Volume No:3, Issue No:5 (October-2017) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

Secure Outsourced Media Search Using Cryptography

M. Pushpa Latha
M.Tech,
Department of Computer Science and Engineering,
Sanketika Vidya Parishad Engineering College,
Visakhapatnam.

V.Samuel Susan, M.Tech
Assistant Professor,
Department of Computer Science and Engineering,
Sanketika Vidya Parishad Engineering College,
Visakhapatnam.

1. ABSTRACT:

This work proposes a privacy-protection framework for an important application called outsourced media search. It explains how programmers and network professionals can use cryptography to maintain the privacy of computer data. Starting with the origins of cryptography, it moves on to explain cryptosystems, various traditional and modern ciphers, public key encryption, data integration, message authentication, and digital signatures. This scenario involves a owner, a server and a user where the owner outsources a search service to the server.

Due to lack of trust, the privacy of the client and the owner should be protected. The framework relies on multimedia hashing and random encryption. It requires involved parties to participate in a privacy enhancing protocol. Additional processing steps are carried out by the server and the user before outsourcing media features from the owner, the server has to send an approval to upload video by the owner and owner have to send encrypted key to the user to download the file without intervention of server.

The proposed framework realizes trade-offs among strength of privacy enforcement, quality of search, and complexity, as a result of the knowledge loss can be tuned throughout hashing and encryption. Intensive experiments demonstrate the effectiveness and the flexibleness of the framework.

Keywords:
Multimedia, Hashing, Data Privacy, Encryption, Decryption.

2. INTRODUCTION:

Multimedia material is nowadays everywhere on Internet. It is massively produced, distributed, and 24×7consumed by users around the globe. As a consequence, the management of multimedia data, e.g., storage and search is typically out sourced to third parties. Outsourcing offers constant availability, fault tolerance, and gigantic processing power to both data owners and users. For example, it is needed when similarity-based searches are performed on extremely large-scale databases of multimedia content. In practice, outsourcing has become a de facto standard For multimedia are positories, as exemplified by YouTube, Flicker, Picasa, etc. Outsourcing is however raising potential privacy problems: i) data owners might involuntarily confide sensitive information to third parties; ii) third parties may profile users according to their queries. Caring for privacy suggests that user queries should not be fully known by a third party server, especially when it is not trusted.

For example, in are mote diagnosis applications, a patient sends medical images to a syndrome database for automatic matching. The privacy concern is that the server should not see the query (which reveals the patient's health status) but still perform the search. This work focuses on a particular application scenario called outsourced media search. In this scenario, a data owner outsources the description of its multimedia data to an external server which provides search service to clients on behalf of the owner. It is typically suited for cloud storage and computing. Here, the untrusted server is a threat to the privacy of both the client and the owner.

Volume No:3, Issue No:5 (October-2017) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

The challenge is that the server must remain capable of performing the search service and meanwhile know little about the owner's data and the client's interests. This three-party scenario is more difficult than the conventional two-party scenario. So far most existing solutions only address the latter, and cannot be easily extended. In this work, the outsourced scenario is tackled by a privacy protection framework based onhashing and random encryption

2.1 Data Encryption and Decryption

- Encryption is the process of translating plain text data (plaintext) into something that appears to be random and meaningless (cipher text). Decryption is the process of converting cipher text back to plaintext.
- To encrypt more than a small amount of data, symmetric encryption is used. A symmetric key is used during both the encryption and decryption processes. To decrypt a particular piece of cipher text, the key that was used to encrypt the data must be used.
- The goal of every encryption algorithm is to make it as difficult as possible to decrypt the generated cipher text without using the key. If a really good encryption algorithm is used, there is no technique significantly better than methodically trying every possible key. For such an algorithm, the longer the key, the more difficult it is to decrypt a piece of cipher text without possessing the key.
- It is difficult to determine the quality of an encryption algorithm. Algorithms that look promising sometimes turn out to be very easy to break, given the proper attack. When selecting an encryption algorithm, it is a good idea to choose one that has been in use for several years and has successfully resisted all attacks.
- Encryption hides your data from curious eyes. This is a process of encoding data to prevent unauthorized person from viewing or modifying it.

