A Unified Hybrid ID-based And Certificate based Cryptosystem For Information Security

Varun Pandey
Computer Science and Engineering (Information Security)
Disha Institute Of Management And Technology
Raipur, India

Prof. Preeti Tuli
Computer Science and Engineering (Information Security)
Disha Institute Of Management And Technology
Raipur, India

Abstract— cryptography encompasses techniques for secure communication over unsecure networks vulnerable from adversaries. The ID-based and certificate based cryptographic schemes are two of the most popular techniques in this field of information security. These schemes have been designed under different theoretical backgrounds and they have their own advantages and drawbacks . Certificate based cryptography and PKI is widely employed in the real world. It can provide explicit authentication of users, even in large scale groups with complex hierarchy. On the other hand ID-based cryptography is advantageous in key management, since key distribution and key revocation are not required, but they also have an inherent drawback of key escrow problem, i.e. users private keys are known to the key generation center (KGC).There have been few works which try to provide them together in an efficient way. A hybrid scheme comprising public key infrastructure (PKI) and ID-based encryption (IBE) can be taken under consideration for improved operational results. Combining both these schemes drastically eliminates problems faced by each scheme individually. Furthermore ,the concept of unified public key infrastructure (UPKI) in which both certificate-based and ID-based cryptosystems provided to users in a single framework increases the efficiency gain as end users do not need to manage other users' certificate. In this paper we proposed combination of cryptographic algorithms in different ways which will provide output with varied efficiencies. The output from one cryptographic system taken as input for the other or both the Id –based and certificate based systems presenting the single output as a combination.

Keywords— UPKI ,ID-based cryptography, Certificate based cryptography, KGC,IBE.

I. INTRODUCTION

General public key based cryptographic techniques have become common practice within network security and also authentication applications within the last decade. One of the most important reasons guiding this popularity will be the ease of key distribution in public places key cryptography. The public-private key pairs are created by the owner of the key plus the public keys could be known by every person. That characteristic involving public key systems makes the important thing distribution less difficult when compared with private key dependent systems. However, you can still find some public crucial distribution problems in public places key based programs. There are two sorts of problems regarding the public key distribution: (i) the media for the distribution, (ii) authentication of the public key owner . Your second problem related with the public key submission is more important compared to first one. Since the public-private key pairs are manufactured by the masters themselves, there should be a mechanism in order to introduce them since valid entities in order to other partners from the application.

A. *Certificate-based cryptography*

With certificate-based public essential cryptography, user's public essential generated by person is authenticated using a certificate issued by way of a certification authority (CA). A certificate can be a digital document brought in by CA which in turn binds a public key into a specific user. It provides explicit authentication from the public key in the sense that the authenticity from the public key is convinced to everyone by verifying the particular certificate. Any participant who would like to use other's public key must primary verify the corresponding certificate to check on the authenticity from the public key. Thus users must retrieve, verify, shop, and manage other's certificates that they're communicating with. It requires great deal of storage, communication along with computing to shop, verify, and revoke certificates. A (digital) certificate can be a signature by a reliable certificate authority (CA) of which securely binds with each other several quantities. Generally, these quantities include at least the name of a user U and its public key PK. Generally, the CA has a serial number SN (to make simpler its management from the certificates), as well as the certificate's issue date D1 and conclusion date D2. By issuing SigCA(U, PK, SN, D1, D2), the CA essentially attests to it's belief that PK is (and will be) person U's authentic public key from your current date D1 for the future date D2. Since CAs cannot tell the long run, circumstances may demand a certificate to be revoked before it's intended expiration date. For example, when a user accidentally shows its secret essential or an enemy actively compromises that, the user per se may request revocation connected with its certificate. However, the user's business may request revocation should the user leaves the company or changes position which is no longer allowed use the essential. If a certification is revocable, then third parties cannot rely on that certificate unless the CA directs certificate status information indicating whether or not the certificate is presently valid. This certificate status information has to be fresh – e. g., to just a day. Moreover, it has to be widely distributed (to most relying parties). Distributing huge amounts of fresh certification information is the "certificate revocation problem. " Solving this challenge seems to require many infrastructure, and the apparent need for this infrastructure is normally cited as an excuse against widespread execution of public. The two main entities involved with CBE are a certifier and also a client. Explicit authentication of public key and Authenticating users throughout large scale are many of the potential advantages in this scheme whereas Users need to retrieve, verify, store, manage others certificate there're communicating that is a high overhead serving as a drawback of certificate based cryptography.

