A Digital Signature Based on PKI To Authentication and Secure Exchanging data used in water boreholes intelligent Decision Support System

Introduction

Water scarcity is a crucial issue, particularly in regions like the Northern Sahara, where groundwater is a lifeline for drinking, irrigation, and industrial purposes. To achieve better exploitation, the authors suggest implementing a Decision Support System (DSS) to sustain the management of water boreholes in the southern part of the country. The data exchanged in their system is confidential and must be secured.

So, the authors introduced a digital signature system based on Public Key Infrastructure (PKI). The system is designed to secure the exchange of critical data within the DSS, ensuring the reliability and integrity of the information shared among users.

Related Works

In this Section, the authors investigated and shared with us what others have done in the realm of digital signatures and PKI. They discuss blockchain-based PKI frameworks, privacy-aware adaptations, and even a method involving QR codes for document authentication. They also discuss about the loopholes which current system have, and the space for hackers to intrude into digital signature and obtain the signed documents.

Proposed Approach

Based on a Digital Signature (DS)

They first briefed about what a DS is. And how it shows us the Integrity of the signed data with the identity of signer. They discuss about the algorithm which is used to create and confirm the signature. They also explained the working of algorithm.

The **M** message is introduced to a cryptographic **h** function resulting in a **hash value h** (message digest). Using the private key, signer **encrypts** the h value (producing so the signature).

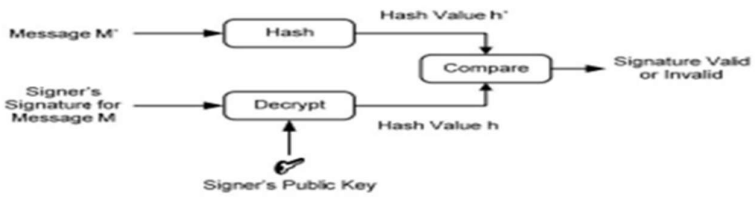


Fig. 2. A digital signature verification simplified process.

To check if the digital signature is valid, the h value of M is **compared** with the **signature's decryption value** using the public key (of the signer's).

If the two values are the **same**, the PK owner is the **message author**. **If not**, the signature is **not valid**.

Their approach for digitally signing the documents is described in two parts :

The signatory

- The value of the cryptographic hash of the data is calculated.
- This value is encrypted with its own private key (signature).
- The data, the signature, the identity of the signatory and the algorithms used are transmitted.

The receiver

- Receives D data and ES encrypted signature.
- Applies the cryptographic hash to D and finds H1.
- Retrieves the signer's public key from their identity.
- Uses it to decrypt the signature received ES and finds H2 – Compares H1 and H2 – The signature is valid if they are identical.

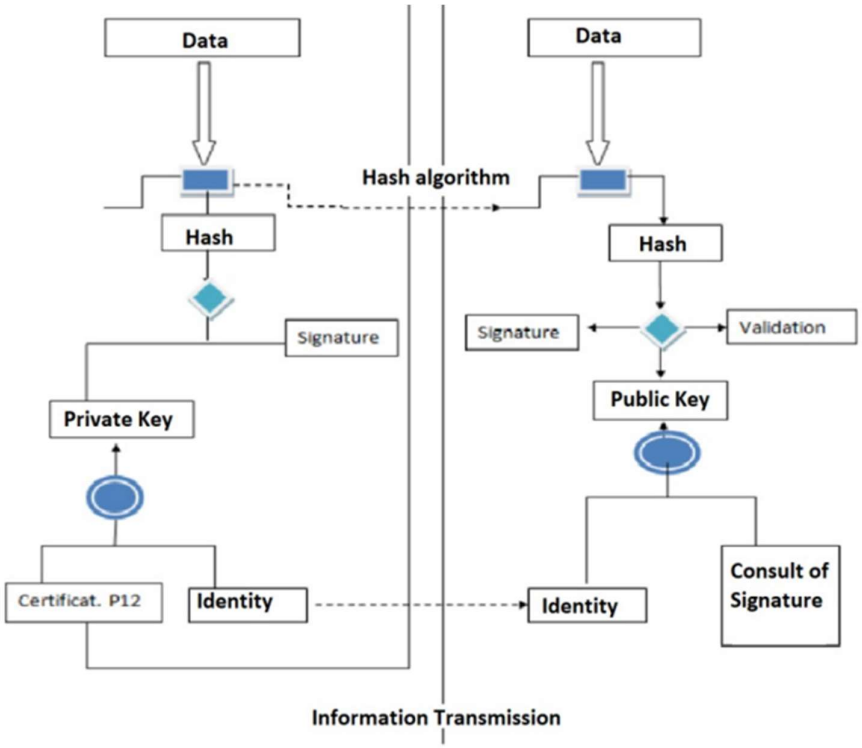


Fig. 3. Signature creation process.

