International Journal of Recent Trends in Engineering & Research
ISSN(ONLINE) : 2455-1457
IMPACT FACTOR : 3.344

ENSURING INTEGRITY FOR DATA EXCHANGE BY USING DATA COLORING PROCESS

S.GUNA SUNDHARI [1],M.JAGATHA[2], S.KANMANI[3],M.KARPAGAM [4]
Mr .G.SENTHIL KUMAR[5]
[1,2,3]Information Technology, S.K.P Engineering College
[4]Assisstant Proffesor, Information Technology, S.K.P Engineering College

Abstract: Maintaining user privacy and preserving data integrity via Encryption and decryption technique. Using a trust-overlay network over multiple data centers to implement a reputation system for establishing trust between Sender and receiver is becoming mandatory .Cryptographic techniques protect shared data objects and ensure the security level data transfer process. These techniques safeguard multi-way authentications and strengthen the security for accessing confidential data in both public and privation However the problem there is no guarantee that only the legitimate user is accessing the confidential data and maintaining privacy till the user quits the secured communication. Hence to overcome the problem the Data coloring and software watermarking techniques is established to provide the authenticity that is legitimate user only sent the data. The most common email encryption is called PKI. In order to open the encrypted file an exchange of keys is done.

Keywords: *Key generation, Data coloring, Encryption, Decryption, Color generation mechanism.*

I. INTRODUCTION

Secure data transmission refers to the transfer of data such as confidential or proprietary informationover a secure channel. Many secure transmission methods require a type of encryption. The most common email encryption is called PKI. In order to open the encrypted file an exchange of keys is done. Secure transmissions are put in place to prevent attacks such as ARP spoofing and general data loss. Software and hardware implementations which attempt to detect and prevent the unauthorized transmission of information from the computer systems to an organization on the outside may be referred to as Information Leak Detection and Prevention (ILDP), Information Leak Prevention (ILP),Content Monitoring and Filtering (CMF) or Extrusion Prevention systems and are used in connectionwith other methods to ensure secure transmission of data.

II. RELATED WORKS

These SR technologies have been applied to automatically transcribe instructor's lecture and process the transcription to acquire near verbatim lecture transcripts for students [1], [2], [3]. The benefits of producing lecture transcripts have shown to enhance both learning and teaching. Students could make up for missed lectures as well as to corroborate the accuracy of their own notes during the lectures they attended. Coupled with a recorded audio/video lecture track and copies of the lecture slides, students could recreate the lecture material for replicating the lecture at their own learning pace. These lecture transcripts and additional multimedia recordings also enable instructors to review their own teaching performance and lecture content to assist them to improve individual pedagogy [4]. Likewise, SR has been used for quickly searching certain keywords to retrieve specific text or video lecture content [5], [6]

III. PROPOSED SYSTEM

To address these issues, a reputation-based trust- management scheme augmented with data coloring and software watermarking is prepared and proposed which ensures the authorization and authenticity. Key generation mechanism is used to generate the key to color generation mechanism, encryption and decryption. The encrypted data can be fetching with the color drops then send to the receiver. The receiver can decrypt the colored data and match the color drops for authenticity which ensure the authorization. And decrypt the encrypted original data to plain text.

ADVANTAGES :

The key secrecy is to be maintained which brings the effective key sharing between the sender and receiver.

The key which is used to share the confidential information plays a vital role in encrypting and decrypting messages.

It attempt to detect and prevent the unauthorized transmission of information .

IV. MODULES

In our project ,we have four modules .They are explained as follows :

1. Key generation mechanism
2. Color generation Mechanism
3. Data coloring
4. Color matching

4.1)KEY GENERATION MECHANISM :

In this project the key used by both the sender and receiver should be same as the proposal is designed based on it The sender and receiver uses a same key to Encrypt and Decrypt and same key is followed for Data coloring. Hence the Symmetric key cryptography helps to achieve the proposal of this project. The key secrecy is to be maintained which brings the effective key sharing between the sender and receiver. Diffe-hellman key exchange algorithm and Two-fish algorithm is used.

4.2)COLOR GENERATION ALGORITHM:

By using the key, the color generation will take place by using Interactive generic Algorithm The RGB is used for Random color generation for different key value The color generation data flow diagram and algorithm is given below

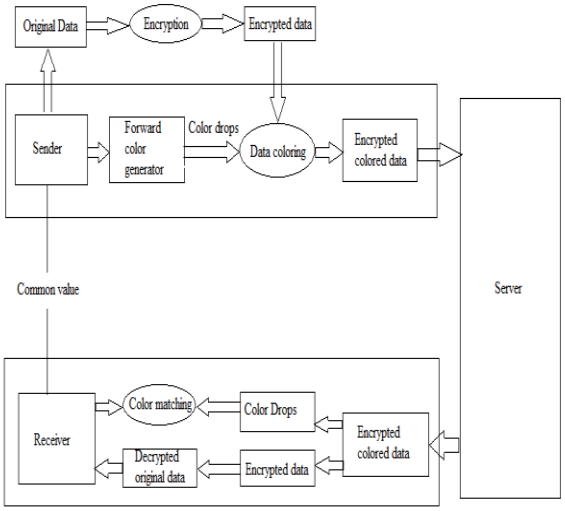
4.3)DATA COLORING:

Color Generation process is done with the Interactive generic color algorithm with the help of key value which is known by the sender and receiver .Once the color is generated then it is converted into any file format .Water marking is a process in which the data can be hidden or embedded into the generated colored file.. The trust model DeyiLi and his colleagues propose offers a second-order fuzzy membership function for protecting data owners. This model is extended here to add unique data colors to protect large datasets during data transfer .The above process is called as Data coloring.

4.4COLOR MATCHING:

The color matching process is used for authenticity Once the sender send the encrypted colored data to the user, then the user can also generate color with the same key After generating the color then the color matching process is take place with the color drops of sender and the generated color It ensures the authentication The Data flow diagram is given below

V. ARCHITECTURE



VI. CONCLUSION

The proposed system has a great advantage over the existing system. The proposed system has the most secure authentication mechanism in accessing the data.

Authenticity is made which ensure that the legitimate user are accessing the data With a Data coloring and Watermarking is done and the results are transfer the data with secured manner using color generation mechanism.

REFERENCE

1. Kai Hwang "Trusted Cloud Computing with Secure Resources and Data Coloring"Volume: 14, Issue: 5, IEEE Sept 2010.
2. Yu-Chao Liu, Yu-Tao Ma, Hai-Su Zhang, De-Yi Li, Gui-Sheng "A Method for Trust Management in Cloud Computing: Data Coloring by Cloud Watermarking", IJAC Aug 2011.
3. K. Hwang, S. Kulkarni, and Y. Hu, "Cloud Security with Virtualized Defense and Reputation-Based Trust Management," IEEE Int'l Conf. Dependable, Autonomic, and Secure Computing (DASC 09), IEEE CS Press, 2009.
4. Feng Zhu, Wei Zhu, Matt W. Mutka, "Private and Secure Service Discovery via Progressive and Probabilistic Exposure" VOL. 18, NO. 11, IEEE November 2008.
5. R. Zhou, and K. Hwang, "Power Trust: A Robust and Scalable Reputation System for Trusted Peer-to-Peer Computing," IEEE Trans. Parallel and Distributed Systems, Apr. 2007, pp. 460–473.
6. E. Michail, A.P. Kakarountas, A. Milidonis, "Efficient implementation of the keyed-hash message authentication code (HMAC) using the SHA-1 Hash function"©2004 IEEE.