Global Journal of Pure and Applied Mathematics.
ISSN 0973-1768 Volume 12, Number 2 (2016), pp. 1491-1500

http://www.ripublication.com

Data Security Based On Big Data Storage

S. Ananthi and Anjali Periwal
Department of Computer Science and Engineering,
Sathyabama University, *Chennai, Tamil Nadu, India.*

Prince Mary. S
Department of Computer Science and Engineering,
Sathyabama University Chennai, Tamil Nadu, India.

Abstract

Security is a prime concern for any service that provides big data storage. The data of an individual should remain confidential and should be accessed only by any authenticated person. One of the aspects of security that is considered prior storing data is the unusual features of the aid consumer. The service that is used for storage must contribute experimental and the supreme-grained converts the allocated file in such a way that only a cipher text of data is shared among others by the data owner under some specified conditions. The required features are obtained by introducing a new technique for providing big data storage i.e. a seclusion-conserving cipher text allocates more than one appliance. In this technique, advantages of proxy re-encryption technique are employed that enables cipher text to be safely and dependently allocated many times and it also ensures that the intelligence of fundamental dispatch and the discerning instructions of cipher text vendor and heir is not leaked. The technique is also vulnerable to the chosen-cipher text attacks.

Keywords: Proxy re-encryption, unusual features, vulnerable, conserving

1. Introduction

Many of us have now switched on to cloud for the storage of data as the processing in the case of clouds is very high. Still, there are people who store their information even on the internet. When compared to the existing system, we can say that big data is more in use these days. The main purpose of data storage is to assure that no information is lost. Previously also there were many techniques which was satisfying these conditions. In the existing system we could see that only the authorized user

could retrieve the correct information, whereas the rest could not. Let us consider that a hospital is storing the medical records of its patients in the cloud. The records are saved in such a way that no one can directly access any information through the cloud. The information gets displayed only to those doctors who are considerable for the patient. With the help of some traditional mechanism, the information is kept secure enough so that no other interrupted user can gain access through it.

In the existing system, it did not guarantee us that only the authorized user could access the information. This is because the data that was stored was made public. So anyone could access the information at anytime. Hence we can say that there no privacy about the patient records. The patient as well may be shifted from one hospital to the other in case the treatment is not done accurately at that particular hospital. So, accordingly, the details of the patient need to be carried out from one place to the other. Even the patient can also send his/her recommendations as to where do they want to be treated. For example, a heart patient can suggest as to which cardiologist, he would want to be treated.

Now the proposed system deals with tackling the above problems. There is a data owner who acts as a patient. All his records are saved in one database together with a key. If the data consumer who is the doctor wants to retrieve the patient information, then he should be able to satisfy some particular conditions. Only after accessing the key, the doctor views the details about the patient. Now, in case the patient does not present, then there is an additional server that stores in the details of the patient. The server acts as a proxy which contains certain sets of questions for the data consumer. If the data consumer is able to respond to those queries, then only can he have access to the key or else he won't be able to get the patient details. The algorithm used for this problem is Simplified Data Encryption Standard (SDES) with the help of a Random Key Generation.

1.1 Anonymous nature

No user knows the information about the encrypted data.

1.2 Updating

When a user receives the encrypted data he can update it several times.

1.3 Sharing

We can share the data only if all the details are correct.

2. Related Work

To maintain anonymity, we are proposing some encryption methods such as anonymous IBE [8]. With the help of these methods we are able to protect the data securely. The updating of the cipher text receiver is hence not supported. Proxy Re-Encryption [5] has been proposed to solve the matter of data sharing. To capture privacy-preserving property and cipher text's recipient update simultaneously, [13] proposed an anonymous IBPRE system, which is CCA security in the Random Oracle Model (ROM). In the context of IBE/ABE, some well-known systems supporting

anonymity that have been proposed, such as [8], [9], [16], and [17]. Leveraging them may partially fulfill our goals. However, we need to focus on the combination of anonymity and ciphertext update properties.

3. Proposed System Architecture

An identity proxy re-encryption scheme with source hiding property, and its application to a mailing-list system. The anonymity service clients, one of the most essential aspects of privacy, should be considered simultaneously. Fine-grained encrypted data owner is allowed to share a cipher text of data among others under some specified conditions. Normal encryption and decryption method used. In existing system the patient any time monitoring the system and not secure. The patient should remember the key. It uses a re-encryption technique to store the data in a secure manner so that no information is lost. It is secure against chosen-cipher text attacks. We use SDES and Random Key Generation method is to be used for encryption, decryption and key generation. More secure compared to existing methods. The proxy Re encryption method used so it is acting as a user. No need to monitor the system and key any time. Design is a multi-step that focuses on data structure software architecture, algorithm, etc. an interface between modules. The design process also translates the requirements into presentation of software that can be accessed for quality before coding begins. Computer software design change continuously as new methods; better analysis and border understanding evolved. The software design is a relatively early stage for revolution. Therefore, a software design methodology lacks the depth, flexibility and quantitative nature for normally associated with more classical engineering disciplines. However techniques for software designs do exist, criteria for design qualities are available and design notation can be applied.

