International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 12 | Dec -2016 www.irjet.net p-ISSN: 2395-0072

Authenticated Document Transfer based on Digital Signature and a Survey of its existing techniques

Aishwarya Mali[1], Chinmay Mahalle[2], Mihir Kulkarni[3], Tejas Nangude[4], Prof. Geeta Navale[5],

[1] *Student, Department of Computer Engineering, Sinhgad Institute of Technology and Science, Maharashtra, India*
[2] *Student, Department of Computer Engineering, Sinhgad Institute of Technology and Science, Maharashtra, India*
[3] *Student, Department of Computer Engineering, Sinhgad Institute of Technology and Science, Maharashtra, India*
[4] *Student, Department of Computer Engineering, Sinhgad Institute of Technology and Science, Maharashtra, India*
[5] *Professor, Department of Computer Engineering, Sinhgad Institute of Technology and Science, Maharashtra, India*

Abstract - *With the use of mobile devices as a client for Internet, the threat of unauthorized and unauthenticated access of crucial documents is increasing day by day. Although Digital Signature is meant to be the solution for the unauthenticated access, its implementation is not adequate till now. Symmetric Data Transfer mechanism is used for the transfer of significant documents, but there is need of a more competent mechanism for safe transfer, authentication as well as verification of the documents. In this paper, we contemplate Asymmetric Data Transfer mechanism for the transfer of documents on Smartphones. But Asymmetric Cryptographic algorithms require complex computations and consume lot of power for execution. Hence a new technique is suggested in the paper, which is merely based on the concept of Asymmetric Cryptography but is feasible for smartphones. The paper also presents some research about the pre-existing techniques for implementation of Digital Signature technology.*

Key Words: **Digital Signature, Asymmetric Cryptography, smartphones, authentication, verification.**

1.INTRODUCTION

Smartphones are being used on a vast scale now-a-days. Many routine activities depend on it, making it an integral part of human life. It might store/use lot of confidential information such as pictures, passwords, call logs, messages, etc. of the user. This information becomes highly vulnerable; if at all smartphone is stolen or borrowed. Vulnerability may also increase when sending document over internet using smartphones.

Some documents might be highly confidential and hence require a high level of security while their transmission, because of the threat of intrusion. This can be achieved using the technique of Cryptography. Basically Cryptography is the art of writing and solving codes. It is the method of encoding the content of a message, so that it can only be read by the person to whom it is intended to be sent. Cryptography thus ensures Data Integrity. Another scenario observed on account of intrusion follows, wherein the document sent is different than the document received. In such a case, the intruder intrudes the original document and sends another document to the receiver; receiver being completely unaware of the situation and assuming that the document is sent by the sender only. Here authentication of document by the sender becomes of utmost importance and that can be efficiently achieved by the use of Digital Signature. Digital signature is a code which is generated by Public Key Encryption and is used to authenticate and verify the document sent over a network. If a digitally signed document is sent over Internet, then the sent and the received document both conform authenticity.

Today Digital Signatures are being used in different forms. Some use the actual signature of a person signed by him/her on the screen of a gadget which may be a touch screen phone/tablet/ipad and detect it using image processing techniques. This isn't a very reliable process as handmade signature may slightly differ from each other and result in forbidden access. Also another way is carrying a small USB-like device containing our Digital Signature and connecting the device to system to embed the signature. The limitation for this is that we have to be dependent on the device for digitally signing any document and carry it always. If the device itself is stolen or misplaced, we might land up in trouble. Moreover, the device is expensive. The most secure way for implementation of Digital Signature considered on this date is Biometric signatures. But again, all the smartphones are not provided with Biometric security systems; rather not all the users use smartphones with Biometric security provisions. So we need to find a way which is cost effective, accurate, highly secured and applicable to almost all the smartphones.

This paper briefs various approaches provided till date for implementation of Digital Signature and their advantages [2]. The problems related to these techniques (disadvantages/limitations) have been identified and enlisted [3]. With an aim to resolve the existing issues, a system has been proposed [4] and its advantages as well as limitations have been mentioned [5]. The final summary of the topic in concern is formulated [6] and future scope has been emphasized[7].

