ISSN:0975-9646

ASMF: Attribute Signature Management Framework for Digital Document Security and Integrity

Deepika Pawar, Prof. Mahendra K. Verma

Department of Computer Science & Engineering
Sushila Devi Bansal College of Technology, Indore (M.P) -453331, India

***Abstract*— Data security and protection is the major factor towards gaining the complete control over the system. It deals with the necessary factors required to offer the robust protection levels towards accessing the authorized data. Authentication and cryptosystems are few of such approaches which deal with user's identity verification and data confidentiality. When the identity and correctness of data travelling through open medium is demanded then hashing is applied due to its one way property. It detects the unauthorized changes and modification performed during transmissions. Well known implementation area of hashing is digital signatures which deal with the documents originality and creators identity. It is modified with adding additional information related to the attributes of users and comes under attribute based signatures (ABS). We have made in depth analysis of some previous approaches offering the ABS phenomenon and found some of the unsolved issues solution to which reduces the complexity, consumption and overhead associated with signature generations and verification. This paper proposes a novel attribute signature management framework (ASMF) for handling the process of digital signatures with attributes and its predicate logic. The solution contains the versatile primitives to allow the signing parties having complete controls over the signature generation and the fine grained access security controls. It has a predicate logic attested with message and hides the signatures privacy. After analyzing the approach analytically some of the benefits were found which can be further verified by the implementation solution over the suggested framework in near future.**

***Keywords*— Data Security, Digital Signature, RSA, MD5, Certificate X.509, Attribute Signature Management Framework (ASMF), Computational Complexity, Resource Consumption, Overhead;**

I. INTRODUCTION

Cryptosystem deals with data security and protection which were designed in temporary fashion where the attacked systems are handled. All the developed models are mathematical strong to handle the unauthorized access and changes tried by the attackers. This mathematical problem is computational hard and the complexity of system needs to be assumed which was in traceable and used as a major building block for security system. Cryptosystems are further pared into symmetric and asymmetric nature depends on the key used. Some of the examples of such cryptosystems are DES, AES and RSA. Here the RSA approach is a public key cryptosystem. The tools developed with these cryptosystems are offering through random oracles for proving the security of a scheme. A random oracle is an oracle that when queried responds with a random reply, subject to the condition that the reply is different for various queries but the same when the same input is queried again. Such an oracle has the desired properties such as preimage resistance and collision resistance. Signatures have existed as a means of authentication for ages. It takes different formats according to the application. Until that point signing a document meant identifying the person. Signatures have been very useful in creating certified documents, but it has generally been necessary to rely on external evidence that the persons signing the document are qualified to do so. This is today's challenge. In the early days of digital signatures, signers owned a pair of keys, a public key known to everyone used as an input for the verification process and a private key known by the signer and used in the signature process. Then the scheme is proved secure under that random oracle assumption. Finally when it comes to actually implementing the scheme the random oracle is replaced with a strong hash function. Researchers believe that proving a cryptosystem secure under the random oracle is equivalent to proving the security of the scheme dependent on exploiting the hash function used. Research in Attribute based signatures followed a certain trend.

Cryptographers would identify an application that requires attribute signatures where that application would require certain properties that no existing cryptosystem provides. They would propose a totally new scheme with new security notions that serve such properties. The result was several schemes each serving a very specific application making it hard to employ in any other. The following are two examples of such schemes:

(i) **Anonymous Credentials:** Such systems have users and organizations. Organizations know the users by their pseudonyms and they issue credentials to these pseudonyms. Users, anonymously, can prove possession of a credential even to organizations that know them with a different pseudonym while unforgeability of credentials is guaranteed.

(ii) Attribute based signatures: A system that is very similar in concept with anonymous credentials, however, it can mix more than one attribute in one query (i.e. signature). Designing a scheme for a specific purpose lead to overlooking common problems. One of the most challenging problems is revocation and finding a standard infrastructure.

Understanding Digital Signature

If a user wants to send a signed document to another user, public key is used to identify the users and it was known to everyone and the secret key is not known. Using the secret key and a message, first user can create a signature and send it to another. The recipient user can verify the signature using the message and the public key. The signature contains several elements that look random to recipient. Among these elements is one which is referred to as a "Fingerprint". Second user (Recipient) knows the verifying procedure which will enable him to make use of the public key and the signature in order to recalculate the "Fingerprint". If what he calculated is equivalent to what he got from first user (Sender) then accept signature otherwise reject it. A Digital Signature Scheme is a set of algorithms. To define the scheme we explain the algorithms.