The main features of data encryption are:

- Prevents unwanted access to documents and e-mail messages
- Strongest levels of encryption are very difficult to break.

2.2 Hashing:

The key in public-key encryption is based on a hash value. This is a value that is computed from a base input number using a hashing algorithm. Essentially, the hash value is a summary of the original value. The important thing about a hash value is that it is nearly impossible to derive the original input number without knowing the data used to create the hash value.

2.3 Multimedia:

Multimedia means that computer information can be represented through audio, video, and animation in addition to traditional media (i.e., text, graphics drawings, and images).Multimedia is the field concerned with the computer-controlled integration of text, graphics, drawings, still and moving images (Video), animation, audio, and any other media where every type of information can be represented, stored, transmitted and processed digitally.

2.4 Data Privacy:

Data privacy, also called information privacy, is the aspect of information technology (IT) that deals with the ability an organization or individual has to determine what data in a computer system can be shared with third parties.

3. LITERATURE SURVEY:

Literature survey is the most important step insoftware development process before developing the tool it is necessary to determine the time factor economy and company strength. Once these things are satisfied, then the next steps are to determine which operating system and language can be used for developing the tool. Once the programmers start building the tool the programmers need lot of external support.

Volume No:3, Issue No:5 (October-2017) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

This support can be obtained from senior programmers, from book or from websites. Before building the system the above consideration are taken into account for developing the proposed system.

L. Weng, L. Amsaleg, A. Morton, S. Marchand-Maillet, worked on the privacy preserving outsourcing media search. This work focuses on a particular application scenariocalled outsourced media search. In this scenario, a data owneroutsources the description of its multimedia data to an external server which provides search service to clients on behalf of theowner. It is typically suited for cloud storage and computing.Here, the untrusted server is a threat to the privacy of boththe client and the owner. The challenge is that the servermust remain capable of performing the search service and Meanwhile know little about the owner's data and the client's interests. This three-party scenario is more difficult than theconventional two-party scenario. So far most existing solutions

Only address the latter, and cannot be easily extended. In this work, the outsourced scenario is tackled by a novel privacy protection framework based on hashing andrandom encryption. In a nutshell, database items and queries are represented by content-based hash values; the hash value of each database item is divided into two parts, one of whichis encrypted. The unencrypted part is used by the server forapproximate indexing and search.

4. PRIVACY PROTECTION TECHNIQUES:

- Cryptography(Random encryption technique)
- Hashing

4.1 Cryptography(Random encryption technique):

Cryptography prior to the modern age was effectively synonymous with encryption, the conversion of information from a readable state to apparent nonsense.

The originator of an encrypted message shared the decoding technique needed to recover the original information only with intended recipients, thereby precluding unwanted persons from doing the same. The cryptography literature often uses Alice ("A") for the sender, Bob ("B") for the intended recipient, and Eve ("eavesdropper") for the adversary. Since the development of rotor cipher machines in World War I and the advent of computers in World War II, the methods used to carry out cryptology have become increasingly complex and its application more widespread. Modern cryptography is heavily based on mathematical theory and computer science practice; cryptographic algorithms are designed around computational hardness assumptions, making such algorithms hard to break in practice by any adversary. It is theoretically possible to break such a system, but it is infeasible to do so by any known practical means. These schemes are therefore termed computationally secure; theoretical advances, e.g., improvements in integer factorization algorithms, and faster computing technology require these solutions to be continually adapted.

