ISSN 2277-3061
Volume 15 Number6
International journal of Computers and Technology

Secret Sharing Approach in Multi-database System

Shipra Choudhary, Apeksha Katarni, Shweta Manjrekar, Mrs. Vidyullata Devmane
Mrs. Vaishali Hirlekar
B.E Student, Computer Engineering Department, SAKEC, Chembur, Mumbai, India
choudhary_shipra@ymail.com
B.E Student, Computer Engineering Department, SAKEC, Chembur, Mumbai, India
akatarni@gmail.com
B.E Student, Computer Engineering Department, SAKEC, Chembur, Mumbai, India
shweta26295@gmail.com
Assistant Professor, Computer Engineering Department, SAKEC, Chembur, Mumbai, India
devmane.vidyullata@gmail.com
Assistant Professor, Computer Engineering Department, SAKEC, Chembur, Mumbai, India
vaishali.hirlekar@gmail.com

ABSTRACT

Secret sharing schemes are ideal for storing highly sensitive data. A secret is divided into many parts and every participant gets his unique part. If we combine all of these parts and try regenerating the secret then it might be impractical, and therefore the threshold scheme is used. Shamir's secret sharing scheme supports the same. Here, some of the parts or all of them are required to reconstruct the secret. Any threshold number of parts are sufficient to reconstruct the original secret. The Administrator who is an authorized entity has a set of files which are encrypted and stored on multiple databases so as to achieve confidentiality and availability of data. Whenever a Client requests to access the files, the Administrator performs authentication of the user through an Authentication module, who makes use if Shamir's secret sharing concept. This is similar to the One Time Password (OTP) mechanism. If the Client is authentic, Administrator grants him the decryption key and the Client can access the file. In this paper, we have proposed this scheme in detail using which we can provide security, replication of data and authentication.

Keywords

Security Goals, Symmetric Key Cryptosystem, Shamir's Secret Sharing Scheme, Threshold, Lagrange Polynomial Interpolation, One Time Password (OTP).

Academic Discipline And Sub-Disciplines

Computer Science - Data Security , Cryptography

SUBJECT CLASSIFICATION

Authentication

INTRODUCTION

Data is regarded as an important asset in recent years. If crucial information gets leaked then many loss such as financial losses, lost sales, customer fleeing to competitors may occur. Hence, there is a need to protect data. Cryptography, a word with Greek origins, means "secret writing". However, we use the term to refer to the science and art of transforming messages to make them secure and immune to attacks[1]. In order to ensure that the data does not reach to unintended or unauthorized person, it is encrypted and stored. Encryption provides confidentiality of sensitive data over insecure channels. There are two types of cryptosystems: *Symmetric key cryptosystem* and *Asymmetric key cryptosystem*. *Symmetric key cryptosystem* uses same key for both encrypting and decrypting the data. These encryption and decryption algorithms are inverse of each other. Examples of symmetric key system include Advanced Encryption Scheme (AES) and Blowfish[2]. *Asymmetric key cryptosystem* uses two keys, namely the public key and the private key. Message is encrypted using a public key and decrypted using a private key. A system is prone to failures because of which availability of data can be affected. And hence multiple databases are being used to store confidential information. Now even if one database is down, client requests can be fulfilled by using other databases. This increases reliability of the system. Simply storing data on databases won't be sufficient. We need to ensure it goes in safe hands. And hence secret sharing scheme is applied. A secret sharing scheme is a technique of sharing a secret *s* into *n* pieces, called shares, and distributing them to a set of *n* users (participants) in such a way that only certain qualified subsets of users can recover the secret by combining their shares and any unqualified subset of users can not do so[3]. Blakley[4] scheme uses hyperplane geometry to solve the secret sharing problem. The secret is a point in a t-dimensional space. The *n* shares are constructed such that each share is defined as an affine hyperplane that passes through the secret point.This scheme does not give flexibility to specify fewer than *w* shares to reconstruct the secret. The more generalized method is Shamir's (*t, n*) threshold scheme[5]. Its simplicity lies in its implementation. A secret sharing scheme is called a *(t, n)* threshold secret sharing scheme for $t \leq n$ if the following two conditions are satisfied: (1) knowledge of any *t* or more shares makes the secret *s* computable; (2) knowledge of any *t-1* or fewer shares leaves *s* completely undetermined in information theoretic sense[3]. This concept can be used by the owners of secure and confidential information to perform

authentication of a user requesting the data. Combining any *t-1* or fewer shares will not regenerate the secret. A Client is authenticated only if she is able to provide required number of shares of the secret correctly.

