Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 12, December 2013, pg.10 – 14

RESEARCH ARTICLE

Secure Transaction System Using ID Based Cryptography

Jaydipsinh B. Jadeja[*], Harikrishna Jethva[**], Bhadreshsinh G. Gohil [***]

*(PG-ITSNS Student, Department of Computer Engineering, Gujarat Technological University, Ahmedabad
Email: jaydip189@gmail.com)
** (Associate Professor, L D Engineering College, Ahmedabad
Email: hbjethva@gmail.com)
*** (Assistant Professor, SIEM, Rajpur, Mehsana
E-mail: bhadu.gohil@gmail.com)

Abstract— Today more and more number of clients are using online transactions, and so online transaction systems are becoming more desirable targets for security attacks. To maintain the clients trust and confidence in the security of their online transaction application, financial firm must identify how attackers compromise accounts and develop methods to protect them. Towards this purpose, we present a modified model to authenticate clients for online transaction transactions through utilizing Identity-Based Cryptography techniques in conjunction with the one-time ID concept for the purpose of increasing security. Identity-based public key encryption facilitates easy introduction of public key cryptography which allows an entity's public key to be derived from an arbitrary id value, such as name or email address or birthdate. The main practical benefit of identity-based cryptography is in greatly reducing the need for, and reliance on, public key certificates. Although some interesting identity-based techniques have been developed in the past, none are compatible with popular public key encryption algorithms. This limits the utility of identity-based cryptography as a transitional step to full-blown public key cryptography. Furthermore, it is fundamentally difficult to reconcile fine-grained revocation with identity-based cryptography. Using ID based cryptography we can enhance the performance of transaction management system with high level security. A noble approach will be selected to provide a solution for secure key exchange for transaction purpose with enhanced security.

Keywords— ID Based Cryptography; Mediated rsa; Transaction System

I. Introduction

1.1 Cryptography

Cryptography is probably the most important aspect of communications security and is becoming increasingly important as a basic building block for computer security. Cryptography is a mathematical based technology to ensure the information security over a public channel. The increased use of computer and communications systems by industry has increased the risk of theft of proprietary information. Although these threats may require a variety of countermeasures; encryption is a primary method of protecting valuable electronic information. By far the most important automated tool for network and communications security is encryption.

Two forms of encryption are in common use: conventional or symmetric encryption and public-key or asymmetric encryption [1].

1.1.1 Symmetric Key Cryptography

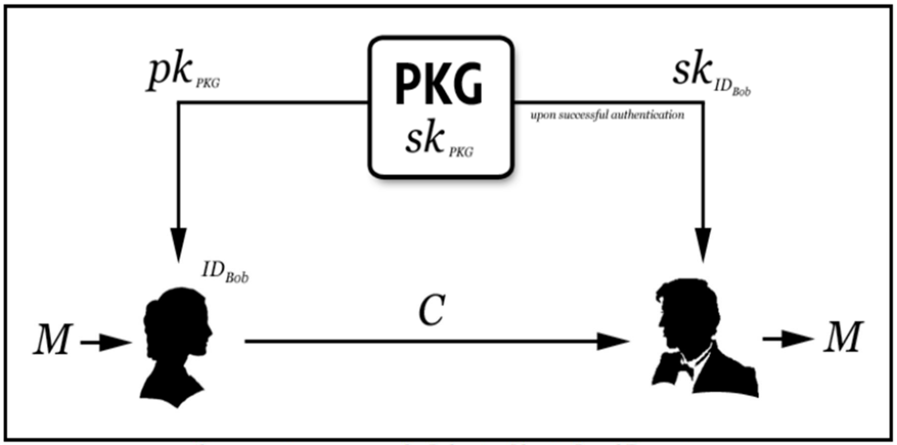
The first and oldest-dating back to the 1970s-dedicated key Cryptography architecture uses the same data encryption technology to manage keys and scramble data. In these systems, called “Symmetric key” systems, because the same key is used to encrypt and decrypt information, the key manager generates a new key for every message at the sender’s request. The key is stored in a database along with the list of receivers. When the receiver authenticates, the key is retrieved from the database and the receiver name is matched against the list of authorized recipients. If everything checks out, the decryption key is sent to the receiver [1].