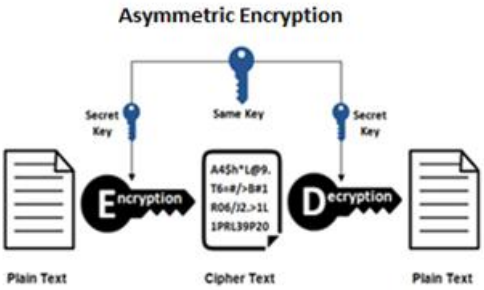
There exist information-theoretically secure schemes that provably cannot be broken even with unlimited computing power—an example is the one-time pad—but these schemes are more difficult to implement than the best theoretically breakable but computationally secure mechanisms. The growth of cryptographic technology has raised a number of legal issues in the information age. Cryptography's potential for use as a tool for espionage and sedition has led many governments to classify it as a weapon and to limit or even prohibit its use and export. In some jurisdictions where the use of cryptography is legal, laws permit investigators to compel the disclosure of encryption keys for documents relevant to an investigation. Cryptography also plays a major role in digital rights management and copyright infringement of digital media.

Volume No:3, Issue No:5 (October-2017) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

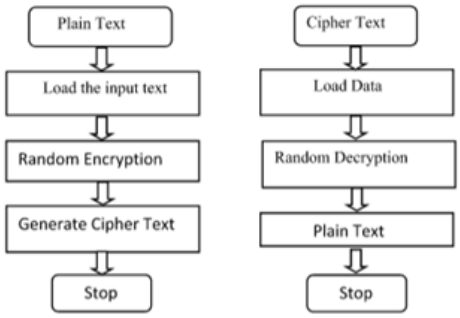
Random Encryption Algorithm:

Character type cipher is always used in web application system and can be deciphered by the illegal users through "run dictionary", so, a new random encryption algorithm for character type cipher is put forward in this paper. The encryption parameters are randomly generated in the algorithm, and random confusion is adopted in the cipher text structure, so the same plaintext can produce different cipher text.the experimentation shows that the algorithm is feasibility and validity. The random algorithm is based on randomization and is used to convert the input into a cipher text incorporating the concept of cryptographic salt. This algorithm forms the basis of the proposed approach.

Any input in web forms will containnumbers, uppercase, lowercase or specialcharacters. Keeping this in mind the input from user is encrypted based on randomization. In our algorithm the validinputs are numbers, lowercase or uppercase characters and at most 10 special characters. The reason for choosing only 10 special characters is that they are rarely used and for additional security. Each character in the input can have 72 combinations (26 lowercase, 26 uppercase, 0-9 and 10 special characters). Hence for a 6 character input there can be 726 combinations possible. To encrypt the input, each input character is given four random values.



CRYPTOGRAPHY ALGORITHM



4.2 Hashing Algorithm

Hashing is the transformation of a string of characters into a usually shorter fixed-length value or key that represents the original string. Hashing is used to index and retrieve items in a database because it is faster to find the item using the shorter hashed key than to find it using the original value. It is also used in many encryption algorithms. The hash function is used to index the original value or key and then used later each time the data associated with the value or key is to be retrieved. Thus, hashing is always a one-way operation. There's no need to "reverse engineer" the hash function by analyzing the hashed values. In fact, the ideal hash function can't be derived by such analysis. A good hash function also should not produce the same hash value from two different inputs. If it does, this is known as a collision. A hash function that offers an extremely low risk of collision may be considered acceptable.

5. EXISTINGSYSTEM

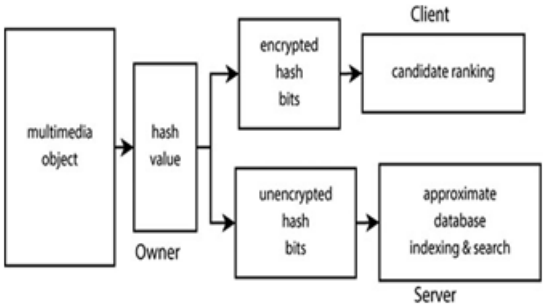
- Privacy-Preserving frame work is the system which is facilitates the information on online media search. Here each user, owner and server having their own login credentials, owner can upload the multimedia items with approval given by admin/server then user can see these all videos.
- One-way hashing and encryption add ambiguity to data and make it difficult for the server to work out contents from database items and queries, so the privacy of both the owner and the client is enforced.