RELATED WORK

To collect knowledge related to security goals like confidentiality, integrity and availability, symmetric encryption-decryption algorithms, secret sharing schemes and multi-database structure and properties we referred published papers and cryptography and security books. We have also taken guidance from professors. We referred books such as Cryptography and Network Security by Forouzan, etc.

We have conceived this idea from online banking transactions which we perform almost daily. Apart from providing login credentials like username and password, a user has to provide a secret code also which is valid only for that session. This is called One Time Password (OTP). It can be sent via an email or a text message. An intruder can easily gain access to the login credentials of the user. These details may help the attacker to obtain secure information from the file-owner (Administrator). The potential damage to the trustworthiness and reliability of the system can be very significant. And hence in such a scenario we can still save the data getting in wrong hands by performing a two-way authentication of the user. We can provide a dynamically generated value which is real-time and ask for that value whenever she wants to access the files. This is in contrast to the static password. It is also advantageous to a user who has same passwords for multiple accounts. Even if the user's traditional password is stolen or compromised, the intruder will still need to authorize himself by feeding the dynamically generated password. They are also not vulnerable to replay attacks. And hence works as an additional security.

EXISTING SYSTEM

The authentication systems nowadays use the following methods for generating an OTP.

1. Time-based one-time password (TOTP)[6] is a temporary passcode. The algorithm that generates each password uses the current time of day as one of its factors to generate OTP, ensuring that each password is unique. The attacker cannot gain access without the TOTP, which changes every 30 or 60 seconds.
2. HMAC-based One-time Password (HOTP)[7] algorithm relies on two basic things: a shared secret and a moving factor (i.e. counter). Each newly generated OTP is derived from older OTPs by repeated application of hash chain algorithm.
3. In challenge-response authentication[8], challenge is made by posing a question by the Administrator and the Client has to authenticate herself by responding i.e. providing a valid answer. The response sent by the Client is compared with a pre-calculated value. The Client is granted access if the values match with each other.

Disadvantages of Existing Systems

1. OTPs are vulnerable to phishing attacks where an intruder may trick user to reveal her confidential information by posing himself as a trusted entity.
2. For TOTP to work, the clock of the user's device and the server needs to be roughly synchronized[9]. And hence if the clock is asynchronized or if the battery of the clock dies then it is a disadvantage to the user. Also intruder can attempt to guess the OTP since it is timestamp-based.
3. Attacker can bypass hash based OTPs by gaining old OTPs using social engineering techniques.
4. Dictionary attack is possible by the eavesdrop (e.g., derived from a password).

PROPOSED SYSTEM

Our proposed approach is based on Shamir's secret sharing scheme using Lagrange's basis polynomial and Lagrange's interpolation technique. There are three entities in the system: the Client who requests for a file, Administrator is the owner of the secured data, and an Authenticator who is responsible for performing authentication of the Client. Encryption of files and storing them on multiple databases is done by Administrator. These files are stored on multiple databases to increase the reliability of the system. The Client asks for these files from the Administrator. In order to check the authenticity of the Client, the Administrator asks the Authenticator to perform authentication on Client. The Authenticator performs authentication by generating a polynomial using Lagrange's basis polynomial technique. The secret points are generated and are sent to the Client. These points are then deleted from the system but the polynomial is retained. The Client is needed to send back *k* points out of the *n* points to the Authenticator. The Authenticator then constructs the polynomial from the received points and matches the secret part of the polynomial. If it matches then the Authenticator signals the Administrator about the authenticity of the Client. And the Administrator then sends the requested file to the Client.