- **Setup (k):** This algorithm creates two keys using a security parameter k. The first is the public key P_k known to all and the second is a secret key S_k given to the signer only.
- **Sign (M, S_k):** This algorithm is run by the signer (first user). He signs the message M using a secret key S_k and outputs a signature "Sig".
- **Verify (Sig, P_k, M):** This algorithm is run by the verifier (Recipient). He uses and the public key P_k to run the verification algorithm that will output either accept or reject.

Attribute-Based Signature (ABS)

A digital signature is the mathematical construction scheme for generating the authenticity information for verifying the digital documents or identity of users. A signature based document will prove that it was created and transmitted without any modifications and having proper privileges assigned to the sender. It uses the attributes from the set of user's information instead of any single feature for showing the signers identity. A valid ABS is the signature which verifies the message content, its predicate and users identity associated with it. It highlights the word single in this familiar security guarantee ABS signatures, as in most attribute-based systems, require that colluding parties not be able to pool their attributes together. Furthermore, attribute signatures do not reveal more than the claim being made regarding the attributes, even in the presence of other signatures. An attribute-based signature assures the verifier that a signer, whose set of attributes satisfies a (possibly) complex predicate, has endorsed the message. It is further divided into three types:

- **Group Signatures**

Group signatures are digital signatures that allow any member of a group to sign anonymously on behalf of the group and in case of a dispute, a trusted group manager can revoke that anonymity. Important concern to a group signature scheme is a group manager, who is responsible of adding group members and has the ability to disclose the original signer in the occurrence of ambiguity. In several systems the tasks of adding members and canceling signature secrecy are separated and given to a membership manager and cancelation manager respectively.

- **Ring Signatures**

A ring signature is similar in concept with group signatures but differs in three key ways. First of all, there is no way to revoke the anonymity of an individual signature (i.e. no one can tell the signer of a message not even the group manager). The next distinction is other group of users can be considered as a group without additional setup. The last distinction is that every user has a public and private key. The way ring signatures work is by having a member choose any set of possible signers that includes him-self, and he signs a message by using his secret key and the others" public keys, without getting their approval or assistance. It is used as a structural block of several cryptosystems. Technically, ring signatures can be viewed as a witness-indistinguishable disjoint of regular signatures, but because of this, only signer who have previously published a confirmation key are suitable to be enrolled in such a group. Ring signatures can thus only ever associate users who, by the act of publishing their key, are declaring their approval.

- **Mesh Signatures**

The idea can be considered as an addition to ring signatures, but with added modularity and a much comfortable primitives for expressing signer ambiguity. Intuitively, mesh signatures (as in ring signatures) need to be anonymous and unforgeable. The access structure can be satisfied using different combinations of atomic signatures, once created the mesh signature will not release what particular subset was used. The atomic signatures may be "static" and repeatedly usable, as different to new. Hence PKI Certificates are suitable even if the mesh signer not have the trust authorities signing key. A mesh signature is a non-interactive witness identical proof that some decentralized Boolean expression is true, where each input of that expression is labeled with a key and message pair and is true only if the mesh signer is in ownership of a valid signature on the stated message under the stated key.

Properties of ABS

An ABS scheme allows a verifier to decide on the set of attributes (s) he would like the signer to possess. The verifier sends the request to a group of possible signers as a monotone Boolean expression. Any member with sufficient attributes can sign. The scheme maintains certain properties as follows:

- **No previous knowledge assumption:** The signer and verifier may or may not have met before; therefore we cannot rely on any kind of previous knowledge.
- **Unforgeable:** It is hard to forge signatures and/or the proof of possession of attributes.
- **Anonymous Identities:** Given the signature it is hard to identify the signer.
- **Unlinkable:** Given two signatures it is hard to know whether the signer is the same or not.
- **Traceable:** Each group of potential signers has a group manager and he is the only one capable of revoking anonymity and discovering the signer's identity. This property is meant to ensure signers do not misuse anonymity.