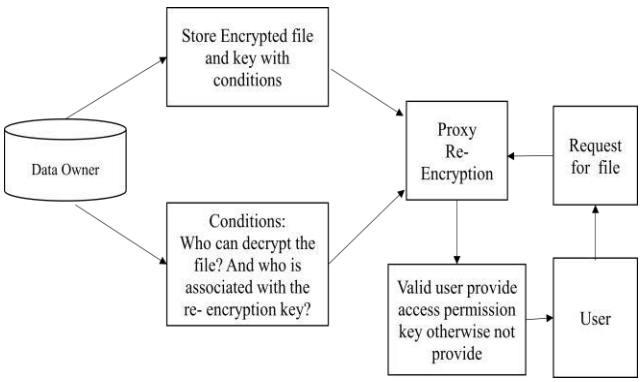

Figure 1: System Architecture

The input design is link between information systems and the user. It comprises the developing specification and procedures for data preparation are necessary to put transaction data into a usable form for processing can be achieved by inspecting

computer to read data from a written or printed document or it can occur by keying the data directly into the system. The design of input focuses on controlling the amount of input required for controlling the errors, avoiding delays, avoiding extra steps and keeping the process simple. The input is designed for security and ease of use with retaining privacy. Input Design considered the following things:

- What data should be given as input?
- How the data should be arranged or coded?
- The operating personnel in providing input.
- Methods for preparing input validations and steps to follow when error occurs.

A quality output is one, which meets the requirements of the end user and presents the information. In any system results processing is communicated to the users and to other system through outputs. In output design the information is to be displaced for immediate need and also the hard copy output. The most important and direct source information to the user. Efficient and intelligent output design improve the system's user decision-making. The output formed in the information system should accomplish one or more of the following objectives.

- Convey information about past activities, current status or future projections.
- Signal important events, opportunities, problems, or warnings.
- Trigger an action.
- Confirm an action.

4. System Implementation

In this paper three modules have been proposed. They are

- Data Outsourcing
- Data Sharing
- Proxy Re-Encryption

4.1 Data Outsourcing

Protect the unusual features for cipher text vendor/heir, provisional details sharing and multiple recipient-updates. The data owner stores the data into the cloud. That the data is either public or private. Data are private means, the data are converted encrypted form using some encryption methods.

4.2 Data Sharing

How to share the data to the specific consumer his project is to a beam, interdisciplinary resolution guidance to set up the assembly, survey, and distributing of unique information analysis in the communal body of knowledge and also in some additional branch stretch contingent on privacy for individual subjects. In particularly to build a disposition for computation, statistics, lawful and stratagem tools that can be incorporated into data repositories to make a privacy-protected data-sharing for lay researchers.

4.3 Proxy Re-Encryption

This module is used to hook the quandary while sharing data. It allows a half believe in affiliation, known as substitute, converts an encrypted text designed for particular user towards an encrypted text concerning an equivalent information is designed for another user without revealing the ability of given decryption key. Its act as a data owner and it is used to check the concern person is valid person or not valid person. If the person is valid means it will provide the access key otherwise not provided.

