ISSN XXXX XXXX © 2017 IJESC

Research Article Volume 7 Issue No.6

Digitally Signing & Encrypting Database Record

Anjali[1], Prof. Ashish Vashisht[2]
M.Tech Student[1], Assistant Professor[2]
Department of Computer Science and Engineering
Kurukshetra Institute of Technology and Management, BhorSaidan, Kurukshetra, India

Abstract:
There are a lot of ways of securing any object of the file system or any complete database. But in today's scenario database is used on sharing basis means a number of users access the same database having different levels of security roles. So securing the whole database file from other users are not more concerned than securing one user's record in the same database from another user. We can grant access levels to different tables to different users but the problem is still there if multiple users work/shares the same table and enter their records or perform their routine tasks. We require a system that can secure our records by encrypting each row in the database for any particular users. So that a user can prove the accuracy of data, he/she must be able to verify the existence the actual copy of data with the data integrity. This article describes how a user can reproduce the validity of the data in the form of evidence if record got tempered in any possibly undetermined activities.

Keywords: Digital Signature**,** Data Signing**,** Security, Database, DB Signer

I. INTRODUCTION

In the present time, everything is kept in the file system in the database. The records maintenance system begins from our birth, Like birth registration system and keeps collecting all of our records at the different steps of our age. We go to school they keep creating our database there. We take admission in the college, sometimes school database transferred to a college or they may create their own database. At the age of 18, we want to have our driving licence again our records are captured and database system is created. Aadhar card is one of the most advanced databases of all the citizens of the India including their personal & biometric details. The Haryana govt. also going to conduct a survey very soon named "Jan Sewa survey" for creating SRDB (State residential database) to facilitate their citizen's different e-governance services. Hence a security mechanism is required to validate & authenticate the every record of the database.

II. PROJECT WORK

In this project, we have tried to combine the encryption technology with the digital signature of the owner of the data. We can also use other encryption technologies to encrypt and secure our records in the database but these encryption methods are common in use and they don't include ownership or data owner authentication. So we have created a mechanism in which we will read each and every record from the database row by row and then implement a hashing algorithm on that record and then restoring the encrypted result in a new column of the same row same database. We have used a digital signature of the owner of the data for creating the encrypted values of each row. so that the data is automatically authenticated by the creator or the owner. Many organisation already using the digital signature in their file system. DigiLocker is the best example where our certificates and other documents are kept and digitally signed. But we have used a digital signature in the records of the database rather than any document or file and with the digital signature, we have encrypted the row data. In our project work, ms SQL database has been used, as per the Aadhar act and IT act, storing and publishing Aadhar numbers and mobile numbers is a criminal activity so we are using dummy data in our project. we are using a land record data to test our application having some fields like nvcode, period, khewat, khatonithese fields contains only dummy data but this technology can be used with any type of records of any database.

III. LITERATURE SURVEY

Encryption is used to protect the confidentiality of information when it must reside or be transmitted through otherwise unsafe environments. Encryption is also used for "digital signatures" to authenticate the origin of messages or data. Encryption algorithms themselves are rarely used alone in practice. Rather, they are typically embedded into a larger security systems to ensure their correct and consistent use, since a failure to do can compromise the security of other messages, even those that have been properly encrypted.

Uses of Encryption

Encryption can be used in several different ways as summarized below. In addition to the characteristics of a particular encryption algorithm that are required to support a given use, the algorithm itself is generally integrated into a larger system that handles other aspects of the area to which encryption is being applied to ensure correct use and to minimize the visibility of the use of encryption. For example, if encryption is used for file protection, directories may also be protected and keys are managed on behalf of users so that normal file access does not change much.

Message Encryption

This is the traditional use of cryptography. Blocks of text are encrypted as units. This is the normal way in which email is encrypted.

Digital Signatures

Authenticating who sent a message is often useful. In the public key scheme, the secret decryption key can be used to

encrypt, allowing the non-secret encryption key to be used to decrypt. Since only the secret key holder is presumed to have the secret key, only he could have encrypted/signed the message. Anyone can check the digital signature by applying the non-secret key. Secret, signed messages can be obtained by digitally signing with your secret key, then encrypting using the recipient's non-secret key.