2. STATE OF THE ART

In today's competing business world, in which enterprises must extend their business environments over the Web for consumers, employees, and partners, digital security plays a vital role in building trust and credibility. [1] highlights a Digital Signature architecture that provides browser-agnostic, client-side signature components and generic server-side signature validation components to help integrate signatures into Web applications. The approach proposed here is Java-*Based Digital Signature architecture for Web-apps*.

The highlights of this architecture are –
- Feature-rich support for handling signatures.
- Built-in standardized API support for dealing with multiple private key stores in either the software or hardware.
- Built-in support for a standardized XML digital signature API and commercial and open source PKCS#7/CMS libraries.
- Ready support for certification path validations using OCSP and CRL.

The advantages of the technique provided in [1] are –
- **Configuration Repository:** The configuration repository is a centralized store for all configuration parameters and is the key component for a centralized, parameter-driven architecture.
- **Certificate and CRL repository:** This component is mainly responsible for organized storage of certificates and CRLs, which are required for successful certificate status validation.
- **Secure Private Key Storage:** This component abstracts the details of underlying private key storage and format. It provides a rational interface to access and manage private keys securely for signing.

With Internet and mobile devices becoming the basic amenities of livelihood, there is a dire need for maintaining privacy. [2] enlightens the necessity by integrating the Digital Signature schemes with the mobile applications which we access on regular basis, such as to play games, receive emails, purchase books, etc. The approach proposed here is named as *Server based Signature* (SBS), which happens to be very useful for mobile communication systems. Handheld devices have poor computational capabilities and short battery life. Traditional Digital Signature protocols based on Asymmetric Cryptographic Algorithms, although guarantee high level of security, but involve extensive computation. SBS claims to: 1. Reduce computation complexity on mobile devices, 2. Reduce communication consumption between signer and verifier and 3. Achieve same security level as that of traditional Digital Signature protocols. It uses *one-way collision resistant Hash function*, which means we can derive successive computations only when first computation is true. If first computation itself is false, successive computations can't be derived.

[2] encompasses –
- **Non-Repudiation of Sender (NRS) and Non-Repudiation of Receiver (NRR)** which implies the Sender and Receiver can't later deny having sent and received the message, respectively.
- **Repudiation Analysis** which explains the scenario when a Sender/Receiver would claim that they haven't sent/received a message even after sending/receiving. It contains the *CA (Certification Authority) Cheated* and *Sign Server Cheated* aspects. This analysis is entirely dependent on *one-way collision resistant Hash function.*
- **Security and Efficiency Analysis** which explains how forging of Digital Signature is prevented under SBS scheme. The entire SBS scheme is divided into 2 parts in terms of Efficiency, viz.: 1. *Computation cost* – that in turn includes *Sign server computation* and *User side computation* and 2. *Communication cost*.

SBS scheme provides a new perspective to Digital Signature Protocols; however the verification process follows the norms of Asymmetric Cryptographic Algorithm itself.

The advantages of the technique provided in [2] are –
- Reduces computation complexity on mobile devices.
- Reduces communication consumption between signer and verifier.
- Achieves same security level as that of traditional Digital Signature protocols.

With the increase in exchange of confidential documents over Internet, the risk of interception and manipulation by intruder also increases. [3] states that Digital signature can be proved to be one of the most efficient ways to secure the

document. Digital signature uses hash function along with Cryptography algorithm. Cryptography is classified into mainly two types: Symmetric cryptography and Asymmetric cryptography. Symmetric cryptography, also known as private key cryptography, involves only 1 lock and 1 key which are also to be traversed over internet followed by encrypted document. This increases the risk of the key itself to be sniffed and hence decrypting the document. Thus, asymmetric cryptography comes into picture. Here key is not shared over network, but instead contains 2 keys; a private key and a public key. There are many approaches and techniques used for designing cryptography algorithm. Some of the effective techniques are discussed in this paper.

The advantages of the technique provided in [3] are –

- **Speed**: By using DS business have not to wait for paper documents to be sent by any postal services. Contracts are written, completed, and signed by all concerned parties in a short period of time.
- **Costs**: Transmission over a network is cheaper than postal services. And if it is done by Digital Signature, it is much cheaper than others.
- **Security**: By using digital signatures and electronic documents amend the risks of documents being decoded, read, removed, or altered while in transmission.
- **Non-Repudiation**: Passing an electronic document digitally identifies you as the signatory and that cannot be later denied.
- **Imposter prevention**: Not a single person else can oven your digital signature or submit an electronic document incorrectly appealing it was sign up by you.
- **Time-Stamp**: With the help of time-stamping your digital signatures you will get the correct time when the documents is signed.
- **Authenticity**: Both paper stamp and digital stamp have same value of authenticity.