Procedure

Algorithm 1: Proposed Security Scheme

Let *f* be the sensitive file and *k* be the threshold value:

1. Administrator encrypts *f* using 3 different keys (by applying blowfish algorithm) and stores them on 3 different databases.
2. When the Client requests for file *f*, the Administrator provides the details such as client-id and email address of the Client to the Authenticator and asks the Authenticator to perform authentication of that Client.
3. The Authenticator will generate a polynomial, construct *n* points from it, mail the values to the Client and delete the values but retain the polynomial's zero-degree coefficient. This value is the secret.
4. The Client has to mail back *k* values to the Authenticator.
5. Authenticator will reconstruct the polynomial using those *k* values. If the secret of the reconstructed polynomial matches then only Authenticator signals the administrator that the Client is authentic.
6. The Administrator then mails *f* along with the decryption key to the Client

Blowfish

Blowfish[2] is a 64-bit symmetric block cipher with variable length key. The algorithm operates with two parts: a key expansion part and a data encryption part. The role of key expansion is to convert a key of at most 448 bits into several sub keys arrays totaling 4168 bytes. The data encryption occurs via a 16-round *Fiestel* network.

Blowfish uses four 32-bit S-Boxes with 256 entries each. It uses P-array which consists of 18 32-bit sub keys.

Blowfish uses four 32-bit S-Boxes with 256 entries each. It uses P-array which consists of 18 32-bit sub keys.

Comparison of Encryption Algorithms

Blowfish algorithm is being used for encryption of files owing to its following advantages over Advanced Encryption Scheme (AES)[2].

While comparing both algorithms on the basis of computational time in seconds it is found that blowfish takes 0.86 s whereas AES takes 1.26 s for encryption and decryption of 64 bit data.

The CPU processing time for blowfish is 0.07 s whereas for AES it is 1.54 s.

Mathematical Explanation

The scheme basically consists of two algorithms:[10]

1. Secret Generation Algorithm
   Secret *S* is didvided into pieces by picking a random degree polynomial $q(x)=a_0+a_1x+a_2x^2+\ldots+a_{n-1}x^{n-1}$ in which $a_0=S$ and represent each share as a point $(x_i, q(x_i)=y_i)$.
2. Secret Reconstruction Algorithm
   For any t shares *(si1,…, sik)*
   Where *(i1,…..,it) {1,2,…..,n},* the secret s can be reconstructed.
   Thus the basic requirement of the secret sharing scheme is
   - With the knowledge of any *t* or more than *t* shares, share holders can reconstruct the secret
   - With the knowledge of any *t-1* or fewer than *t-1* shares, shareholders cannot reconstruct the secret S

   The Shamir secret sharing algorithm show that how to divide the key *k* in *n* pieces in such a way that *k* is reproduced from *p* pieces but even a complete knowledge of *p-1* pieces gives absolutely no information about the key *k*. This secret sharing scheme basically works by the concept of Lagrange's interpolation. The concept of Lagrange's interpolation is finding out missing data with all other data present.