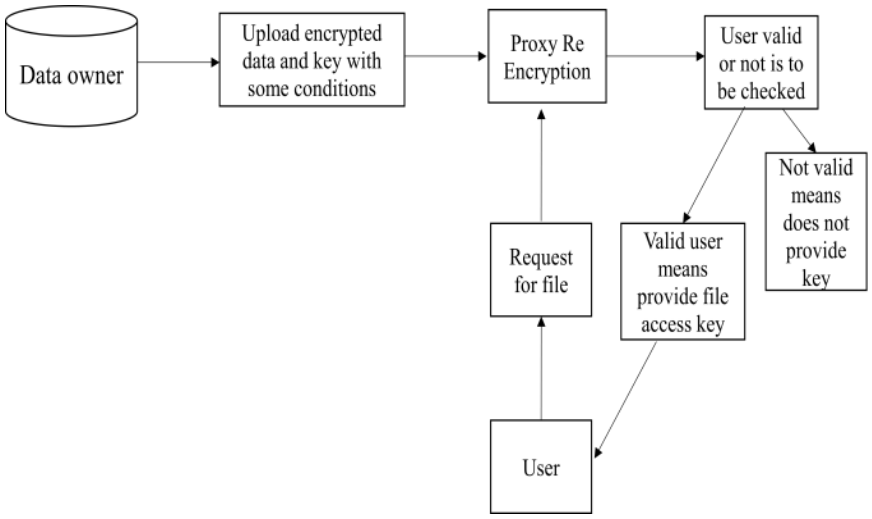

Figure 2: Data flow Diagram

5. Algorithm for S-DES

Step 1: Data owner will give his input file and it is stored in encrypted form.
Step 2: Get the encryption key from the data owner.
Step 3: Encrypt the input file with that key.
Step 4: After encryption, the input file will be stored in a big data.
Step 5: Get the request from the data consumer.
Step 6: Once the request is received from the data consumer then the proxy will be activated immediately.
Step 7: Check whether the particular consumer is valid or not
1) If the consumer is valid
a) Decryption key will be shared with the consumer
Else
1) If the consumer is not valid
a) Decryption key will not be given to the consumer
Step 8: The consumer receives the decryption key from the proxy.
Step 9: Decrypt the input file with the decryption key.
Step 10: Finally, the consumer can view the original file of the data owner.

6. Result and Discussions

In the Fig (1), there are two processes to be done. In encryption process, the patient will update his data file, encryption key and with some conditions are stored. For decryption process, to view the details of the patients first the proxy will check whether the particular doctor is valid or not using the proxy method if the doctor is valid then the proxy will provide a key to him otherwise that the doctor will be rejected if he is not valid. Fig (2) When the doctor gets the decryption key of the patient, he has to enter that key in this page to view the details of the patients. Fig (3) The doctor will give the name and problem of that patient to get the details of that patient. Fig (4) When the doctors try to open the details of a patient then this proxy will get activated and it will act as a data owner and starts raising questions to the doctor to check whether he is valid doctor or not. Fig (5) shows the output result if the doctor gives the correct details of his occupation then the proxy will share the decryption key for him to view the details of a patient.