Currently people are more relied on the smartphone because of its user friendliness and ease of mobility. Smartphones now-a-days have become the basic need of an individual. People provide input like personal information, bank details, passwords etc. to various applications using smartphones. To secure the data in the mobile devices text-based passwords and graphical passwords are used; still the data in the device can't be guaranteed to be secure and it may be accessed by any unauthorized person. [4] aims to use the data streams generated by the log files based on the user's location, call log, message logs, etc. and verify whether the individual using the smart phone is an authenticated user or not. [4] employs a technique wherein the sensor based data stream generation is replaced by the log files which were previously generated automatically.

The advantages of the technique provided in [4] are –

- The traditional way of securing the data is rejected and new techniques of data security are presented.
- The verification of the user is done using the data stream generated based on the log files, so there is no need of explicitly embedding sensors to generate the data streams.
- Verification is done based on different aspects such as location, call logs (Call duration and individual called), message log (Messages sent and replied), indoor and outdoor mobility.
- The use of the explicit sensors is avoided so the battery life of the device will not get affected. The Power consumption of the SALCS based model is less than that of GPS based model.
- Cost effective technique of verification of the user is provided, maintaining integrity of data.

[5] proposes a Location based generation of Digital Signature approach on mobile devices, named as *The Geo-Encryption based GPS aided generation of Digital Signature scheme*. Geo-Encryption is a *GPS (Global Positioning System)* based encryption scheme that integrates the position and time into the encryption and decryption processes. It allows message to be encrypted for limited location and area. The message can be decrypted only when the recipient is physically positioned at the location as that of sender. A *Geo-Locking function* is employed during encryption process to combine the recipient's geographic location, time and an encryption key to produce *Geo-secured key* for transmission with the message. Geo-Lock function creates *Geo-Lock Value* by using *Position-Velocity-Time (PVT) to Geo-Lock mapping*. Geo-Lock value is used to generate Geo-Secured Key from *Session Key* and recover Session Key from Geo-Secured Key. Geo-encryption is effective only when the sender is aware of the receiver's location and the time at which receiver will be at that location.

The scheme [5] also uses a *Mobility Model for GPS-based Encryption*. It allows the mobile nodes to update movement parameters in the Sign server, thereby aiding the sender to geo-encrypt the receiver's estimated location and finally it presents methods for estimating the node's movement parameters. The *mobility parameters* include *'V' – average velocity of mobile device and 'ø'-direction in which mobile device is traveling*. *'ø' is measured as the positive angle between the positive X-axis*. Every time the mobile device

reads latitude and longitude from GPS reader to calculate V and ω, the mobile device has to determine whether or not to replace the old values of the parameter with the new values and then send them to Sign Server. The Updating process takes place only when the difference between old and new values of a parameter exceeds the threshold. Smaller the threshold value for the parameters, the more often parameters are updated.

The proposed scheme [5] is an extension to *Server based Signature (SBS)* scheme described in [2], hence it includes –
- Location based Analysis.
- Repudiation Analysis.
- Security Analysis.

The advantages of the technique provided in [5] are –
- Reduces computation complexity on mobile devices.
- Reduces communication consumption between signer and verifier.
- Achieves same security level as that of traditional Digital Signature protocols [5].

The main aim of [6] is to present reliable technique of authentication using Digital Signature so that users can authenticate the document at any time, at any place using various platforms. Platforms include laptop, desktop, web portals etc. This also includes the mobile devices which are palmtops, mobiles, tablet PCs. In this technique there is no need of explicitly using third party software for the authentication of the digital signature. [6] presents a Digital Signature technique in which the signature will not be stored on any server instead it will be regenerated whenever needed. This regeneration of the signature will be based on the JavaScript program, which will be downloaded in the backend when the key regeneration process is initiated.

The advantages of the technique provided in [6] are –
- Allows true mobility of the digital signature.
- Multi platform access and authentication of the digital signature is possible.
- The key for the access of digital signature is not stored on any server or device. It will be regenerated whenever required.