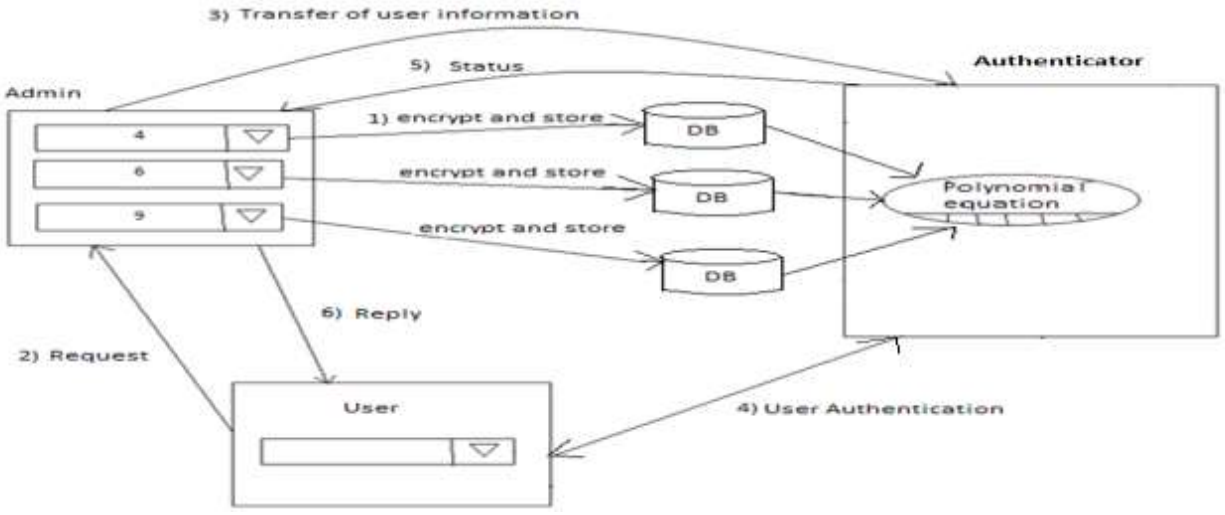

Figure 1. Basic Flow

Scope of the Proposed System

The software system basically authenticates a client. The authentication responsibility is given to Authenticator so that Administrator can perform different tasks apart from Client verification. Basically Administrator is a non-technical user and so he does not know details of authentication mechanism. This is taken care by the Authenticator. Administrator can login to the system, encrypt and store files on database, browse the file that needs to be sent to the Client. The proposed system can be used by bank managers to authenticate a client requesting for online transaction.

CONCLUSION

In this paper, we propose a secret sharing based concept to generate secure tokens or OTP which can be used to authenticate a user asking for highly sensitive data. The data is encrypted and stored on multiple databases which provide confidentiality and reliability of the system. We can also increase the degree of polynomial to make the secret tougher to crack. We can also make use of multi-cloud system for file storage.

ACKNOWLEDGEMENTS

We wish to express our profound gratitude to our principal Dr. V.C.Kotak for allowing us to go ahead with this project and giving us the opportunity to explore this domain. We would also like to thank our Head of Department Prof.Mr.Uday Bhave for our constant encouragement and support towards achieving this goal.

We take this opportunity to express our profound gratitude and deep regards to our guide Prof.Mrs.Vidyullata Devmane and our co-guide Prof.Mrs.Vaishali Hirlekar for their exemplary guidance, monitoring and constant encouragement for project completion and paper publication.

REFERENCES

1. Behrouz A. Forouzan, "Introduction," in *Cryptography & Network Security*, Edition 2007, New York: McGraw Hill Companies, pp. 9-10
2. Chaitali Haldankar, Sonia Kuwelkar, "Implementation of AES and Blowfish algorithm," in *International Journal of Research in Engineering and Technology*, vol. 03, issue 03, pp 143-146, May-2014
3. Todorka ALEXANDROVA et al., "Secret images sharing scheme using two-variable one-way functions," in *IEEE*, pp. 553-557, 2010
4. Esam Elsheh, A. Ben Hamza, "Secret sharing of 3D models using Blakley scheme," in *IEEE*, pp.92-95, 2010
5. A. Shamir, "How to Share a Secret," in *Communications of ACM*, pp 612–613, New York, USA, November 1979
6. Margaret Rouse. (2016, March 26). *time-based one-time password(TOTP)* [Online] Available: http://searchsecurity.techtarget.com/definition/time-based-one-time-password-TOTP
7. Peter Major. (2016, March 26). *One-Time Passwords - HOTP and TOTP* [Online] Available: http://blogs.forgerock.org/petermajor/2014/02/one-time-passwords-hotp-and-totp
8. https://en.wikipedia.org/wiki/Challenge%E2%80%93response_authentication
9. https://en.wikipedia.org/wiki/Time-based_One-time_Password_Algorithm
10. A. Amuthan, B. Aravind Baradwaj, "Secure routing scheme in MANETs using secret key sharing," in *International Journal of Computer Applications*, vol 22, no.1, pp. 38-43, May 2011

ISSN 2277-3061
Volume 15 Number6
International journal of Computers and Technology

Author' biography with Photo

Shipra Choudhary is pursuing BE in Computer Engineering from Shah and Anchor Kutchhi Engineering College, University of Mumbai

Apeksha Katarni is pursuing BE in Computer Engineering from Shah and Anchor Kutchhi Engineering College, University of Mumbai.

Shweta Manjrekar is pursuing BE in Computer Engineering from Shah and Anchor Kutchhi Engineering College, University of Mumbai.

Vidyullata Devmane is an Assistant Professor in Computer Engineering department in Shah And Anchor Kutchhi Engineering College. She has 15 years of teaching experince. She is currently pursuing her Ph.D.

Vaishali Hirlekar has done Masters in Computer Engineer. She is currently working as as Assistant Professor in Shah And Anchor Kutchhi Engineering College and has 4 years of working experience.