B. *ID-based cryptography*

Identity-based cryptography is a kind of public-key cryptography when a publicly known string representing a person or organization is needed as a public key. The public chain could include a contact address, domain identify, or a physical IP address. Throughout 1984, Shamir [1] proposed the ID-based cryptography which can greatly simplify crucial management. In ID-based cryptography a great entity’s public key comes directly from the public identity data, for example, identify, e-mail address, IP address of the user, etc. The corresponding private key of the user is generated by the trusted authority termed key generation heart (KGC) and fond of the user by using a secure channel. In comparison with certificate-based cryptography, ID-based cryptography is usually advantageous in crucial management, since distribution involving public key just isn't required. A sender can send an encrypted message into a receiver using the receiver’s public id information, even prior to receiver obtains his private key via KGC. If the signature is acquired, it can always be verified immediately by employing sender’s public id information. But an untouched problem of ID-based cryptography may be the key escrow problem, i. e., KGC knows user’s private crucial. Therefore, malicious KGC can decrypt cipher texts of the user and forge signatures while using the name of the person. It also has a secure channel concerning users and KGC to provide private keys firmly. Therefore, providing an escrow-free non-public key issuing mechanism is usually an important issue to create the ID-based cryptography more practical in real life. Because of most of these inherent problems ID-based cryptography was considered to be suitable only for communications in a very small organization whereby KGC is entirely trusted.

C. *Private Key Issuing in ID-based Cryptography*

With ID-based cryptography issuing private keys to be able to users in escrow-free way ended up an important concern. Recently, Lee et 's. [2], [3] proposed an original private key issuing protocol within the single-authority multiple-observer (SAMO) type, which is the 1st pioneering work that will reduce the id cost in multi-authority-based crucial issuing protocol. Within this approach a solitary key generation core (KGC) provides user identification and incomplete key issuing function and multiple crucial privacy agents (KPAs) offer key privacy support without additional user identification. This proposal reduced the identification cost from multiple identifications by simply multiple authorities to a single identification by simply KGC. But these plans have weaknesses because of the lack of authentication. of protocol messages. In these structure KGC first checks user’s identification and offers partial private crucial, then KPAs look at KGC’s user identification and gives key privacy service with virtually no further direct recognition of user. Since explicit authentication had not been employed in these types of schemes, it’s hard for KPAs acknowledge KGC’s identification result and also the overall scheme evolved into complicated.

D. *Combining Certificate-based and ID-based Schemes*

Traditionally certificate-based cryptography in addition to ID-based cryptography are already considered separately. Certificate based cryptography in addition to public key infrastructure (PKI) might be deployed to authenticate end users in large degree, hierarchical groups, while ID-based cryptosystem is usually used to authenticate users in a very closed, highly trustworthy group. In designing a non-public key issuing protocol in ID-based cryptography researchers in many literatures tried to exclude the employment of certificate due for the high overhead involving certificate based program. It looks quite reasonable using some sense, but if we take into account the case that PKI is already existent, adding ID-based cryptography to certificate-based cryptography just isn't a heavy weight. There have recently been several works which try to combine certificate-based in addition to ID-based systems. Chen et 's. [4] proposed some sort of hybrid scheme involving public key facilities (PKI) and ID-based encryption (IBE) program which merges standard PKI with identity-based encryption program. They suggested that this combination of a couple schemes, PKI for global name in addition to ID for community name, is beneficial and scalable. They further talked about various trust relationship between multiple authorities with this hybrid system. Value et al. [5] considered the issue of interoperation between entities in typical PKI and organisations in ID-based facilities. These schemes deemed interoperation between a couple systems, but they've not discussed far more in-depth implementation issues of the combined system. In this paper we show that combining those two cryptosystems in a single framework is feasible with small extra load and contains many advantages. This work can be considered as an productive implementation example of the concept of [4], [5].

