Volume : 3 | Issue : 6 | June 2014 • ISSN No 2277 - 8179

Research Paper

A Secured and Robust Distributed Data Storage in Multi Proxy Server Using Certificate Authority

Engineering

KEYWORDS : IBSDDS, Certificate manager, Biometrics;

Prasanna Regmi

Department of Computer Science and Engineering Saveetha School Of Engineering, Saveetha University, Chennai(INDIA)

ABSTRACT

External proxy servers stores the user data that is enabled by the data storage system to reduce the maintenance cost and to enhance the access and availability. For the security purpose, it is mandatory for the file owners to encrypt their files and outsourcing to proxy server. The owner of the respective file first encrypts his files and send the cipher texts to the proxy servers. Then, the cipher text encrypted under the identity of the owner to that of the receiver is then transferred by the proxy servers.

I. INTRODUCTION

To manage the personal files of the user a mechanism called DAS is provided by the cloud. In DAS schemes, user can outsource the encrypted files to un trusted servers. Without knowing anything about the original files, the proxy servers can perform some functions on the outsourced cipher texts. users are especially concerned on the confidentiality, integrity and query of the outsourced files. As cloud is managed by an untrusted third party so that cloud computing is a lot more complicated than the local data storage systems.

Principles of Security—The CIA Model

The confidentiality, integrity, and availability (CIA) triad is a simple but widely applicable security model. All secure systems should be guided by these three key principles. A measurement tool is provided by the CIA for security implementations. It is applicable across the entire spectrum of security analysis—from access, to a user's Internet history to the security of encrypted data across the Internet.

- **Confidentiality** The unauthorized disclosure of sensitive information is prevented by Confidentiality. It is the ability to ensure that the necessary level of secrecy is enforced and that information is hidden from unauthorized users. confidentiality is the aspect of security most often attacked. To ensure the confidentiality of data transferred from one computer to another using cryptography and encryption method .

- **Integrity**

Integrity prevents unauthorized modification of data, systems, and information, thereby providing assurance of the accuracy of information and systems. If your data has integrity, you can be sure that it is an accurate and unchanged representation of the original secure information. A common type of a security attack is man-in-the-middle. In this type of attack, an intruder intercepts data in transfer and makes changes to it.

- **Availability**

Availability is the prevention of loss of access to resources and information to make sure that information is offered for use when it is needed. The information requested should be readily accessible to the authorized users at all times. DOSIS one of several types of security attacks that attempts to deny access to the appropriate user, often for the sake of disruption of service

DISTRIBUTED DATA STORAGE

To take advantage of the huge amount of data available the digital storage of data facilitates information retrieval, allows a new wave of services and web applications. Compared to the print world the challenges of preserving and sharing data stored on digital media are significant in which data "stored" on paper can still be read centuries later. A big challenge is there for defining the storage requirements for digital libraries. In this context, following scenarios:

- resource deficits may occur due to Prediction of storage requirements below real needs.
- Prediction of storage requirements turn out to be above real needs, resulting in expenditure and administration overhead for resources that end up not being used.

Information technology (IT) revolution has led to the digitization of various kinds of information.1 Digital libraries appear as one more step toward easy access to information spread through variety of media.

II. OVERVIEW

IBSDDS

Without checking the public key certificates a user's identity can be an arbitrary string and two parties can communicate with each other. The four entities PKG, the data owner, the proxy server and the receiver in an identity-based secure distributed data storage (IBSDDS) scheme. Users identities and issues is validated with the secret keys by the PKG.

An efficient IBSDDS scheme should provide the following properties.

1) Unidirectional.
2) Non-interactive.
3) Key optimal.
4) Collusion-safe.
5) Non-transitive.
6) File-based access.

To retrieve an exact file, this scheme constructs lots of request for every single file where access permissions is made by the owner, so it will create the burden of proxy server and rising the time delay for sharing the files from receiver to file owner. Secure distributed data storage can change the burden of maintaining a large number of files from the owner to proxy servers.

III. PROPOSED SYSTEM

To overcome the problem, we introduce two scheme, the first scheme is authorization for identity using X.509 Certificate, i.e. it makes the confidentiality and integrity of the outsourced data certificates and reduces the time delay for sharing the files and then checks the CRL for managing the revoked. The another scheme is Access Permission such as private and public. In public access retrieve files anywhere but in private access, cannot retrieve files without file owner permission. To propose a distributed proxy server for availability and reduce the time delay..

X.509 certificate

On July 3, 1988 X.509 was initially issued and in association with the X.500 standard. It assumes a strict hierarchical system of certificate authorities (CAs) to issue the certificates. With web of trust models, like PGP it is contrasted where anyone (not just special CAs) may sign and thus attest to the validity of others' key certificates. The flexibility is included in the Version 3 of X.509 to support other topologies like bridges and meshes.

An X.509 certificate is something that can be used

- To Verify a person's identity so you can be sure that the person really is who they say they are.
- To Send the person who owns the certificate encrypted data than only they will be able to decrypt and read.

A certification authority issues a certificate binding a public

key to a particular distinguished name in the X.500 tradition, or to an alternative name given such as an e-mail HYPERLINK "http://en.wikipedia.org/wiki/E-mail_address"addressor a DNS entry.

Structure of a certificate
In a formal language, the structure foreseen by the standards is expressed.

