International Journal of Research, Science, Technology & Management
ISSN Online: 2455-2240, Volume 5 Issue III, December 2016

ENRICHING INFORMATION BROKERING SYSTEM WITH PRIVACY USING SECURED WEB PLATFORM

Rustom B, Shehnaz Bano

ABSTRACT

In recent era, large amount of data are collected in different organizations like health care centers, Law enforcement systems, government organizations, the needs of security for inter communication through information sharing efficiently arises. Information brokering system is the process of collecting and re-distributing information. Now days, information brokering system has honest assumptions on brokers who can fulfill the requirements of user by locating right data provider where required data is present. Data broker collects large amount of detailed information from thousand or million of provider and also responsible for user authentication and request forwarding to appropriate user. With increasing concerns on protecting the sensitive data, the organizations prefer information sharing in a privacy-preserving manner, instead of purely full trust on brokers as the brokers may leak information to unauthorized users or even be hacked. It follows that sensitive data have to be encrypted before outsourcing for data privacy, user privacy. In this research work, we Enriched information brokering system with privacy using secured web platform by proposing a new secrete key generation algorithm. Also to enrich privacy used Hybrid Cryptosystem with the use of Selective encryption using AES, Vigenere Cipher, and Reverse Circle Cipher without explicit key and Hybrid Algorithm for Data Compression Using Genetic and Advanced Huffman Algorithm for word and PDF files. By using these algorithm the PPIB system using web platform will require less time than Distributed PPIB.

Index Terms: *Secrete Key, Semantic Web, Privacy Preserving.*

1. INTRODUCTION

This research work is to enable Privacy-Preserving Information Brokering System for effective utilization of outsourced and encrypted web data under the aforementioned model; our system design should achieve the privacy and performance guarantee. While sending data from data provider to data requestor via broker, it may possible that Broker can leak the data to unauthorized user so the data privacy and user privacy will be lost. Our approach implements PPIBS using secured Web platform by privacy enhancing encryption algorithms and secret key generation algorithm to maintain user and data privacy.

Information Brokering is the process of collecting and re-distributing information. Now a day, information brokering system has honest assumptions on brokers who can fulfill the requirements of user by locating right data provider where required data is present. Data broker collects large amount of detailed information from thousand or million of provider and also responsible for user authentication and request forwarding to appropriate user. Moreover, with increasing concerns on protecting the sensitive and/or proprietary data, the organizations prefer sharing data in a more secure and privacy-preserving manner, instead of establishing a purely full trust relationship on brokers as the brokers may leak data information to unauthorized entities or even be hacked. It follows that sensitive data have to be encrypted before outsourcing for data privacy.

One of the most popular ways to do so is Privacy-Preserving Information Brokering in Distributed information sharing approach. The system requires number of brokers and coordinator. As a distributed system consists of number of servers so there is many network threats at each end of the server. So it is difficult to provide security at every server. To tackle this problem, Privacy-Preserving Information Brokering in semantic web approach has been proposed.

In the past, people depended on physical computer storage or servers to run their programs. However, with the introduction of web technology, people as well as business enterprises can now access their programs through the internet as well as they can share their information with others. Now-a-days Data brokers play a vital role for locating exact data provider where the required data is present with the help of request send by data requestor. Here Information Brokering System assumes that the brokers are trusted. But there is huge threat of data leak aging by broker. This results into loss in data privacy and user privacy and due to this system performance is get degraded. So the need of secure and privacy-Preserving information brokering system arises. It is not suitable for many new applications, like healthcare or law enforcement system.

2. LITERATURE SURVEY

[1] Existing access control models typically assume that resources are stored securely under the protective care of a trusted party, which continuously observers each access request to verify if it is compliant with the specified access control policy. These scenarios where this approach is becoming no longer adequate. In this scenario, the data owner encrypts the data before outsourcing and stores them at the server. Possible access authorizations are to be enforced by the owner. In this paper, we address the problem of enforcing selective access on outsourced data without need of involving the owner in the access control process. The solution puts forward a novel approach that combines cryptography with authorizations, thus enforcing access control via selective encryption.

[2] Cloud computing is an emerging computing paradigm in which resources of the computing infrastructure are provided as services over the Internet. As promising as it is, this paradigm also brings forth many new challenges for data security, which is not within the same trusted domain as data owners. The problem of simultaneously achieving fine-graininess, scalability, and data confidentiality of access control actually still remains unresolved. This paper addresses this challenging open issue by, on one hand, defining and enforcing access.