E. *Motivation of Unified Public Key Infrastructure*

A different critical problem of ID-based cryptography is that it must be not easy to implement hierarchy of trust. Gentry et al. [6] showed an example of hierarchical ID-based encryption, but it isn't flexible to suit to the real world requirements. Therefore, though we try and use ID-based cryptography for customers, it looks preferable to rely on document and PKI to create upper trust power structure. In this papers we introduce a new concept called specific public key infrastructure (UPKI) by which both certificate-based along with ID-based cryptography are given to users inside a highly combined fashion. Here we assume the existence of a trusted authority known as key generation along with certification authority (KGCA) that has the role of both CA along with KGC. It assessments identification information involving user and problems a certificate for any user-chosen public key X. It also problems ID-based partial private key towards user. We furthermore assume the everyday living of multiple KPAs like in [3] which provide key level of privacy service. In the proposed private key providing protocol user is usually authenticated with document and user's authorized public key X can be used to blind the protocol messages so that only the reputable user can access the ID-based personal key. This approach can solve the difficulties of both [2], [3] in addition to [4], [5]. We also show that when interactions between end users are mainly carried out using ID-based cryptography, then end users don't need to deal with other end users' vouchers, which is a great efficiency gain as compared to traditional PKI.

II. RELATED WORK

There have been lots of works to design private key issuing protocol for ID-based cryptography which does not have key escrow trouble. A straightforward strategy to the key escrow problem is usually to distribute the important issuing function in order to multiple authorities [7], [8]. Should the master key of your KGC is sent out to multiple authorities along with a private key is computed in the threshold manner [7], key escrow problem of your single KGC can be prevented. Generating a brand new private key by having up multiple private keys [8] will be another approach. Even so, these approaches involves high identification price tag, because each authority must identify the very same user independently just before key issuing. Thinking about the high cost associated with user identification, sometimes requires offline interactions based on policy, multiple independent identifications for that same user simply by multiple authorities can be a big burden. Another way of solve the important escrow problem will be issuing user's private key with an interactive protocol in between user and KGC with a couple user-chosen secret data [9], [1]. Gentry [9] offered a certificate-based encryption (CBE) structure where private important is computed applying user-chosen secret data, but it grew to be a certificate-based scheme losing the benefit of ID-based cryptography. 's Riyami et al. [10] successfully removed the necessity of certificate (they named it certificateless general public key cryptography) in the similar design applying user-chosen secret data, but their structure provides only implicit authentication in the public key. The random-looking general public key generated because of the user is not certified in the slightest. Thus any participant who wants to use the general public key for the very first time cannot be convinced if thez public key indeed is one of the user. Recently, Lee et al. [2], [3] proposed an original private key issuing protocol from the single-authority multiple onlooker (SAMO) model, that's the first pioneering work which could reduce the identification cost in multi-authority centered key issuing project. In this approach 1 key generation middle (KGC) provides individual identification and incomplete key issuing function and multiple important privacy agents (KPAs) supply key privacy support without additional individual identification. This proposal decreased the identification price tag from multiple identifications simply by multiple authorities into a single identification simply by KGC. [2] seriously isn't efficient and not robust mainly because it uses serial important privacy service simply by multiple KPAs. [3] helps [2] in efficiency and robustness through the use of secret sharing among multiple KPAs and also threshold cryptography with key privacy support. But these schemes are subject to various attacks through malicious KGC and also attackers [11]. The primary reason of the weakness is that user isn't authenticated using standard way and the correctness of protocol can't be verified publicly.

III. PROBLEM IDENTIFICATION

Previous methodologies proposed a model that combines ID-based and certificate based cryptography schemes in a single framework which provides advantages of both these schemes. both schemes are integrated in a single framework but it cannot be declared as most efficient integration in all cryptographic parameters .This technique uses two algorithms combined together ,but there are several algorithms for both Id-based and certificate based cryptography. The various combinations of these algorithms give us different efficiency and effectiveness under different cryptographic parameters

IV. PROPOSED METHODOLOGY

This work considers combination of both the ID-based cryptosystem and Certificate based crypto system. Both the schemes have advantages and disadvantages of their own. This flaw can be sort out with the combined approach resulting in overcoming the drawbacks of both the cryptosystems when taken in combination.

A. An input message is passed through the ID-based cryptosystem and the resulting output is fed as the input to the Certificate based cryptosystem or vice-versa providing the final output.

B. A message is taken as input for Id-based cryptosystem and certificate based crypto system separately and the output of both the cryptosystems are combined together to produce the final output.