Huge amount of learning objects are available on Internet. User just has to access the learning object which is stored on the remote repositories using the network connectivity whenever required. Now a day there is a need of authentication and verification of the learning object uploaded on Internet. [7] aims to study different technique to verify the learning objects, whether it is uploaded by a trusted source or not. In this script the verification of the learning object is done using digital certificate. This digital certificate is authenticated using Digital Signature. The author uploads the learning object on the repository and also gives information about the learning object, requesting a digital certificate from the user.

The advantages of the technique provided in [7] are –
- Easy and efficient way of verification of the learning objects.
- The digital signature validates the learning objects.
- The link about the particular repository will give detail information about the author an also gives various objects.

3. PROBLEM IDENTIFIED

In [1] typically, there are multiple trusted certification authorities in a given business context, so it's critical to maintain a central repository of all related certificates and CRLs.

SBS scheme in [2] uses one-way collision resistant Hash function which is quite an old technique and at the same time ambiguous in its efficiency. Repudiation and Security Analysis depends upon the Hash function. So if hash function is mistakenly computed wrong, then the further analysis would be wrong. Verification process is kept the same as that of Asymmetric Cryptographic Algorithm. So if the authors claim that Asymmetric Cryptographic Algorithm is computation intensive and SBS reduces computation complexity, then by not changing the verification process they are contradicting their own claims.

Major problems identified in [3] are –
- **Expiry**: Digital signatures, are also like just other electronic media and we all know that each of them have a limited time. So it shows that DS is also come with its expiry.
- **Certificates**: Both sender and receiver must have to buy authorized certificates for the effective use of digital signature.
- **Software**: Sender and receiver both have to buy authorized software too, to make transmission smoother and easier.
- **Law**: In some states and countries, commandments regarding computer-generated and technology-based issues are weak or even non-existent. Exchange in such

jurisdictions becomes very risky for those who use digitally signed electronic documents.

- **Compatibility**: There are many compatibility issues are also found during the use of digital signature in different- different platform.
- The generation process and verification process of digital signature needs **substantial quantity** of time. So, for regular exchange of communications the speed of communication will decrease.
- If a user changes his private key after every fixed break of period, then the **record** of all these changes **must be reserved**. If an argument arises over a previously sent message then the old key pair needs to be referred. Thus loading of all the preceding keys is another overhead.

In [4] SALCS based verification technique does not involve data streams generated by sensors. It is not as effective as the traditional GPS model. Previously generated datasets are needed to be stored in record for verification hence leading to memory wastage.

The Geo-Encryption based GPS aided generation of Digital Signature scheme [5] uses one-way collision resistant Hash function which is quite an old technique and at the same time ambiguous in its efficiency. Repudiation and Security Analysis depends upon the Hash function. So if hash function is mistakenly computed wrong, then the further analysis would be wrong. The *biggest disadvantage* of this method is that a Sender can communicate with a Receiver only if the Receiver is in the location premises of the Sender. The Threshold value for Location parameters must be kept small to optimize the update process.

The technique proposed in [6] is vulnerable to man-in-the-browser attacks, unless significant care is taken in the data entry at the platform. The JavaScript downloaded from the company server may learn the secret sentence while executing in an user's browser. If the JavaScript is malicious, then the company could obtain that value and subsequently compute user's private key itself and forge her signatures. The proposed scheme cannot protect against an user telling someone else her secret sentence or perhaps choosing one that is easily guessed.

The work in [7] has the following limitations –

- The approach relies in the existing public key infrastructure of Costa Rica. To implement the proposed approach in a different country, it needs to have a similar infrastructure. If such requirement does not exist, it is possible to build an entity to create, manage and distribute digital certificates. The creation of that body will consume significant money and time.
- If the growth of persons with digital certificate slows, it is possible that many authors cannot sign their own learning objects.
- We trust the author when he/she claims the authorship and ownership of a learning object with his/her digital signature. It may happen that a dishonest author signs a learning object that does not belong to him/her. Plagiarism detection and the enforcement of intellectual property are beyond the scope of this paper.