Stream Encryption

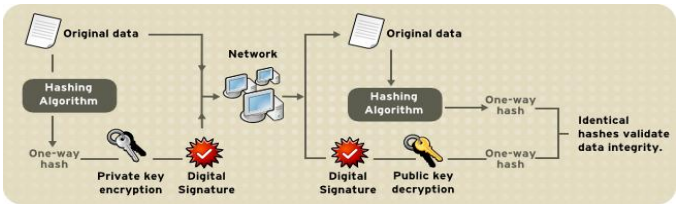
Some encryption schemes increase security by varying the key for separate packets of a long message. Often, the key is computed from previous packets. As long as all packets ultimately arrive, this works, but if packets are lost, subsequent packages are not decrypt able. Various synchronizations can be used to minimize the loss. This is particularly an issue for potential encryption of audio or video where the underlying transport will drop packets when load gets high.

File Encryption

Various encryption algorithms have been applied to files and databases. The main issue here is one of packaging the encryption naturally into normal file access and managing keys when a key may need to be used for a long time after it was originally used to encrypt.

IV. PROPOSED SYSTEM

No organisation wants security scars. That's why IT and Information Security departments generally do extensive due diligence on their cloud hosting and software providers to protect against data breaches, data loss, malware, viruses, phishing and other security threats. To help defend database, we've compiled an e-signature security checklist specifically for evaluating e-signature services. We purpose not only looking at the security of the service but also how signers are authenticated with the digital signature. In the proposed system a connection with the database established with the valid user credentials.



On successfully connecting with the database a log file is generated keeping track and records of all the activities being performed with the date and time of the event. The log file can be used to monitor the cause in the case of any exception or failure as this log file contains success & failure log of every activity.As part of this, verify whether you have the ability to search, find and playback a specific transaction's process audit trail for auditors or other business stakeholders, in just a few clicks.Another table is created in the database with some fields CertSrNo, Name, Issuer Name, Subject, Version, Public Key, Thumbprint, Signature Algorithm, Valid From, Valid Till keeping record of the digital certificate being used to encrypt the data.

User Authentication

E-Signature laws don't say much when it comes to security techniques and technology, but the legal definition of an electronic signature always includes language around signer identity. This means you need to:

Authenticate users prior to e-signing
Tie that authentication to the e-signature AND the e-signed record

Possibilities and characteristics of purposed system

A solution that supports multiple authentication methods, such as:

- Remote user authentication through user ID / password
- Email address verification through e-sign session invitation
- Remote user authentication through secret Q&A (a.k.a. challenge-response)
- Ability to leverage existing credentials
- Dynamic KBA through third-party databases (e.g. Equifax)
- Support for digital certificates
- Ability to upload images as part of an e-sign transaction, e.g. photo of a driver's license
- The ability to configure different authentication methods within the same transaction;
- Flexibility to adapt the authentication method(s) to the risk profile of your organization and EACH process being automated (e.g., customize the challenge-response questions and the number of questions based on your requirements);
- Flexible options for in-person signature attribution, including hand-off affidavits and SMS password (PIN) sent to a personal mobile device (verify whether user authentication via SMS is included free of charge).

After evaluating user authentication capabilities, the next step will be to verify that the e-signature service captures the authentication as part of the document audit trail and embeds the audit trail into the e-signed document.

Database& Signature Security

Creatingan e-signature solution that packages and secures the final e-signed database using a digital signature. The e-signature solution should apply the digital signature at two levels:

At the signature level to prevent tampering with the signature itself.
At the document level to prevent tampering with the document's contents.

Digital signature security ties together signing intent with the information that was agreed to at the time of signing. It also locks down and tamper proofs the e-signed document so unauthorized changes can't slip by unnoticed. While vendors like Docu Sign apply a digital signature as an envelope to a document (once all signatures have been captured), this is not a recommended practice. This approach leaves the document and signatures unprotected while the process is being completed and results in the wrong date and time stamp being place on individual signatures. If a signer and a co-signer e-sign a record on two separate days, you want that history reflected in the audit trail. The best practice is to apply digital signature encryption as each e-signature is added to the document. This builds a comprehensive audit trail with the date and time that each signature was applied.