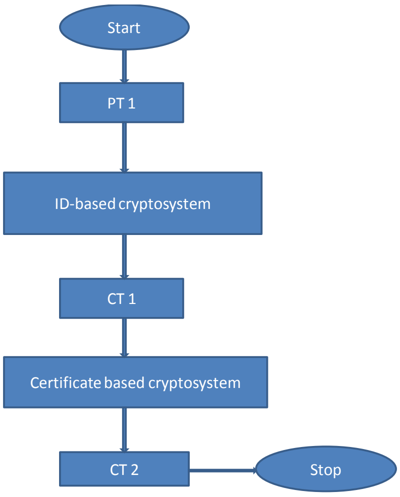

Figure : Serial cryptosystem

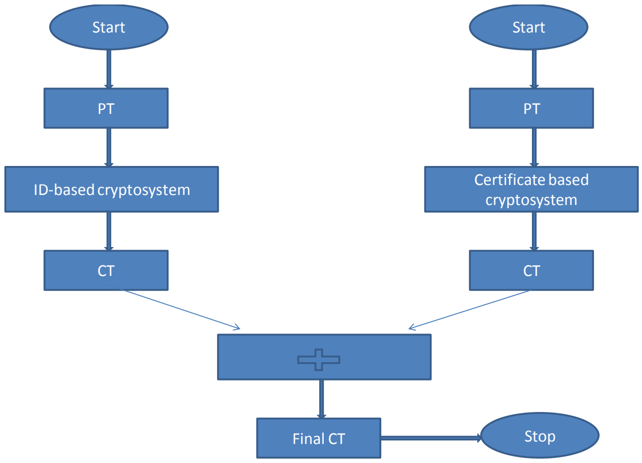

Figure : Parallely Combined Cryptosystem

V. CONCLUSION

In this paper we considered the advantages of both the Id-based and Certificate based cryptographic schemes.This paper proposed the several techniques we consider for different combinations of algorithms for both ID-based and certificate-based cryptographic schemes and check for the efficiency and effectiveness of each combination seperatly under various cryptographic parameters and give most efficient and effective combination of algorithmic technique.The unified Public Key infrastructure (UPKI) has been introduced that includes both ID-based and Certificate based cryptography together .Furthermore , if required than we will present modification in the work.

ACKNOWLEDGMENT

I am very much grateful to Department of CSE, DIMAT to give me opportunity to work on Location Privacy in Wireless Sensor Networks. I sincerely express my gratitude to Mrs. Preeti Tuli of Dept. of M.Tech CSE, DIMAT for giving constant inspiration for this work. I am also thankful to Prof. Somesh Dewangan, Dept. of CSE, DIMAT for helping me directly and indirectly during this work. I am really thankful to my all friends for their blessing and support.

REFERENCES

[1]. A. Shamir, “Identity based cryptosystems and signature schemes”, Advances in Cryptology - Crypto’84, LNCS 196, Springer-Verlag

[2].B. Lee, C. Boyd, E. Dawson, K. Kim, J. Yang and S. Yoo, “Secure Key Issuing in ID-Based Cryptography”, In ACSW Frontiers 2004 - Second Australasian Information Security Workshop (AISW2004), volume 26 of Australian Computer Science Communications,

[3].B. Lee, E. Dawson, S. Moon, “Efficient and Robust Secure Key Issuing Protocol in ID-based Cryptography”, Preproceedings of the 6-th International Workshop on Information Security Applications (WISA 2005)

[4].L. Chen, K. Harrison, A. Moss, D. Soldera, and N.P. Smart, “Certification of Public Keys within an Identity Based System, ”ISC 2002, LNCS 2433, Springer-Verlag

[5].G. Price and C. J. Mitchell, “Interoperation between a conventional PKI and an ID-based infrastructure,”EuroPKI 2005, Canterbury, UK, June 30 – July 1, 2005. Revised Selected Papers, Springer-Verlag, LNCS 3545

[6].C. Gentry, A. Silverberg, “Hierarchical ID-Based Cryptography”, Asiacrypt 2002, LNCS 2501, Springer-Verlag

[7]. D. Boneh, and M. Franklin, “Identity-based encryption from the Weil pairing”, Advances in Cryptology – Crypto 2001, LNCS 2139, Springer-Verlag

[8]. L. Chen, K. Harrison, N. P. Smart, D. Soldera, “Applications of multiple trust authorities in pairing based cryptosystems”, InfraSec 2002, LNCS 2437, Springer-Verlag

[9]. C. Gentry, “Certificate-based encryption and the certificate revocation problem”, Advances in Cryptology – EUROCRPYT 2003, LNCS 2656, Springer-Verlag

[10]. S. Al-Riyami, K. Paterson, “Certificateless public key cryptography”, Advances in Cryptology – Asiacrypt 2003, LNCS 2894, Springer-Verlag

[11]. S. Kwon, S. Lee, “Security Analysis and Improvement for Key Issuing Schemes in ID-Based Cryptography”, TrustBus 2006, LNCS 4083, Springer