Implementation of Proposed System

- To make it all work seamlessly, the team worked with **Java** language.
- For coding they chose **NetBeans IDE**.
- The team configured a **Linux server** using open **SSL** to serve as the backbone of their Public Key Infrastructure.
- For the **hash function**, they have used the **sha-256** algorithm to have the message digest of the data on our document.
- They used the **RSA** algorithm for the **encryption/decryption** with the private key/public key.
- They used **iText5**, an open-source library, to manipulate and create PDF documents.

Fig. 5. The certificate view.

Fig. 6. The document format Choose.

Fig. 7. Signing a PDF document interface.

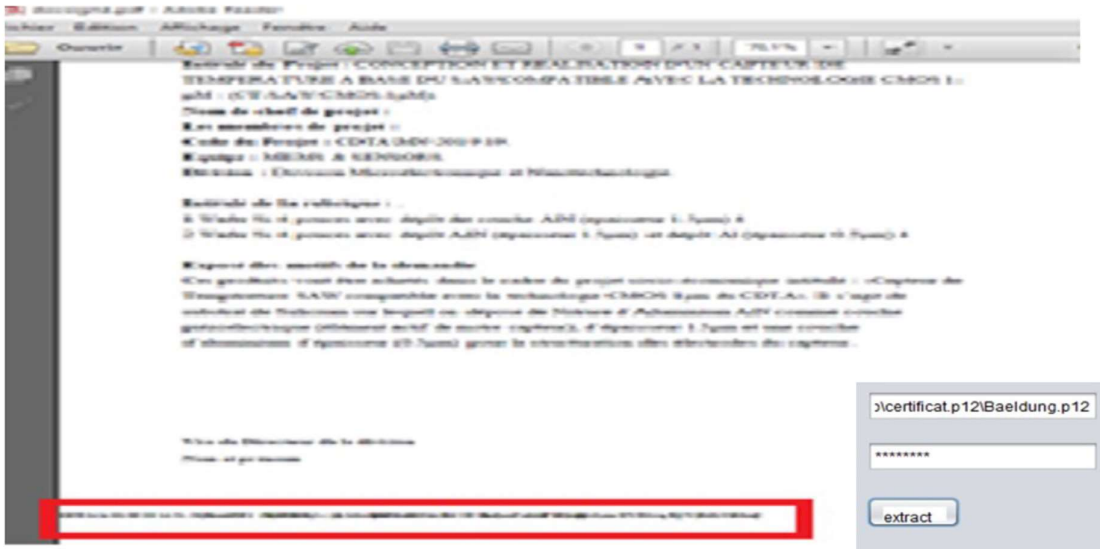


Fig. 8. The signed document.

Fig. 9. The public key extraction

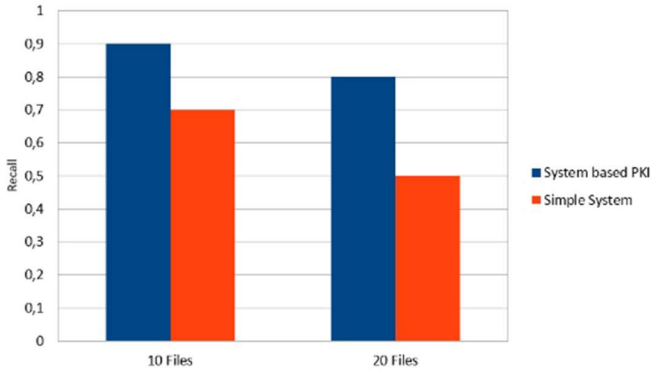
Fig. 10. The Signature verification.

Experimental Setup

- To test the approach, they made a comparison between a **system using the PKI signature** and another that uses **simple authentication methods**.
- To Evaluate, they used recall measure:

$$Recall = \frac{NumberOfAuthorizedAccessSignedKPI}{FilesNumberOfSignedPKIFiles}$$

- The goal here is that, the system should **only present relevant signed KPI documents to authorized users** during database queries.



- This model for secure information transfer consisted of following **quality aspects**:

  - **Safe Usage**
  - **Content Integrity**
  - **Confidentiality**
  - **Authentication of Sender & Receiver.**

Conclusion and Future Work

This paper proposes a digital signature system designed to secure data exchange within the Decision Support System (DSS). Building on a previous project, the signature system emphasizes simplicity for users. The use of modern tools, including PKI, Java, and Linux, contributes to extend system security. The future plan involves transforming the application into multiple applets for integration into various application workflows. Performance of the algorithm signature can be increased to create the signatures on a smart card directly.