4. PROPOSED SYSTEM

The system proposed in this paper emphasizes on the use of Digital Signatures based on the concept of Asymmetric Cryptography. It is to be noted here that we are employing the basic concept behind Asymmetric Cryptography and not implementing any of the algorithms that implements this logic. Here we aim at developing a standalone system that allows a user (either from technical or nontechnical background) to authenticate his important documents of any specific use, using Digital Signature of his own choice and then transfer it securely over the network to the intended person.

The flow of the system is as follows –

1. The users are required to register themselves on a mobile portal, providing their basic information like name, mobile number, email id, username and password. They also need to specify the pattern of the digital signature they want to adopt.
2. All this information will be stored in the database and digital signature specifically will be stored in encrypted form.
3. Whenever a user wants to send any document, he/she simply needs to import the document from mobile storage and attach his/her digital signature to it and then send it to the intended recipient.
4. The document transfer takes place through email.
5. The locking-unlocking process (encryption-decryption) takes place automatically at the backend.
6. Finally the intended recipient receives the document with only 1 notification and acknowledgement is sent back to the sender.

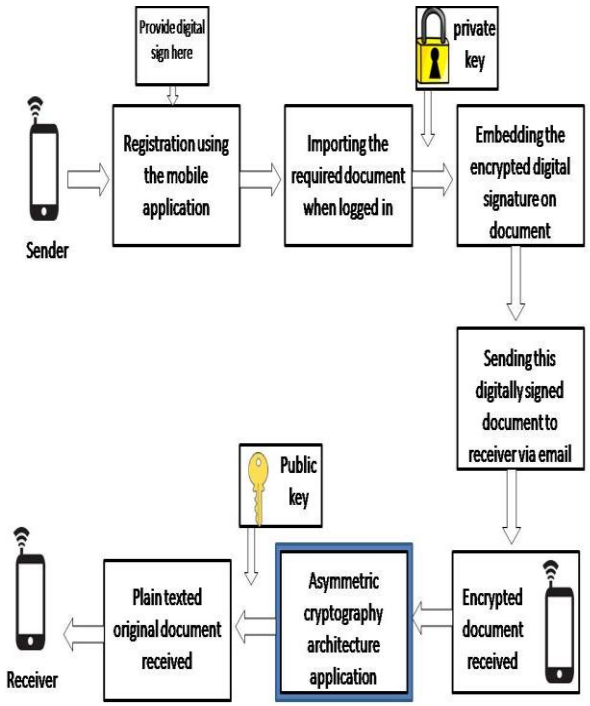

Figure 5.1: System Architecture

Generally Asymmetric Cryptography is implemented as follows –

Suppose Alice and Bob want to communicate with each other.

1. Alice and Bob send their respective public keys to each other.
2. Alice then encrypts some message using Bob's public key and sends it over the network.
3. Bob receives the message sent by Alice and to have access to it, decrypts it using his own private.
4. If Bob wants to send some message to Alice, then same procedure is repeated.

But the system in consideration proposes a different perspective of Asymmetric cryptographic algorithm. It can be graphically depicted as follows –

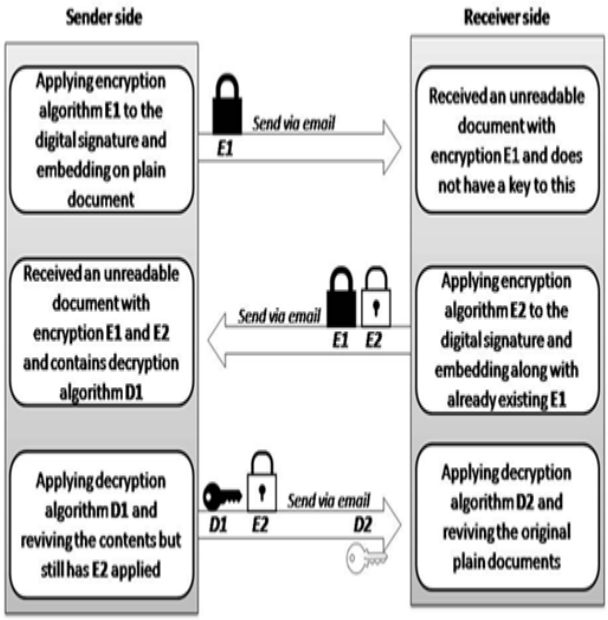

Figure 5.2 : Asymmetric Cryptography Architecture

Again consider that Alice and Bob converse with each other but now applying the approach depicted in Fig. 5.2.