- **Anonymous Attributes:** The attribute disclosure should be to the minimum.
- **Coalition Resistant:** If a verifier requires more than one attribute from the signers, the signers should not be able to get together their individual attributes and sign as one entity.
- **Separability:** The tasks of different authorities should be separable and each entity should be capable of performing its task independently from others.

II. RELATED STUDY

During the last few years the security of digital document is considered as major issues. Its protection is implemented using digital signature. We have gone through a variety of signature algorithms and attribute based signature is one of its recent approach. Here with this literature review we put a light on various existing approaches and their functional behavior to develop a better approach.

In the paper [6] attribute based cryptography is discussed for getting the fine grained access control. It holds and verifies the secret information associated with the digital documents. Also a great use of attribute based signature is shows here to develop the practical solution satisfying the predicate conditions. The problem associated with the authentication and anonymity in distributed access control system, dealing with resources consumption is very much important. The detected size of signature generated by existing ABS schemes grows linearly with the number of attributes used for forming a signing predicate. The paper also proposes the first two attribute-based signature schemes with constant size signatures. Their security is proven in the selective-predicate and adaptive-message setting, in the standard model, under chosen message attacks, with respect to some algorithmic assumptions related to bilinear groups.

Some of the paper shows the evolution of ABS based on the size of signature and the predicate logics as mentioned in the paper [7]. The length of signature mostly depends on the largest attribute which can be predicted by some attackers. Thus the paper proposes an attribute-based signature scheme with uniform size irrespective of the nature of attribute size. This scheme is unforgeable conditionally depends on the success probability of any polynomial time adversaries. It is proved to be unforgeable and unconditionally anonymous in the standard model. The security of our schemes has been proven under the standard computational Diffie-Hellman assumption.

In the paper [8] cryptographic methods are studied against the system scalability factors, access control and other key generation activities. Mainly it applies the attribute based encryption for performing the storage over cloud servers. The approach of ABE is further divided in KP-ABE and CP-ABE. For preserving the security and data protection CP-ABE is more appropriate. To implement this the CP-ABE is applied to the data by service providers on the documents uploaded by the users. For implementing the signature approaches the ABE is converted to attribute based Signature (ABS) schemes. The paper also discusses the variants of ABS like Ring ABS, Group ABS and Mesh ABS. Thus, ABS proves to verify that the signer holds a subset of attributes satisfying that signing policy. It can be efficiently used in real scenarios like data sharing in cloud computing for certification and confidentiality with satisfying signing policies.

The paper [9] further works on specific elements of ABS implementation using designated signature verifier entity. The paper proposes a threshold attribute based signature verifier scheme and works as an effective model for assuring the identity of the sender. The scheme named as t-ABUDVS scheme consists of the following algorithms: t-ABUDVS= (Setup, Extract, PS, PV, DS, DV, Sim).The security of suggested scheme will be reduced to the hard problem in which the signature is constructed. The paper also put lights on the definition of the bilinear Diffie-Hellman problem.

The paper [10] presents a novel attribute-based signature scheme for recovering the corrupted or lost messages. While comparing the scheme with traditional approaches, this ABS scheme with message recovery is not having any requirements regarding the retransmission of the original copy of message for verifying the signatures validity because of its nature by which the original message recovery from signature is prevented. The scheme also reduces the total length of the original message with appended signature. The paper deals with its three contributions i.e. attribute-based signature with message recovery, bilinear pairing construction and signature applicability for larger sized messages. It also support exible threshold predicates and are proven to be existentially unforgeable against adaptively chosen message attacks in the random oracle model under the assumption that the Computational Die-Hellman problem is hard.

In the paper [11] a new ABS technique based on the IRMA attribute-based authentication is proposed for healthcare industry. The proposed scheme of IRMA has an smart card based effective and practical implementation prototypes working successfully. The paper extends the existing functionality along with new implementation of ABS for IRMA devices. It also give a study on practical issues that arise due to the introduction of the signature functionality to an existing attribute-based authentication scheme, and we propose possible cryptographic and infrastructural solutions. For implementing the solution the paper gives a design evaluation using its use cases analysis.

