/W SPECIFICATIONS:

- Operating System : Windows 10
- Server-side Script : Python 3.6
- IDE : PyCharm
- Libraries Used : Pandas, MYSQL
- Framework : Flask.

4.8 SYSTEM DESIGN:

Input Design:

In a statistics system, the inputs are the inputs which might be processed to provide the outputs. When designing enter, builders must consider input devices consisting of PC, MICR, OMR, and so on.

The fine of the gadget's input therefore determines the fine of the device's output. Well-designed enter bureaucracy and monitors have the subsequent homes:

- Must efficiently serve a specific purpose together with storing, recording, and retrieving statistics.
- This guarantees the right finishing touch with accuracy.
- It ought to be simple and clear to be filled.
- Must have user awareness, consistency, and simplicity.
- All those targets are done via know-how the fundamental concepts of design.
- What inputs are required for the system?
- How give up users respond to numerous paperwork and screen elements.

Output Design:

Output design is the most important task of any device. In the output layout, it is required to determine the output ratio of the dye and to not forget the essential output energy and the objectives to file the prototype.

V.MODULES

1. **Unwell:**
   Login: Patient should login with valid information utilized in his/her registration.
   Registration: Each affected person is registered. Appointment: The affected person will make an appointment with the signs and symptoms
   View Report: The affected person will view reports after the medical exam.
   To conclude: About the log forever system.
2. **DOCT:**
   Login: The medical doctor has to login with the valid info used in his/her registration.
   Registration: Each patient must sign up and get hold of an administrative request.
   Visa nomination: all institutions
   Download Report: Download the document. Send report: send file as input
   To finish: About the log forever gadget.
3. **HEALTH MANAGEMENT:**
   Login: Open Management with default credentials. Purpose: All appointment requests from patients.
   View Doctor Request: View all registered medical doctor requests.
   Submit Information: The affected person's request is forwarded to the physician Close:
   The final go out of the machine.

|| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | SJIF: 8.423|| Volume 12, Special Issue 2, April 2023 ||

8th National Conference on Advanced Computing Technologies (NCACT'23)

Organized by

Department of CSE, Velammal Engineering College, Chennnai, India

***4.* Powers:**

Login: administration may be opened with a loss of credentials.
View Request: View all requests from the agent. Generate Key: General key to authorize sufferers.
Close: The final exit of the device.

***5.* SERVANT DEPUTY:**

Login: management may be opened with a loss of credentials.
Request View: View all requests for teachers. Submit a request: Submit requests to the authority Close:
The final exit of the device.

Test cases Model building:

S.NO	Test cases	I/O	Expected O/T	Actual O/T	P/F
1	Read data	File data.	Data read successfully	Data read success.	P
2	Performing Encryption on file data	Encryption has to perform on file data	Encryption should be performed on file data	Encryption successfully completed.	P
3	Generating Key pair	Key has to generate	Key will generate	Key Generated successfully.	P
4	Cipher text	File data Encrypted data will Decrypt	Data should be decrypt	Data decrypted successfully	P

4(b)

VI. CONCLUSION

We have proposed and replaced plan based on the coverage and the agent's encryption technique. Our layout completely gets rid of the value of political updating, which needs to be finished on a third- birthday party server. In addition, the re-encryption method encapsulates multiplication for high scalability and higher basic gadget performance. In the test, we advanced a GUI device to put into effect the CP-ABE replace plan. Data proprietors can add encrypted documents and money owed to outside bills via our gadget. Administrators or facts owners do not want to retrieve policies from the local database and interact with an external server for the re-encryption manner. With our net device, plans may be up to date anytime, anywhere. As a end result, it gives transparent management access to device files and management plan updates. In addition, we've proposed a technical model of the task to permit the effective reconstruction of the historical report for accurate listening. Finally, we proven the overall performance of report re-encryption. The consequences display that the re-encryption system performed with multithreading is higher than the method without it.

FUTURE SCOPE

We will provide significant experiments to test the cloud supervisor with a big quantity of records and large-scale get right of entry to gadgets in a actual cloud environment.

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.

|| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | SJIF: 8.423|| Volume 12, Special Issue 2, April 2023 ||

8th National Conference on Advanced Computing Technologies (NCACT'23)

Organized by

Department of CSE, Velammal Engineering College, Chennnai, India

[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] L. Cheung, J. Cooley, R. Khazan, and C. Newport, ''Collusion resistant group key management using attribute-
based encryption,'' Cryptol. ePrint Arch., Tech. Rep. 2007/161. [Online]. Available:https://eprint.iacr.org/2007/161.pdf

[4] 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.

[5] 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.

[6] 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.

[7] 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.

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

[10] X. Liang, Z. Cao, H. Lin, and J. Shao, ''Attribute based proxy re-encryption with delegating capabilities,'' in Proc. 4th Int. Symp. Inf., Comput., Commun. Secur. (ASIACCS), 2009, pp. 276–286.

[11] 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.

[13]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. [14]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.

[15]L. Cheung and C. Newport, ''Provably secure ciphertext policy ABE,'' in Proc. 14th ACM Conf. Comput. Commun. Secur. (CCS), Richmond, VI, USA, Oct. 2007, pp. 456–465.

INNO SPACE
SJIF Scientific Journal Impact Factor

SJIF: 8.423

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INTERNATIONAL CENTRE

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details