Volume No:3, Issue No:5 (October-2017) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

- In this system we are getting the security issues because not implemented the standard cryptography algorithm so without provide full encryption we couldn't able to get the full security for our applications.

6. PROPOSED SYSTEM:

- Here overcome the drawback in existing system through implementing the Encryption & Decryption algorithms for providing security.
- In proposed system implemented the Encryption & Decryption algorithms for protect the security for data and at the same time maintain the security for user and owner credentials.
- The proposed framework realizes trade-offs among the strength of privacy enforcement, the quality of search, and complexity, because the information loss can be tuned during hashing and encryption.
- Due to lack of trust, the privacy of the client and the owner should be protected. The framework relies on multimedia hashing and random encryption.
- To provide the full security for users and data By implementing the random encryption and Decryption. Here decision making is the great enhancement for providing the security for user and data by using random number generation technique.



A flow chart of the proposed solution.

7. MODULE DESCRIPTIONS:

7.1 Upload Module:

In this module admin willupload the multimedia items. These uploaded multimedia items can use every registered users and the same time uploaded videos can delete by admin.

7.2 Download Module:

In this module the file which is uploaded by the staff will be downloaded. To download the files an encrypted key will be generated to the user registered mail. If the input key matches then the uploaded file will be downloaded

7.3 Display Video Module:

In this module if the client wantto just watch the video without downloading then he can watch the video online without downloading and at the same time he can store the data permanently for future use.

7.4 Send Mail Module:

Sender first verifies a receiver's certificate and encrypts an email by the receiver's public key; then the receiver decrypts the received email with his private key. IBE avoids the certificate verification of PGP. Using IBE, a sender directly encrypts an email using a receiver's email address. Though both PGP and IBE keep the security of cloud email, their performances are less than CIBPRE. When a sender wants to send an encrypted email to multiple receivers, the size of the cipher text generated by CIBPRE is constant. In contrast, both PGP and IBE cause the size linear with the number of receivers. When a sender wants to forward a historically encrypted email to multiple receivers, CIBPRE only requires the sender to generate a re-encryption key (with constant size) and send the key to cloud, and then the cloud encrypts the email and generates a constant size cipher text.

7.5 Owner Module:

The Owner module will have all the data that belongs to the staff side and the data that he is uploaded details will also stored in the owner side. The user details will also store in the owner side .Owner can delete the files which the manager wants to delete.

Volume No:3, Issue No:5 (October-2017) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

8. USAGE:

The project is identified by the merits of the system offered to the user. The merits of this project are as follows:

- It's a web-enabled project.
- This project offers user to enter the data through simple and interactive forms. This is very helpful for the client to enter the desired information through so much simplicity.
- The user is mainly more concerned about the validity of the data, whatever he is entering. There are checks on every stages of any new creation, data entry or updating so that the user cannot enter the invalid data, which can create problems at later date.
- Sometimes the user finds in the later stages of using project that he needs to update some of the information that he entered earlier. There are options for him by which he can update the records. Moreover there is restriction for his that he cannot change the primary data field. This keeps the validity of the data to longer extent.
- User is provided the option of monitoring the records he entered earlier. He can see the desired records with the variety of options provided by him.
- Data storage and retrieval will become faster and easier to maintain because data is stored in a systematic manner and in a single database.
- Decision making process would be greatly enhanced because of faster processing of information since data collection from information available on computer takes much less time than manual system.
- To propose the Cryptography Algorithms for maintain the security user credentials and user data.
- By using random encryption and decryption technique for storing the user credentials in secure format.
- To propose random number generation for sending the one time password to mail which is used for down load the multimedia items.
- Random number generation technique used for OTP creation and Encryption& Decryption algorithms for protect the security for user credentials and at the same time maintain the security for user data.