1. Alice encrypts the message using her public key (say E1) and sends it over the network to Bob.
2. Bob receives the message but cannot access it, since it is encrypted with Alice's public key. Bob too encrypts the received message with his public key (E2). At this point the message is double encrypted by Alice as well as Bob's public key. The message is then sent back to Alice.
3. When Alice receives the message she decrypts it using her private key (say D1), since the data has her public key encryption. She can access the data although it is encrypted by Bob's public key. The message is transmitted to Bob again.
4. When Bob receives the message, it has only single encryption and that is Bob's public key encryption. Hence Bob can decrypt it using his private key (say D2) and have access to the message.

5. ADVANTAGES AND CONSTRAINTS OF THE PROPOSED SYSTEM

The advantages of the proposed system can be summarized as follows –

- The overall process of attaching Digital Signature to document and transferring it over the network to the intended recipient, is made very handy by the use of smart phones.

- The overall level of information security and data integrity is increased.
- Users can authenticate their documents by attaching Digital Signature to them at anytime from any place, by the use of database.
- The system achieves Information security, Data Integrity, Authenticity and Usability by all means.

The proposed system has following 2 constraints although –

- Documents to be transferred need to be stored in mobile storage compulsorily.
- Large amount of, but light-weight computation required in the overall process.

6. CONCLUSION

This paper summarises different aspects of Digital Signature and how it has been implemented in the real world. The aim is to present in abstract about how Digital Signature can be implemented in mobile devices by referring the current techniques and their shortcomings. An Asymmetric Cryptography concept based technique for secure and authenticated transfer of documents over network is also proposed. An attempt has been made to provide an effective and secure solution to eliminate traditional practices, thereby making use of Digital Signature handy and mobile.

7. FUTURE SCOPE

As the use of the internet is increasing day by day, there is a need of Data Authentication and Verification. Digital Signature is one of the solution for these problems. This paper has presented a technique to make digital signature handy and easy to use. Proposed solution is smartphone based that makes the Digital Signature portable. Android platform is used here, which is open source and hence there is huge scope of improvement and advancement. Asymmetric Encryption technique is proposed for the encryption of the Digital Signature which gives a very secure way to verify the authenticity of the data. Also it is very cost efficient technique for the authenticity and verification of data. There is no need of using any explicit device to access a digital signature only the mobile is required which is connected to the network.

ACKNOWLEDGEMENT

This research was supported by **Graphikera Technologies**. We thank Mr. Husain Basrawala, Chief Technology Officer, Graphikera technologies, for all the support throughout the research. Also we would like to express our sincere gratitude towards Prof. Geeta S. Navale, Head of Department, Computer Engineering, Sinhgad Institute of Technology and Science for guiding, assisting and providing her valuable suggestions to us from time to time; that has greatly helped to improve the manuscript.

REFERENCES

[1] Harigopal K.B. Ponnapalli and Ashutosh Saxena, “A Digital Signature Architecture for Web Apps”, Infosys, India, March/April 2013.

[2] Yeu Lei, Deren chen, Zhongding Jiang, “Generating Digital Signature on mobile devices”, 18th International Conference on Advanced Information Networking and Application, 2004.

[3] Shivendra singh, Md. Sarfaraz iqbal, Arunima Jaiswal, “Survey on Techniques Developed using Digital Signature: Public key Cryptography”, International Journal of Computer Applications (0975 – 8887) Volume 117 – No. 16, May 2015.

[4] Senaka Buthpitiya, Anind K. Dey, Martin Griss, “Soft Authentication with Low-Cost Signatures”, 2014 IEEE conference on pervasive computing and communications.

[5] Santi Jarusombat and Surin Kittitornkun, “Digital Signature on Mobile Devices based on Location”, 2014 IEEE Conference.

[6] Carlisle Adams and Guy-Vincent Jourdan, “Digital Signatures for Mobile Users”, 2014 IEEE Conference, Toronto, Canada.

[7] Alpizar-Chacon, Mario Chacon-Rivas, “Authenticity and versioning of learning objects using the digital signature infrastructure of Costa Rica”, 2014.