An Implementation of Secure Data Exchange Ensuring Authentication and Authorization Using Color Drops

S.Sandosh 1, S.Uthayashangar 2

1 (Dept. of Information Technology, Manakula Vinayagar institute of technology/Pondicherry University /India)
2 (Dept. of Information Technology, Manakula Vinayagar institute of technology/Pondicherry University /India)

Abstract- Secure communication is when two entities are communicating and do not want a third party to listen in. For that they need to communicate in a way not susceptible to eavesdropping or Interception. Here maintain user privacy, and preserve 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 private. 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.

Key terms: - Color generation mechanism, Data coloring, Decryption, Encryption, Group Key generation/management.

I. INTRODUCTION

Secure data transmission refers to the transfer of data such as confidential or proprietary information over 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 connection with other methods to ensure secure transmission of data.

Even though these techniques are play a vital role but there will be chance to hacker or attacker can able to steal the data and there is no assurance that the authorized use can only access those data. the data may be encrypted or not but the unauthorized person can also able to access the data. 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.

II. DEFINITION & TERMINOLOGY

Cryptography defines the art and science of transforming data into a sequence of bits that appears as random and meaningless to a side observer or attacker.

Cryptanalysis is the reverse engineering of cryptography—attempts to identify weaknesses of various cryptographic algorithms and their implementations to exploit them. Any attempt at cryptanalysis is defined as an attack.

Cryptology encompasses both cryptography and cryptanalysis and looks at mathematical problems that underlie them. Cryptosystems are computer systems used to encrypt data for secure transmission and storage.

Plaintext is message or data which are in their normal, readable (not crypted) form.

Encryption: Encoding the contents of the message in such a way that hides its contents from outsiders.

Cipher text results from plaintext by applying the encryption key.

Decryption: The process of retrieving the plaintext back from the cipher text.

Key: Encryption and decryption usually make use of a key, and the coding method is such that decryption can be performed only by knowing the proper key.
Watermark is a recognizable image or pattern in paper that appears as various shades of lightness/darkness when viewed by transmitted light (or when viewed by reflected light, atop a dark background), caused by thickness or density variations in the paper. Watermarks have been used on postage stamps, currency, and other government documents to discourage counterfeiting. There are two main ways of producing watermarks in paper; the dandy roll process, and the more complex cylinder mould process.

Data coloring is a process of generation the colors with the different values which may produces output in jpeg format.

III. KEY GENERATION MECHANISM

The key which is used to share the confidential information plays a vital role in encrypting and decrypting messages. Hence in symmetric cryptography both the sender and receiver keys are same where asymmetric cryptography has overcome the security level of the symmetric cryptography as the asymmetric uses one public key for encryption and private key for decryption. But in this project the key used by both the sender and receiver should be same as the proposal is designed based on it. Hence the symmetric key cryptography is to be followed. Though 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. Hence the Diffie-Hellman key exchange algorithm is used.

Diffie–Hellman establishes a shared secret that can be used for secret communications while exchanging data over a public network. In this algorithm a value is taken on both the sides sender and receiver, and the keys are generated both the sides with the following.

<table>
<thead>
<tr>
<th>Alice</th>
<th>Bob</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secret</td>
<td>Public</td>
</tr>
<tr>
<td>a</td>
<td>p, g</td>
</tr>
<tr>
<td>a</td>
<td>p, g, A</td>
</tr>
<tr>
<td>a, s</td>
<td>p, g, A, B</td>
</tr>
</tbody>
</table>

1. Alice and Bob agree to use a prime number p=23 and base g=5.
2. Alice chooses a secret integer a=6, then sends Bob A = g^a mod p
   - A = 5^6 mod 23
   - A = 15,625 mod 23
3. Bob chooses a secret integer b=15, then sends Alice B = g^b mod p
   - B = 5^{15} mod 23
   - B = 30,517,578,125 mod 23
   - B = 19
4. Alice computes s = B^a mod p
   - s = 19^6 mod 23
   - s = 47,045,881 mod 23
   - s = 2
5. Bob computes s = A^b mod p
   - s = 8^{15} mod 23
   - s = 35,184,372,088,832 mod 23
   - s = 2
6. Alice and Bob now share a secret (the number 2) because 6*15 is the same as 15*6.

These values are used to generate three different keys common algorithm and the three different key are used to generate the color and data coloring mechanism and also the original data can be encrypted with the generated key by the sender. The receiver side the colored data an be decrypted and color matching process has been made to ensure authenticity and also the encrypted original data can be decrypted to plain text.

IV. CRYPTOGRAPHIC ALGORITHM

Here to provide an encryption to the data the cryptographic technique is used. By the proposal the same key is used for cryptography and coloring mechanism so that we have to choose only symmetric key cryptography so that the TWOfish cryptographic algorithm is used.

In cryptography, Twofish is a symmetric key block cipher with a block size of 128 bits and key sizes up to 256 bits. It was one of the five finalists of the Advanced Encryption Standard contest, but it was not selected for standardization. Twofish is related to the earlier block cipher Blowfish.
Twofish’s distinctive features are the use of pre-computed key-dependent S-boxes, and a relatively complex key schedule. One half of an n-bit key is used as the actual encryption key and the other half of the n-bit key is used to modify the encryption algorithm (key-dependent S-boxes). Twofish borrows some elements from other designs; for example, the pseudo-Hadamard transform (PHT) from the SAFER family of ciphers. Twofish has a Feistel structure like DES. On most software platforms Twofish was slightly slower than Rijndael (the chosen algorithm for Advanced Encryption Standard) for 128-bit keys, but it is somewhat faster for 256-bit keys.

Twofish was designed by Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, and Niels Ferguson; the "extended Twofish team" who met to perform further cryptanalysis of Twofish and other AES contest entrants included Stefan Lucks, Tadayoshi Kohno, and Mike Stay.

V. PROPOSAL

Data coloring: the architecture uses data coloring at data object level. This lets us segregate user access and insulate sensitive information from sender.

Watermarking: The Data transfer is use of shared files and datasets, which compromise privacy, security, and copyright in a environment. The user needs to work in a trusted software environment that provides useful tools for building applications over protected datasets. In older days, watermarking was mainly used for digital copyright management. Later some experts have suggested using watermarking to protect software modules. The trust model Deyi Li 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 in the cloud.

The above Figure shows the forward and backward color-generation processes. The color drops (data colors) are added into the input photo (left) and remove color to restore the original photo (right). The coloring process uses three data characteristics to generate the color: the expected value (Ex) depends on the data content known only to the data owner, whereas entropy (En) and hyperentropy (He) add randomness or uncertainty, which are independent of the data content and Collectively, these three functions generate a collection of cloud drops to form a unique “Color” that the providers or others users can’t detect.

The use of data coloring at varying security levels based on the variable cost function applied. This Progressive approach can also be applied to protect documents, images, data, and relational databases during transmission. The figure shows the details involved in the color-matching process, which aims to associate a colored data object with its owner, whose user identification is also colored with the same Ex, En, and He identification characteristics. The color-matching process assures that colors applied to user identification match the data colors. This can initiate various trust-management events, including authentication and authorization. Combining secure data storage and data coloring, the data objects can be prevented from being damaged, stolen, altered, or deleted. Thus, legitimate users have sole access to their desired data objects. The computational complexity of the three data characteristics is much lower than that performed in conventional encryption and decryption calculation. The watermark-based scheme thus incurs a very low overhead in the coloring and decoloring processes. The En and He functions’ randomness guarantees data owner privacy. These characteristics can uniquely distinguish different data objects.

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 because, a 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.

VII. REFERENCES