[3] AES is iterated symmetric block cipher. The algorithm is supple in supporting any combination of data and encryption key size of 128, 192 or 256 bits. However, AES only allows a 128 bit data length that can be divided into four basic operational blocks. These blocks operate as array of bytes and organized as a matrix of the order of 4x4 that is called the state. Advantages:

- High Avalanche effect in AES
- AES is still unbreakable as it uses large key and block size

[4] A general solution to the privacy-preserving information sharing problem. First, to address the need for privacy protection, they propose a novel IBS, namely Privacy Preserving Information Brokering (PPIB). It is an overlay infrastructure consisting of two types of brokering components, brokers and coordinators. The brokers, acting as mix anonymizer, are mainly responsible for user authentication and query forwarding. The coordinators, concatenated in a tree structure, enforce access control and query routing based on the embedded nondeterministic finite automata—the query brokering automata. While providing integrated in-network access control and content-based query routing, the proposed IBS also ensures that a curious or corrupted coordinator is not capable to collect enough information to infer privacy experimental results show that PPIB provides Comprehensive privacy protection for on-demand.

[5] Reverse circle cipher is symmetric poly alphabetic block cipher uses a circular substitution and reversal transposition methods to take benefits of both confusion and diffusion. It combines the simple character level displacement principle of the Caesar cipher, the distribution principle of the Vernam poly alphabetic cipher and the diffusion principle of the transposition cipher. It does not work in the bit level neither it manipulates the orientation of bytes; rather it manipulates directly onto the ASCII (American standard code for information interchange) or UTF (Unicode transformation format) values of the text.

In [6] Cloud computing can simply be described as computing based on the internet. In this paper, propose a secure cloud storage system supporting privacy-preserving public auditing with the use of homomorphism non- linear authenticator and random masking to guarantee that the during the efficient auditing process TPA would not gain any knowledge about the data content stored on the cloud server which eliminates the burden of cloud user from the tedious and very expensive auditing task as well as the users get free from leakage of outsourced data.

[7] There are number of data compression algorithms, which are dedicated to compress different data formats. Even for a single data type there are number of different compression algorithms, which use different approaches. This paper examines lossless data compression algorithms and compares their performance. Huffman Encoding Algorithms use the probability distribution of the alphabet of the source to develop the code words for symbols. The frequency distribution of all the characters of the source is calculated in order to calculate the probability distribution. For this task a binary tree is created using the symbols as leaves according to their probabilities and paths of those are taken as the code words.

3. SYSTEM ARCHITECTURE

3.1 Secrete Key generation

The data requestor is user who request for data to coordinator by giving many attributes like name, email address, disease, address, gender and other personal information. This request accepted by coordinator then he creates secrete key for whole session also, it will send again to user for acknowledgment.

Algorithm 1: Generation of Secret key as a token

- Start
- Accept the Patient Profile attribute set A
- Convert all the attributes to String type
- Concatenate all the String to get a single String
- Accept the auto incremented User No.(no. of Users using web app.) by 1
- Value=User No. mod 9
- for i=0 to Key length<9

- do i = i+1
- Fetch value th character from the String
- Continue till 9 characters are selected
- Rotate each string character when adding new character till key length.
- Get secret key by concatenating all the 9 characters.
- return secret key
- Stop

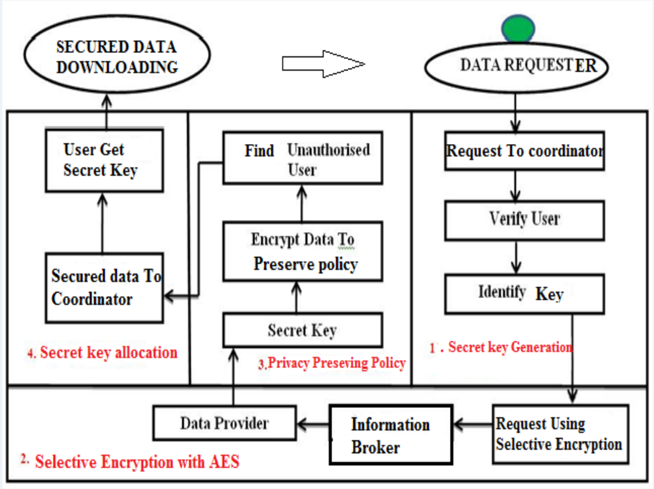

Figure 1: Proposed System

3.2 Selective Encryption with AES

In Health care application to preserve the privacy of the user with his personal data such as disease Name, Name of patient, Address, name of Hospital and name of doctor will be encrypted using selective encryption with AES algorithm and this encrypted request forward to the broker. Broker then searches a respective data provider according to specialty of diseases and to get required response data from data provider that is from another hospital.