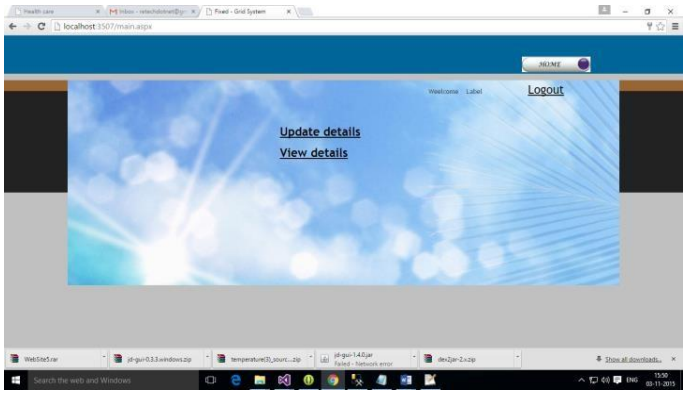

Figure 1: Patient Information

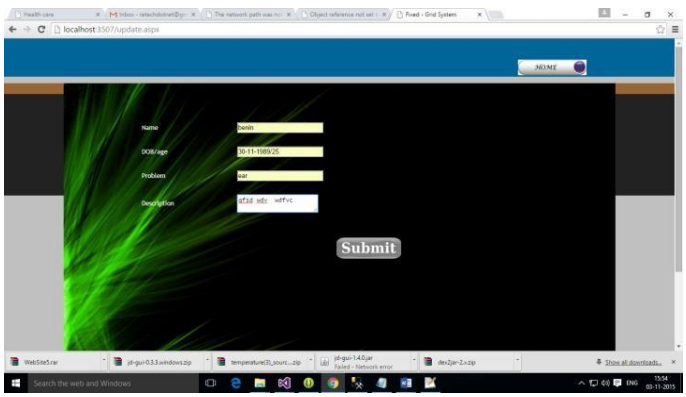

Figure 2: View Patient Details

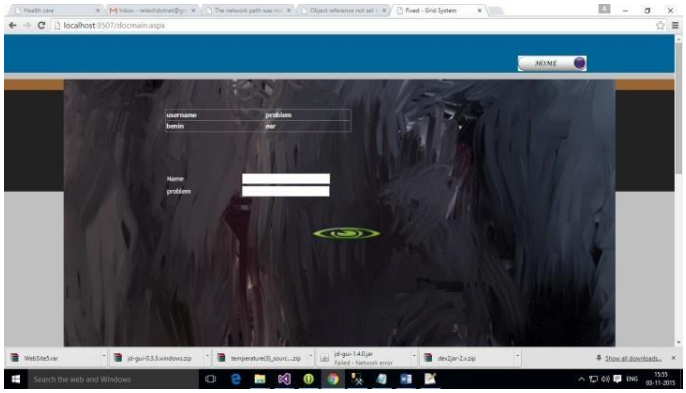

Figure 3: Doctors Usage

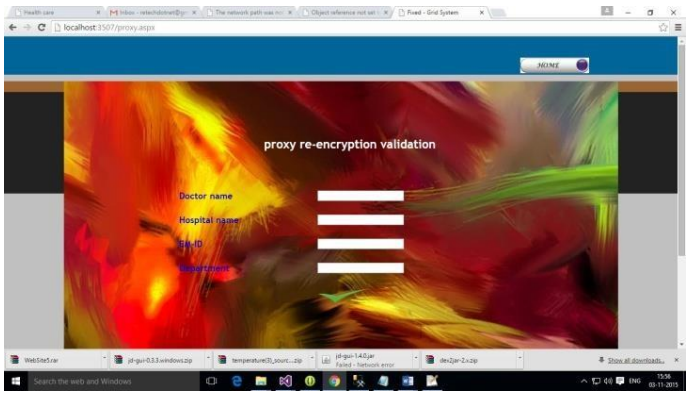

Figure 4: Proxy Validation

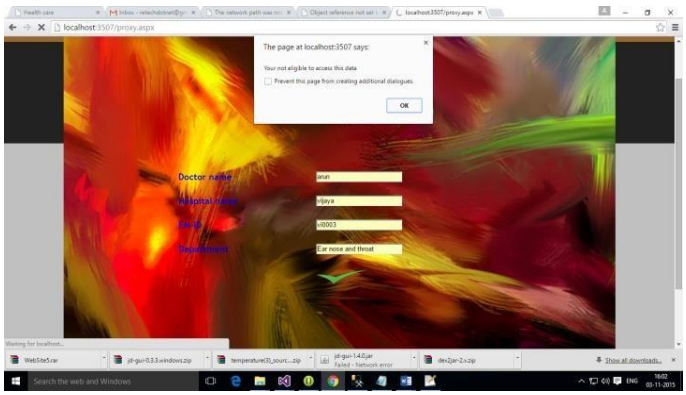

Figure 5: Final Output

7. Performance Evaluation

From the graph, we can see that the horizontal axes represent the sets of data and the vertical axes represents the security purpose in terms of percentage. We can say that the graph is basically a comparison between the existing system and the proposed

system method Fig (6). As we can see that as the data value increases, the security of the system is even higher. The proposed system is more secure than the existing one as can be seen from the figure itself.

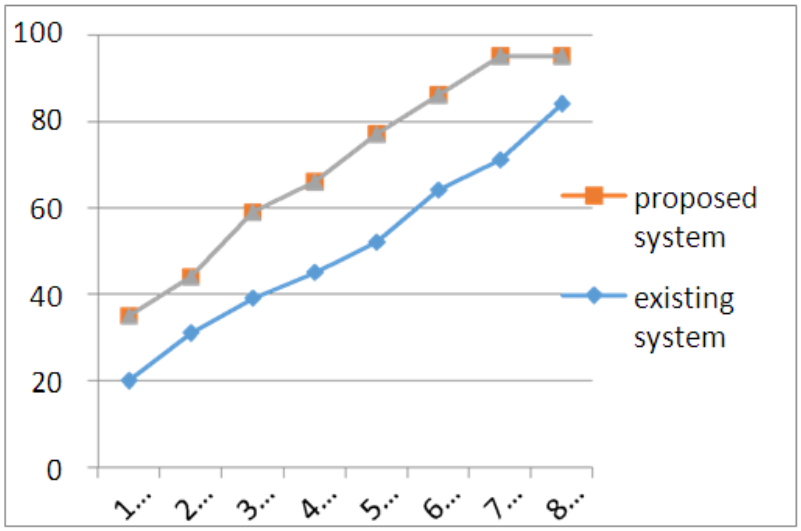

Figure 6: Comparison Graph

8. Conclusion

We established a narrative's perception, anonymous hierarchical identity-based encryption, to maintain the unusual features for ciphertext owner/consumer, conditionally sharing the data and updating of several receivers. Additionally, we have also proposed a physical system for the perception. Meantime, CCA-secure technique is demonstrated in a principle subordinate to the accommodation in a P-bilinear Diffe-Hellman presumption. Through a foremost from our intelligence, it endures a kind of primeval in the relevant works.