While discussing the ABS most of the authors claims to deals with unforgeability which deals with signing key. A user can only be able to put its signature if he is having a complete control of its key and policy. It is having different entities like signature authority, verifier, users, receiver. The work is made clear for applying the signature on group of users with leaking secrets and is having expressive predicate. It applies the policy of perfect privacy anonymity for hiding the users and its signature identity. Some of its extended variants are Traceable ABS (TABS), Decentralized TABS [12]. The work is also presented with practical implementation and efficient construction of suggested approach. It also prevents the expressiveness of designed policies with static assumption.

III. PROBLEM DEFINITION

Internet technology is changing very rapidly with evolutionary architecture on which the webs that are achieving the practical realities. The Internet of Things (IoT) [13] is one of such area which deals with the concept of day to day electronic devices monitoring device, sensors, and home appliances accessing the internet for their effective use. It works towards transforming the devices to smart working objects which was flexible in nature and analyses process which was there with the internet. As the technology is going the requirement of security is also generating the demanding situations. Existing security primitives is not applied directly on IoT due to their segregated and heterogeneous standards and communication stacks. Moreover, the high number of interconnected devices arises scalability issues; therefore a exible infrastructure is needed able to deal with security threats in such a dynamic environment [14].

While the signature is one of such process which is necessary to assure the users identity and its document confidentiality. Considering the attribute based signature (ABS) schemes, after analyzing the approaches and the material we have found some of the current issues which needs to be resolved for implementing an more robust security controls over IoT. These are:

(i) High computational cost related to the signature process and which is directly proportional to the predicate formula which will not work for hand held devices. In some cases the signature predicate formula is smaller but the document confidentiality is more thus here the security is compromised with existing scheme [15]. Thus to reduce overhead is the primary task with this work.

(ii) Some of the approaches will generate the variable sized signature but the signature for the user will be same sized and it depends on the attributes. Thus the signature must be designed in such a way which will generate the constant sized signatures to reduce the overhead and its associated complexity.

(iii) The existing schemes sometimes expose the key, this must be improved to gain more robustness against the unforgeability and attribute signature privacy issues. This can be handled by introducing the random function for key generation and handling using key exchange mechanism.

After analyzing the problems with existing mechanism a new attribute based signature (ABS) is required with better construction privacy, lesser computational cost and reduced signature size with same or higher protection levels.

IV. PROPOSED WORK

Attribute Based Signature (ABS) offers the benefits to the user by passing the selected attributes from set of attributes for generating the signature with higher strength. It offers the phenomenon of anonymity for serving the privacy of user's identity and the signature. Here the key revocation is associated with attribute generation which will improve the performance of ABS. But it was a challenging situation for the signature verifier because he doesn't know the users selection towards its attributes and hence the verification process is not directly applied here. This paper proposes a novel attribute signature management framework (ASMF) which deals with all the above mentioned problems along with its efficient implementation. It shows an improvement over the key revocation using a designated authority for dealing with users selected attributes. The designed authority works as interacting medium between the verifier and the user and applies a negotiation of attributes. For generating the signature the user ask the intermediate for its secret key share along with a revocation check for its identity and the desired attributes. Here the key exchanges are handled using the RSA algorithms.

The process starts with forming a users group interested in making the digital signature based documents. All the users are having different set of properties associated with their identities and system usages habits. We called them as attributes. These attributes are extracted from the users and stored to attribute store. Later on the data fragment passed by the user on which the signature has to be attached are passed to the hash generation modules which is having an MD5 digest algorithm working in parallel with the signature predicate logic module. It contains the additional information about the users in the form of their attribute passed for documents identity verification in the form of signature. The hash algorithm calculates the digest using this predicate logic. Now the RSA cryptosystem is used for encrypting the generated digest using the signer's private key. This private key will proves the authenticity of users along with its attributes. After applying the encryption X.509 certificate is added to hold the authentication information of users. This authentication information verifies by authentication server as identity check. All the temporary data generated by the system is stored with signature in the data repository. It is used to recreate the signature if repeat demands generated by the user for other document. It also holds the predicate logic decided for signature generation. Now the signed message of document is transmitted over the open channel.

Now the second phase of proposed ASMF framework is for verification process. This phase starts with extraction of digest associated with the data fragments. Before extraction we need t decrypt the digest using signer's private key maintained with the public key register. Once the digest is decrypted then the associated hash with the data is extracted and the original data is passed again for recalculating the hash using MD5 algorithm. The recalculated hash the compared with the extracted hash along with the users attributes verification. If the attributes are matched with the users identity associated stored then the validity of the signature and the sender is confirmed. Finally the message is made available to the receiver with its proof mentioned with the certificate.