What to look for:

- The document must be secured with a digital signature
- EACH signature must be secured with a digital signature
- A comprehensive audit trail should include the date and time of EACH signature
- The audit trail must be securely embedded in the document
- The audit trail must be linked to each signature
- Ability to verify the validity of the signed record offline, without going to a website
- One-click signature and document verification
- Ability to download a verifiable copy of the signed record with the audit trail
- The document must be accessible to all parties

V. RESULTS

Signing worked great in a perfect manner. Since its purpose is to ensure authenticity of data, its implementation involves calculating a unique hash based on its content, encrypting it with a private key, and including the result in the original document. Anyone with access to the public key can retrieve the hash and compare it to a result of its own calculations based on the same algorithm. Any discrepancies indicate that the original data has been modified. It is important to note that in every scenario involving asymmetric keys, effectiveness of the protection they are supposed to provide depends on the trust in credibility of an issuer of public keys. More specifically, those utilizing public keys need to trust that the corresponding private keys are in the hands of their rightful owner. Obviously, this raises a question about the basis of such trust, which is where digital certificates come into play.

VI. CONCLUSION

Encryption and signing constitute two most common practical applications of cryptography. Both of them leverage the concept of digital keys, which in essence are strings of characters generated by specially crafted algorithms. In general, keys can be divided into two categories, depending on whether they are intended to function independently or in related pairs, with one of them designated as public and the other as private. In the first case, a single key, known exclusively to its owner, operates in a symmetric manner, capable of handling both encryption and decryption. While this approach tends to be efficient from a performance standpoint, it introduces the challenge if encrypted data needs to be shared (since this requires an additional, secure method of transmitting the key). In the second case, one key (designated as private) remains in control of its owner, while the other (the public one) is readily available to anyone who requests it. Such mechanism is not only more versatile (due to its support for encryption as well as digital signatures), but also eliminates the challenge associated with its symmetric counterpart, since there is no need to transport the private key between the party encrypting data and its intended recipient. (Access to the private key is sufficient to decrypt any content protected with the corresponding public key). However, due to the inferior performance associated with this approach, it is very common to combine both methods, with data being encrypted using a symmetric key, which in turn is encrypted with a public key. On the receiving end, a holder of the private key applies it to retrieve the symmetric key, which subsequently is used to decrypt the original content.

VII. REFERENCES

[1].Goldreich, Oded (2001), Foundations of cryptography I: Basic Tools, Cambridge: Cambridge University Press, ISBN 978-0-511-54689-1

[2].Goldreich, Oded (2004), Foundations of cryptography II: Basic Applications (1. publ. ed.), Cambridge [u.a.]: Cambridge Univ. Press, ISBN 978-0-521-83084-3

[3].Pass, Rafael, A Course in Cryptography (PDF), retrieved 31 December 2015.

[4].J. Katz and Y. Lindell, "Introduction to Modern Cryptography" (Chapman & Hall/CRC Press, 2007)

[5].Stephen Mason, Electronic Signatures in Law (4th edition, Institute of Advanced Legal Studies for the SAS Digital Humanities Library, School of Advanced Study, University of London, 2016). ISBN 978-1-911507-00-0.

[6].Lorna Brazell, Electronic Signatures and Identities Law and Regulation (2nd edn, London: Sweet & Maxwell, 2008);

[7].Dennis Campbell, editor, E-Commerce and the Law of Digital Signatures (Oceana Publications, 2005).

[8].M. H. M Schellenkens, Electronic Signatures Authentication Technology from a Legal Perspective, (TMC Asser Press, 2004).

[9].Jeremiah S. Buckley, John P. Kromer, Margo H. K. Tank, and R. David Whitaker, The Law of Electronic Signatures (3rd Edition, West Publishing, 2010).