1.1.2 Public Key Cryptography

In the early 1980s, a series of mathematical innovations led to important new kinds of encryption algorithms. These algorithms, called “public key” or “asymmetric” systems use a different key to encrypt data than the one they use to decrypt data. The famous Diffie-Hellman and RSA algorithms are the best-known examples of public key algorithms. While they are ill-suited to encrypting large chunks of data, asymmetric algorithms are perfectly suited to managing keys, since they can readily encrypt smaller, key-sized objects [1].

1.1.3 ID Based Cryptography

In 1984, Adi Shamir, of RSA notoriety, introduced the concept of identity-based cryptography. Its primary innovation was its use of user identity attributes, such as email addresses or phone numbers, instead of digital certificates, for encryption and signature verification. This feature significantly reduces the complexity of a cryptography system by eliminating the need for generating and managing users' certificates. It also makes it much easier to provide cryptography to unprepared users, since messages may be encrypted for users before they interact with any system components.



Alice encrypting a message for Bob using Identity-Based Encryption

Figure 1.1 ID Based Cryptography [10]

The process of encryption and decryption proceeds as follows:

1. Alice prepares plaintext message M for Bob.
2. Bob receives C from Alice. In most implementations it is assumed that C comes with plaintext
3. Bob decrypts C using his private key sk_{IDBob} to recover plaintext message M.

II. Literature Review

1.2 Identity based encryption

Identity-based encryption (IBE) is a public-key encryption technology that allows a public key to be calculated from an identity and a set of public mathematical parameters and that allows for the corresponding private key to be calculated from an identity, a set of public mathematical parameters, and a domain-wide secret value. An IBE public key can be calculated by anyone who has the necessary public parameters; a cryptographic secret is needed to calculate an IBE private key, and the calculation can only be performed by a trusted server that has this secret.

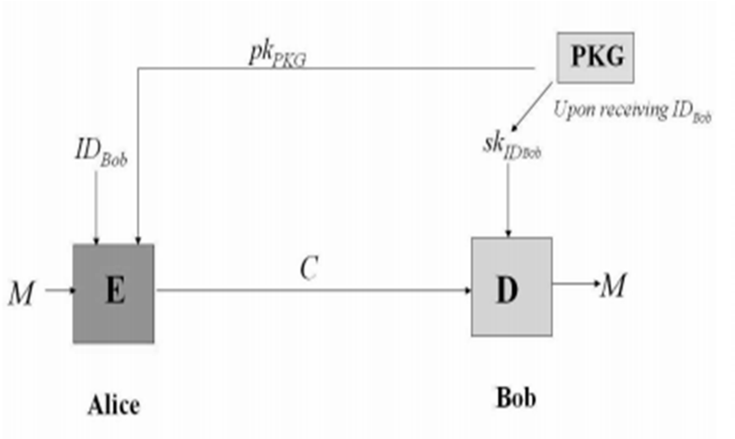


Figure 2.1: Identity-Based Encryption [3].

2.2 Related Work

In ID based Cryptography era, Algorithm efficiency interest among researchers and lots of work had been done in this regard to provide better systems using rsa algorithm.

i **B. Lee, "Unified Public Key Infrastructure Supporting Both Certificate-Based and ID-Based Cryptography," 2010 International Conference on Availability, Reliability Security, pp. 54–61, Feb. 2010.**

In this paper they introduce a new concept called unified public key infrastructure (UPKI) in which both certificate-based and ID-based cryptography are provided to users in a highly combined manner. Here they assume the existence of a trusted authority called key generation and certification authority (KGCA) who has the role of both CA and KGC. It checks identification information of user and issues a certificate for a user-chosen public key X. It also issues ID-based partial private key to the user [2].

Results: In cryptography the proposed method is a new approach to divide an authority into multiple parties. This approach will be useful in many applications where the authority is really powerful and some kind of control or observation is required. It will help to make the real world authorities be more distributed ones.

ii B. Lee, C. Boyd, J. Yang, and S. Yoo, "Secure Key Issuing in ID-based Cryptography," no. Gentry, 2003.

In this paper They propose a new secure key issuing protocol in which a private key is issued by a key generation center (KGC) and then its privacy is protected by multiple key privacy authorities (KPAs). In this protocol They provide a secure channel by using a simple blinding technique in pairing-based cryptography. Only a legitimate user who has the secure blinding parameter can retrieve his private key from the protocol. In the proposed scheme user-chosen secret information is used, but it is used only for blinding purpose. The proposed secure key issuing protocol issues a real ID-based private key, thus it can be used with any ID-based cryptosystems preserving the advantage of ID-based cryptography [4].