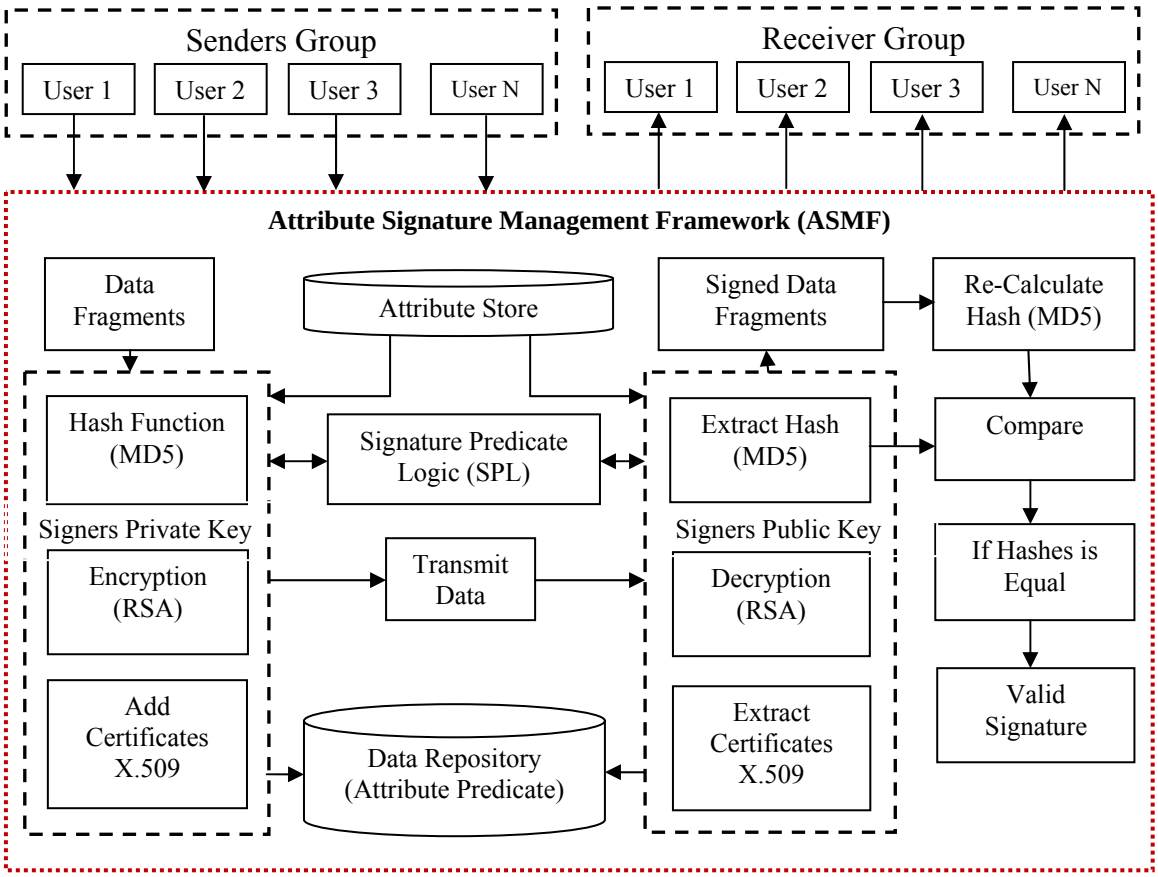

Figure 1: Proposed Framework for Attribute Signature based Management.

Components Needs to be developed

(i) Attribute Extractor
(ii) Signature Predicate Logic Generator
(iii) MD5 Hash Algorithm
(iv) RSA Cryptosystems
(v) Certificate Manager
(vi) Hash Matching
(vii) Messaging System

Thus with the help of the above components and their designed functionality the complete attribute based signature mechanism can be achieved. Apart from that we are also focusing on caparison of suggested approach with traditional mechanism. Thus some computation overhead, resource consumption and complexity measurements module is also required for proving the effectiveness of proposed approach.