3.3 Privacy preserving policy

The brokers forward the selective data which are selected by selective encryption with AES to respective provider. Data provider already got the secrete key from coordinator which is unique key. The data provider will encrypt the text file data using two tier encryption algorithms:

1. Vigenere cipher algorithm.

2. Reverse Circle Cipher Encryption without explicit key

If the data file provided by data provider is word or PDF file then that will be encrypted by using Huffman Compression algorithm.

Algorithm 2: Advanced Huffman Compression:

Input: File (F)

Output: Compressed File (CF)

- Start
- Set Byte array B[ ] of File F.
- Assign Sequence of positive integers { l1, l2, ……………., lk }
- Summation all as $\sum_{i=1}^{k} 2^{-li} \leq 1$

  Where each 'l' represents a node.
- Define a queue Q.
- Add all nodes into the priority queue.
- Set priority according to highest probability of bits i.e.no.of.1's in node.
- Calculate average probability of Lavg according to no. of 1's.
- Setting bounds as H[S]<= L avg < H[S]+1
- Where H[S] is entropy (Distribution)
- Remove first two nodes of higher priority from queue.
- Create a new node called Nn.
- Add two nodes from step 10 into Nn and unmatched probability.
- Stop

3.4 Key Allocation

By using secrete key which was already generated by coordinator for data provider to get the decrypted data i.e. original data from data provider to data requester.

4. CONCLUSION AND FUTURE SCOPE

4.1 Conclusion

In Recent times, Information Brokering System facing many privacy challenges. Many organizations which use IBS mostly worry about data privacy and user privacy. In this dissertation work, proposed Privacy Preserving Information Brokering System in Semantic Web using Hybrid Cryptosystem to provide confidentiality and authentication of data. The main aim is to securely store and manage the text based files using Vigenere Cipher and the Selective Reverse Circle Cipher and word, PDF based files using Advanced Huffman compression algorithm, so that only authorized users can have access stored files and data privacy is maintained. Selective encryption using AES provides user privacy. The main advantage of this system is every time unique key i.e. Secrete Key is generated.

4.2 Future Enhancement

1. As a future research this experimental study can be done on another real time application such as Law Enforcement System, through which rapidly sharing and accessing of

data related to criminal and national security investigation.

2. System privacy can be enriched with vast token generation policy.

3. Two tier encryption algorithms can be implemented for image files.

4. This technique can implement using web platform for Distributed Privacy preserving system.

5. RESULT

The figure 2 shows the comparison for compression and decompression techniques proposed in the web scenario and in the standalone system for Huffman compression and decompression algorithms for time parameter. The stand alone system is proposed by the author who actually uses the linear threads to perform the compression and decompression techniques. Whereas the proposed system by us in web system uses the implicit multi- threads to perform these operations. So the web system consumes less time and gives better results which is been shown in the above graph for multiple sizes of the text files.

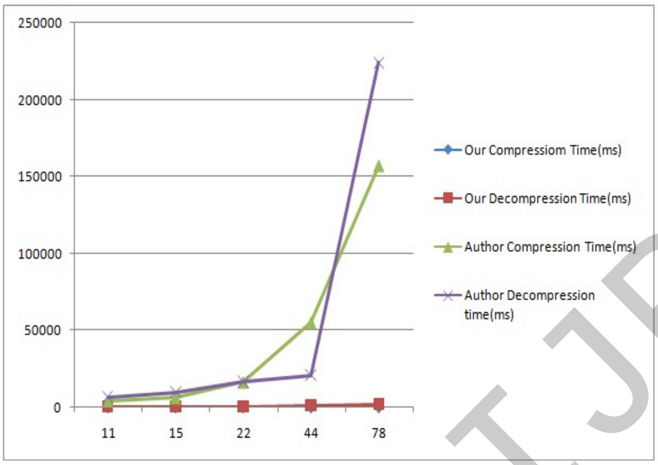

Figure 2: Compression and Decompression time Vs file size

ACKNOWLEDGEMENTS

I express true sense of gratitude towards our Head Of Department Prof. Chhaya Nayak, and my project guide Prof. Vibha Maduskar for their invaluable co-operation and guidance that they gave me throughout my project and providing me all the lab facilities, which made project work very convenient and easy. I would also like to express my appreciation and thanks to BM College of Technology Principal Dr. Nitu Trivedi and all my friends who knowingly or unknowingly have assisted me throughout my hard work.