The structure of an X.509 v3 digital certificate is as follows:

- Version
- Serial Number
- Algorithm ID
- Issuer
- Validity
- Subject
- Subject Public Key Info
- Issuer Unique Identifier (optional)

To enable the identification of the subject X.509 certificates contain several required and optional attributes . You can obtain the following list of attributes in an X.509 certificate:

- Version number: The certificate version.
- Serial number: A unique identifier for the certificate.
- Signature algorithm ID: The algorithm used to create the digital signature.
- Issuer name: The name of the certificate issuer.
- Validity period: The period during which the certificate is valid.
- Subject name: The name of the subject represented by the certificate.
- Subject public key information: The public key algorithm.
- Issuer unique identifier: The identifier for the issuer.

BLOW FISH ALGORITHM
In 1993 Bruce Schneier designed Blowfish algorithm which is a symmetric-key block cipher and included in a large number of cipher suites and encryption products. Blowfish is a new secret-key block cipher of a variable-length,. It iterates a simple encryption function 16 times. Its main features are:

- Block cipher: 64-bit block.
- Variable key length: 32 bits to 488 bits.
- Much faster than IDEA and DES.
- Unpatented and royalty free.
- No license required.

The Blowfish Algorithm:

- Manipulates large blocks of data
- Has a 64-bit block size.
- Consists of a scalable key, from 32 bits to at least 256 bits.
- Employs pre-computable sub keys.
- Consists of a variable number of iterations.
- Uses sub keys that are a one-way hash of the key.
- Has no linear structures that reduce the complexity of exhaustive search.
- Uses simple design which is easy to understand.

Blowfish is designed to encrypt and decrypt blocks of 64-bits. Since it is an unlicensed, variable-length key encryption algorithm. The algorithm has been developed to be efficient, simple, fast, compact and secure. An eighteen 32-bit P-array and four S-boxes of 256 32-bit values is used by the algorithm that are created from the key, which can be up to 448-bits.

BIOMETRICS To prevent the identity being stolen, biometric data is usually encrypted when it's gathered. Here we will discuss on the back end, how biometric verification works. A software application is used to identify specific points of data as match points to convert the biometric input. An algorithm is implemented that is used to process the match points in the database that translates that information into a numeric value.

- Face: Analysis of facial characteristics.
- Fingerprint: Analysis of an individual's unique fingerprints.
- Hand geometry: Analysis of hand/finger shape and size.
- Retina: Analysis of capillary vessels situated at the back of the eye.
- Iris: Analysis of the coloured ring surrounded by the eye's pupil.
- Signature: Analysis the way in which person signs.
- Vein: Analysis of pattern of veins in the back.
- Voice: Analysis of the frequency, tone and pitch of a person's voice.

Biometrics will play a critical role in future computers, and especially in electronic commerce. A *fingerprint scanner may be included in future by the personal computers* where index finger could be placed..Based on your identity the computer would analyze the fingerprint to determine who you are and authorize different levels of access. To make electronic purchases access levels could include the ability to use credit card information.

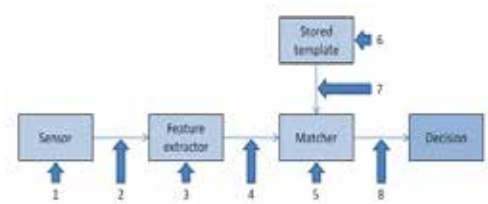

Fig.1 Flow Diagram of Biometrics
Fingerprint recognition, retinal and iris scanning, facial recognition, hand and finger geometry and DNA analysis may be included in Physiological techniques.

Handwriting recognition, voice or speech recognition, gait, and keystroke dynamics comes under Behavioral techniques.

the fundamental operational steps in all automated systems are:

1. Capture: To enter the biometric data into a database first it is captured and digitized.
2. Extraction: using the measurable unique data a template is created.
3. Comparison: A new sample. is compared with the template.
4. Match/Non-Match: Anew sample is matched by the existing template or may not be.

IV. CONCLUSION The user files is outsourced to un trusted proxy servers using distributed data storage schemes. To provide the security for a file the file owners encrypt their files and outsourcing to proxy server. The encrypted file is then transferred by the proxy server to the owner further to encrypt file for the receiver exclusive of the necessity of knowing the content of the original files. Then, using the new scheme the file owner registered their details and also apply the biometrics such as finger print,then get certificate from the certificate manager.

REFERENCE

1. Jinguang Han, Student Member, IEEE, Willy Susilo, Senior Member, IEEE, and Yi Mu, Senior Member, IEEE"Identity-Based Secure Distributed Data Storage Schemes". | 2. G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik(2008) "Scalable and efficient provable data possession," | 3. B. Blanchet and A. Chaudhuri,(2008) "Automatic formal analysis of a protocol for secure file sharing on untrusted storage," | 4. L. Bouganim and P. Pucheral(2002) "Chip-secured data access: Confidential data on untrusted servers" | 5. B. Carbunar and R. Sion(2012) "Toward private joins on outsourced data," IEEE Transactions on Knowlege and Data Engineering, vol. 9,no. 24, pp. 1699–1710. | 6. E.-J. Goh, H. Shacham, N. Modadugu, and D. Boneh(2003) "SiRiUS: Securin remote untrusted storage," in Proc. Network and Distributed System Security Symposium - NDSS'03, (San Diego, California, USA), pp. 1–15. | 7. H. Hacig¨um¨us, B. R. Iyer, C. Li, and S. Mehrotra(2002) "Executing SQL over encrypted data in the database-service-provider model,"in Proceedings: SIGMOD Conference - SIGMOD'0, vol. 2002,pp. 216–227. |