V. BENEFITS OF WORK

- Our technique provides a feasible way to realize the "piecewise key generation.
- To allow for high efficiency and flexibility.
- Small number of exponential computations is enough for user signing.
- Less Complexity
- Efficient Data Outsourcing.
- Computational Cost is low.
- Better performance in server end, so that the data outsourcing becomes easier in data transferring communities.

VI. CONCLUSION

Data security depends upon the handling mechanism used to exchange the information between different ends. For verifying the authenticity of digital documents we need to verify the senders and the document both after receiving it. The file deals with it Is digital signature. Providing the user with more facility towards the data security and a assurance a new field is working with exiting mechanism known as attribute based signature. We had made a study on various attribute based signature mechanism and analyze their working capabilities to detect some of the unsolved issues. Mainly the computational complexity associated with these algorithms is very high and the types of resources they are consuming is also high. Thus a new approach is required to solve the issues. In this paper we propose a novel attribute signature management framework (ASMF) to overcome these issues. At the analytical level of evaluation we are getting the effective outcomes which could be latter verified by its prototypic implementation developed in near future.

REFERENCE

[1] Digital signing of original reports, By ALS Laboratories, Version 1 Published in 2010

[2] James H. Davenport and Dalia Khader, "Digital signatures: What you are versus \Who you are", in IACR Technical Review, 2010.

[3] S Sharmila Deva Selvi, Subhashini Venugopalan and C. Pandu Rangan, "A New Approach to Threshold Attribute Based Signatures", in Theoretical Computer Science Laboratory Department of Computer Science and Engineering Indian Institute of Technology, Madras, 2010.

[4] Hemanta K. Maji, Manoj Prabhakaran and Mike Rosulek, Attribute-Based Signatures", in Department of Computer Science, University of Illinois, Urbana-Champaign, 2010.

[5] Piyi Yang , Tanveer A. Zia , Zhenfu Cao and Xiaolei Dong , "Efficient and expressive fully secure attribute-based signature in the standard model", Australian Information Security Management Conference, Edith Cowan University, Dec 2011.

[6] Javier Herranz, Fabien Laguillaumie, Benoit Libert and Carla Rafols, "Short Attribute-Based Signatures for Threshold Predicates", in RSA Conference, San Francisco, United States, Springer, 2012.

[7] Fugeng ZENG, Chunxiang XU, Qinyi LI and Xiujie ZHANG, "Attribute-based Signature Scheme with Constant Size Signature", in Journal of Computational Information Systems, ISSN: 2875–2882, Vol 8, Issue 7, 2012.

[8] Rupesh Vaishnav, "Attribute Based Signature Scheme For Attribute Based Encrypted Data In Cloud", in International Journal of Engineering Research & Technology (IJERT),ISSN: 2278-0181, Vol. 1 Issue 10, Dec 2012

[9] Feng Cai, Wangmei Guo and Ximeng Liu,"Threshold attribute based universal designated verifier signature scheme in the standard model", in WSEAS Transaction on Communications, ISSN: 2224-2864, Vol. 13, 2012.

[10] Kefeng Wang, Yi Mu and Fuchun Guo, "Attribute-based signature with message recovery", in Research Online Lecture Notes in Computer Science, University of Wollongong, 2014.

[11] Brinda Hampiholi, Gergely Alpaar, Fabian van den Broek, and Bart Jacobs, Towards Practical Attribute-Based Signatures"", in Institute for Computing and Information Sciences, Radboud University, Nijmegen, The Netherlands, 2015

[12] Essam Ghadafi, "Decentralised Traceable Attribute Based Encryption", Presentation in University College London, April 2015

[13] Nigel Mc Kelvey , Kevin Curran and Nadarajah Subaginy , "The Internet of Things", in IGI Global Journals, Category of Mobile and Wireless Computing, DOI: 10.4018/978-1-4666-5888-2.ch570, 2005

[14] S. Sicari, A. Rizzardi, L.A. Grieco and A. Coen-Porisini, "Security, Privacy & Trust in Internet of Things:the road ahead", in Preprint submitted to Elsevier, Feb 2015.

[15] Xiaofeng Chen, Jin Li, Xinyi Huang, Jingwei Li and Yang Xiang, Secure Outsourced Attribute-Based Signatures"", in IEEE Transaction on Parallel and Distributed Systems, ISSN: 1045-9219, VOL. 25, NO. 12, Dec 2014.