REFERENCES

[1] Sabrina De Capitani di Vimercati, Sara Foresti, Sushil Jajodia, Stefano Paraboschi, Pierangela Sama-rati ,"Encryption Policies for Regulating Access to Outsourced Data" , ACM Transactions on Database Systems, Vol. 35, No. 2, Article 12, Publication date: April 2010.

[2] Shucheng Yu, Cong Wang, Kui Ren, Wenjing Lou ,"Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing" , INFOCOM, 2010 Proceedings IEEE , Publication Year: 2010.

[3] Mandal, A.K., Parakash, C. , Tiwari, A,"Performance evaluation of cryptographic algorithms: DES and AES", Electrical, Electronics and Computer Science (SCEECS), 2012 IEEE Students' Conference on 1-2 March 2012.

[4] Fengjun Li, Bo Luo, Peng Liu, Dongwon Lee, and Chao-Hsien Chu, “Enforcing Secure and Privacy- Preserving Information Brokering in Distributed Information Sharing" , IEEE Transactions On Information Forensics And Security, Vol. 8, No. 6, 2013.

[5] Ebenezer R.H.P. Isaac, Joseph H.R. Isaac and J. Visumathi, “ Reverse Circle Cipher for Personal and Network Security, Information Communication and Embedded Systems (ICICES), 2013 International Conference on 21-22 Feb. 2013.

[6] Cong Wang, Sherman S.-M. Chow, Qian Wang, Kui Ren, and Wenjing Lou, “Privacy-Preserving Public Auditing for Secure Cloud Storage”, IEEE Transactions On Computer,Vol 62,Feb 2013.

[7] S.R. Kodituwakku, U. S.Amarasinghe, “Comparison Of Lossless Data Compression Algorithms For Text Data”, S.R. Kodituwakku et. al. / Indian Journal of Computer Science and Engineering, Vol 1 No 4 416-425,Jan 2006.

[8] Ashwak M. AL-Abiachi, Faudziah Ahmad and Ku Ruhana “A Competitive Study of Cryptography Techniques over Block Cipher” UKSim 13th IEEE International Conference on Modelling and Simulation 2011

[9] Diaa Salama Abd Elminaam, Hatem Mohamed Abdual Kader, and Mohiy Mohamed Hadhoud ” Evaluating The Performance of Symmetric Encryption Algorithms” International Journal of Network Security, Vol.10, No.3, PP.213-219, May 2010

[10] Diaa Salama Abdul. Elminaam, Hatem Mohamed Abdul Kader and Mohie Mohamed Hadhoud “Performance Evaluation of Symmetric Encryption Algorithms” IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.12, December 2008

[11] Richard Fikes, Robert Engelmore, Adam Farquhar, Wanda Pratt, “Network-Based Information Brokers”, Knowledge System Laboratory, Stanford University

[12] Rosziati Ibrahim and Teoh Suk Kuan “Steganography Algorithm to Hide Secret Message inside an Image” Computer Technology and Application 2 (2011) 102-108

[13] Thomas Leontin Philjon. and Venkateshvara Rao. “Metamorphic Cryptography - A Paradox between Cryptography and Steganography Using Dynamic Encryption” IEEE-International Conference on Recent Trends in Information Technology, ICRTIT 2011

[14] Ashwak M. AL-Abiachi, Faudziah Ahmad and Ku Ruhana “A Competitive Study of Cryptography Techniques over Block Cipher”, UKSim 13th IEEE International Conference on Modelling and Simulation 2011

[15] Mini Malhotra, Aman Singh, Department of Computer Science, Lovely Professional University, Punjab, India, “Study of Various Cryptographic Algorithms”, International Journal of Scientific Engineering and Research (IJSER), ISSN (Online): 2347-3878,Volume 1 Issue 3, November 2013

BIOGRAPHIES

Mrs. Punam Nikam received her B.E. degree in Computer Engineering from PREC, Loni, Pune University in 2008. Currently In her post graduate Mtech course in computer science and Engineering of BM College of Technology, Indore, Madhyapradesh ,India. She is doing research work on “Enriching information brokering system with privacy using secured web platform.”

Prof. Chhaya Nayak, M. Tech (CSE) .She is working as a Head of department in computer science and Engineering of BM College of Technology, Indore, Madhyapradesh, India.

Prof. Vibha Maduskar, M.Tech (CSE) .She is working as a professor in computer science and Engineering of BM College of Technology, Indore, Madhyapradesh, India.