References

[1] G. Ateniese, K. Benson, and S. Hohenberger, "Key-private proxy re-encryption," in Topics in Cryptology-CT-RSA (Lecture Notes in Computer Science), vol. 5473. Pp. 279-294, Berlin, Germany: Springer-Verlag, 2009.

[2] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," in Network and Distributed System Security. Pp. 29-43 Berlin, Germany: Springer-Verlag, 2005.

[3] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," ACM Trans. Inf. Syst. Secure., Vol. 9, no. 1, pp. 1-30, 2006.

[4] M. Bellare and S. Shoup, "Two-tier signatures, strongly unforgeable signatures, and Fiat-Shamir without random oracles," in Public Key Cryptography (Lecture Notes in Computer Science), vol. 4450. Pp. 201-216, Berlin, Germany: Springer-Verlag, 2007.

[5] M. Blaze, G. Bleumer, and M. Strauss, "Divertible protocols, and atomic proxy cryptography," in Advances in Cryptology. Pp. 127-144, Berlin, Germany: Springer-Verlag, 1998.

[6] D. Boneh and X. Boyen, "Efficient selective-ID secure identity-based encryption without random oracles," in Advances in Cryptology-EUROCRYPT (Lecture Notes in Computer Science), vol. 3027. Pp. 223-238, Berlin, Germany: Springer-Verlag, 2004.

[7] D. Boneh, X. Boyen, and E.-J. Goh, "Hierarchical identity based encryption with constant size ciphertext," in Advances in Cryptology-EUROCRYPT (Lecture Notes in Computer Science), vol. 3494. Pp. 440-456, Berlin, Germany: Springer-Verlag, 2005.

[8] X. Boyen and B. Waters, "Anonymous hierarchical identity-based encryption (without random oracles)," in Advances in Cryptology-CRYPTO (Lecture Notes in Computer Science), vol. 4117. , pp. 290-307, Berlin, Germany: Springer-Verlag, Aug. 2006.

[9] J. Camenisch, M. Kohlweiss, A. Rial, and C. Sheedy, "Blind and anonymous identity-based encryption and authorized private searches on public key encrypted data," in Public Key Cryptography (Lecture Notes in Computer Science), vol. 5443. Berlin, pp. 196-214, Germany: Springer-Verlag, 2009.

[10] R. Canetti, S. Halevi, and J. Katz, "Chosen-ciphertext security from identity-based encryption," in Advances in Cryptology-EUROCRYPT (Lecture Notes in Computer Science), vol. 3027. Pp. 207-222, Berlin, Germany: Springer-Verlag, 2004.

[11] R. Canetti and S. Hohenberger, "Chosen-ciphertext secure proxy re-encryption," in Proc. 14th ACM Conf. Comput. Commune. Secure. (CCS), pp. 185-194, Oct. 2007

[12] C.-K. Chu and W.-G. Tzeng, "Identity-based proxy re-encryption without random oracles," in Information Security (Lecture Notes in Computer Science), vol. 4779. Pp. 189-202, Berlin, Germany: Springer-Verlag, 2007,.

[13] R. Cramer and V. Shoup, "Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack," SIAM J. Comput., Vol. 33, no. 1, pp. 167-226, Jan. 2004.

[14] L. Ducas, "Anonymity from asymmetry: New constructions for anonymous HIBE," in Topics in Cryptology-CT-RSA (Lecture Notes in Computer Science), vol. 5985. Pp. 148-164, Berlin, Germany: Springer-Verlag, 2010.

[15] K. Emura, A. Miyaji, and K. Omote, "An identity-based proxy re-encryption scheme with source hiding property, and its application to a mailing-list system," in Public Key Infrastructures, Services and Applications (Lecture

Notes in Computer Science), vol. 6711. Pp. 77-92, Berlin, Germany: Springer-Verlag, 2011.

[16] C.-I. Fan, L.-Y. Huang, and P.-H. Ho, "Anonymous multireceiver identity-based encryption," *IEEE Trans. Comput.*, Vol. 59, no. 9, pp. 1239-1249, Sep. 2010.

[17] Y. S. Rao and R. Dutta, "Recipient anonymous ciphertext-policy attribute based encryption," in *Information Systems Security* (Lecture Notes in Computer Science), vol. 8303. Berlin, Germany: Springer-Verlag,pp.329-344,2013.