Results: In cryptography the proposed method is a new approach to divide an authority into multiple parties. This approach will be useful in many applications where the authority is really powerful and some kind of control or observation is required. It will help to make the real world authorities be more distributed ones.

iii S. K. Nayak, "An ECDLP based Untraceable Blind Signature Scheme" pp. 829–834, 2013.

In this paper, they present a novel blind signature scheme based upon security of ECDLP. The proposed scheme is untraceable. The proposed scheme is also universally verifiable. The proposed scheme can withstand some of the active attacks like forgery attack, key-only attack, and known-message attack, chosen message attack [5].

Results: The scheme also satisfies untraceability property. They have proved that their scheme is universally verifiable. The proposed scheme has low computational overhead and proved to be resistant against active attacks. The proposed scheme is suitable for applications, such as, e-banking, e-commerce and e-voting.

iv **Gopal, P.V.S.S.N.,"New ID-based signatures scheme from bilinear pairings over elliptic curves",2013 IEEE 3rd International On Advance Computing Conference (IACC) , pp.361 – 365Feb. 2013**

In this paper, they propose a new ID-based signature scheme using bilinear pairings. This scheme is secure against existential forgery on adaptive chosen message and ID attack with the assumption that the CDHproblem is intractable [7].

Results: They have proved that the proposed scheme is unforgeable in the random oracle model with assumption that the CDH problem is intractable.

v D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," pp. 213–229, 2001.

In this paper they have proposed a fully functional identity-based encryption scheme. The performance of our system is comparable to the performance of ElGamal encryption [8].

Results: The security of our system is based on a natural analogue of the computational Diffie-Hellman assumption on elliptic curves. Based on this assumption we show that the new system has chosen ciphertext security in the random oracle model.

vi S.Rajalakshmi and S.K.Srivatsa,”Identity-Based Encryption Using mRSA in Electronic Transcation”, pp.435-440,2007.

In this paper, they propose Identity Based Encryption with mediated RSA and then applies this concept to do secure transaction through Internet[11].

Results: In this scheme Identity Based Cryptography so that no third party involved in generating the public keys.

III. Conclusion

We survey the state of research on identity-based cryptography. We start from reviewing the basic concepts of identity-based encryption and signature schemes, and subsequently review some important identity-based cryptographic schemes, a computational primitive widely used to build up various identity-based cryptographic schemes in the current literature. We also survey the cryptographic schemes such as a “Secure Key Issuing in ID-based Cryptography” and a “An ECDLP based Untraceable Blind Signature Scheme", which were able to be constructed thanks to the successful realization of identity-based encryption. Finally, we discuss how feasible and under what conditions identity-based cryptography may be used in current and future environments and propose some interesting open problems concerning with practical and theoretical aspects of identity based cryptography.

.

References

[1] Stallings.,2003.Cryptography and Network Security Principles and Practices, Prentice-Hall of India Private Limited, 3rd Edn.

[2]B. Lee, “Unified Public Key Infrastructure Supporting Both Certificate-Based and ID-Based Cryptography,” *2010 Int. Conf. Availability, Reliability. Security.* pp. 54–61, Feb. 2010.

[3]J.Baek, J.Newmarch, R. Safavi-naini, W. Susilo, and C. Science, “A Survey of Identity-Based Cryptography Based Encryption “.

[4]B. Lee, C. Boyd, J. Yang, and S. Yoo, “Secure Key Issuing in ID-based Cryptography,” no. Gentry, 2003.

[5]S. K. Nayak, “An ECDLP based Untraceable Blind Signature Scheme” pp. 829–834, 2013.

[6] K. G. Paterson, “ID-based signatures from pairings on elliptic curves,” vol. 38, no. 18, pp. 1025–1026, 2002.

[7]Gopal, P.V.S.S.N., “New ID-based signatures scheme from bilinear pairings over elliptic curves”,2013 IEEE 3rd International On Advance Computing Conference (IACC) , pp. 361 – 365 Feb. 2013

[8]D. Boneh and M. Franklin, “Identity-Based Encryption from the Weil Pairing,” pp. 213–229, 2001.

[9]A. P. Standard and F. O. R. Protecting, “The Identity-Based Encryption Advantage,” vol. 1, no. 408.

[10]C. March and C. Youngblood, “An Introduction to Identity-based Cryptography,” no. March, 2005.

[11].S.Rajalakshmi and S.K.Srivatsa,”Identity-Based Encryption Using mRSA in Electronic Transcation”, pp.435-440,2007.