9. CONCLUSION:

In this paper, a survey of the broad areas of privacy-preserving data and the underlying algorithms is done. The broad areas of classification includes Privacy-preserving data publishing, Privacy-Preserving Applications, Distributed Privacy, cryptography and adversarial collaboration are analyzed. A variety of data modification techniques such as randomization has been studied and analyzed based on their activities Outsourced media search is a challenging scenario, where the privacy of the owner and the clients should be protected. We address this scenario by a privacy protection framework. The framework requires the owner to send an encrypted key to the client registered mail to download their multimedia items, which are then outsourced. At the client, multimedia items are visible to watch but for downloading them the client should provide a valid mail to get the encrypted key.

10. REFERENCES:

[1] P. Weinzaepfel, H. Je´gou, and P. Perez, "Reconstructing an image from its local descriptors," in Proc. of IEEE Conference on Computer Vision and Pattern Recognition (CVPR), June 2011, pp. 337–44.

[2] L. Weng, L. Amsaleg, A. Morton, and S. Marchand-Maillet, "A privacy-preserving framework for large-scale content-based information retrieval," IEEE Transactions on Information Forensics and Security, vol. 10, no. 1, pp. 152–167, Jan. 2015.

[3] S. Rane and P. Boufounos, "Privacy-preserving nearest neighbor methods: comparing signals without revealing them," IEEE Signal Processing Magazine, vol. 30, no. 2, pp. 18–28, 2013.

Volume No:3, Issue No:5 (October-2017) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

[4] R. Lagendijk, Z. Erkin, and M. Barni, "Encrypted signal processing for privacy protection: Conveying the utility of homomorphic encryption and multiparty computation," IEEE Signal Processing Magazine, vol. 30, no. 1, pp. 82–105, 2013.

[5] Z. Erkin, A. Piva, S. Katzenbeisser, R. Lagendijk, J. Shokrollahi, G. Neven, and M. Barni, "Protection and retrieval of encrypted multimedia content: when cryptography meets signal processing," EURASIP Journal on Information Security, p. 20, 2007.

[6] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in Advances in cryptology–EUROCRYPT'99. Springer, 1999, pp. 223–238.

[7] M. Naor and B. Pinkas, "Efficient oblivious transfer protocols," in Proc. of the 12th Annual ACM-SIAM Symposium on Discrete Algorithms (SODA), 2001, pp. 448–457.

[8] A. C.-C. Yao, "How to generate and exchange secrets," in Proc. of 27th Annual Symposium on Foundations of Computer Science (FOCS), Oct. 1986, pp. 162–167.

[9] J. Bringer, H. Chabanne, and A. Patey, "Privacy-preserving biometric identification using secure multiparty computation: An overview and recent trends," IEEE Signal Processing Magazine, vol. 30, no. 2, pp. 42–52, 2013.

[10] Z. Erkin, M. Franz, J. Guajardo, S. Katzenbeisser, I. Lagendijk, and T. Toft, "Privacy-preserving face recognition," in Proc. of 9th International Symposium on Privacy Enhancing Technologies (PET), 2009, pp. 235–253.

[11] A.-R. Sadeghi, T. Schneider, and I. Wehrenberg, "Efficient privacypreserving face recognition," in Proc. of 12th International Conference on Information Security and Cryptology (ICISC), 2009, pp. 229–244.

[12] M. Osadchy, B. Pinkas, A. Jarrous, and B. Moskovich, "SCiFI - A system for secure face identification," in Proc. of IEEE Symposium on Security and Privacy (SP), 2010, pp. 239–254.

[13] P. Sabbu, U. Ganugula, S. Kannan, and B. Bezawada, "An oblivious image retrieval protocol," in Proc. of IEEE International Workshop on Advanced Information Networking and Applications, 2011, pp. 349–354.

[14] M. Gertz and S. Jajodia, Eds., Handbook of Database Security - Applications and Trends.Springer, 2008.