Key Exchange Using Biometric Identy Based Encryption for sharing encrypted data in cloud environment

Waleed K. Hassan, Hisham Al-Assam
Applied Computing Department, The University of Buckingham, UK.
{waleed.hassan, hisham.al-assam1}@buckingham.ac.uk

ABSTRACT

The main problem associated with using symmetric/ asymmetric keys is how to securely store and exchange the keys between the parties over open networks particularly in the open environment such as cloud computing. Public Key Infrastructure (PKI) have been providing a practical solution for session key exchange for loads of web services. The key limitation of PKI solution is not only the need for a trusted third partly (e.g. certificate authority) but also the absent link between data owner and the encryption keys. The latter is arguably more important where accessing data needs to be linked with identify of the owner. Currently available key exchange protocols depend on using trusted couriers or secure channels, which can be subject to man-in-the-middle attack and various other attacks. This paper proposes a new protocol for Key Exchange using Biometric Identity Based Encryption (KE-BIBE) that enables parties to securely exchange cryptographic keys even an adversary is monitoring the communication channel between the parties. The proposed protocol combines biometrics with IBE in order to provide a secure way to access symmetric keys based on the identity of the users in unsecure environment. In the KE-BIOBE protocol, the message is first encrypted by the data owner using a traditional symmetric key before migrating it to a cloud storage. The symmetric key is then encrypted using public biometrics of the users selected by data owner to decrypt the message based on Fuzzy Identity-Based Encryption. Only the selected users will be able to decrypt the message by providing a fresh sample of their biometric data. The paper argues that the proposed solution eliminates the needs for a key distribution centre in traditional cryptography. It will also give data owner the power of fine-grained sharing of encrypted data by control who can access their data.

Keywords: Identity-Based Encryption, Fuzzy Identity-based Encryption, Biometric based key exchange

1. INTRODUCTION

Typically, cloud environment refers to the ability of increasing the storage size and/or adding extra capabilities than what traditional information technologies can offer. Now, many small and medium size organizations are growingly realizing the advantages of migrating their data or applications to be hosted in cloud environments [1]. However, the increasing number of applications and the volume of sensitive information that individuals, companies, and organization are storing on the cloud has led to a serious security concerns. This is particularly important because once data is transferred to a cloud environment, the control is completely transferred to be in the hand of a third "trusted" party i.e. cloud service providers CSPs. Therefore, the security of the data and the privacy of the users are the key issues reluctance of individuals and companies to use the cloud environment [1] [2]. Many researchers have been focussing on the possibility of protecting such data even if it is outside the physical control of the data owner. One intuitive solution to maintain data security is by encrypting the data before being migrated to the cloud. However, using traditional cryptography, the key exchange or key establishment issue is also emerged big challenge to exchange cryptographic keys between parties. There are a number of mature solutions in traditional cryptography to exchange keys based on the so called a Key Distribution Centre (KDC) [3]. Diffie-Hellman (DH) is one of most convenient protocol for key exchange [4] where in its general form, it is secure against eavesdropping but not secure against man-in-the-middle attacks [5]. Existing solutions to overcome the man-in-the-middle attack incorporate authentication of two trusted parties, which cannot be adopted in the cloud due to the absence of an agreeable trust model in the cloud.

Identity based encryption (IBE) presented by [6] is a key step forward to solve the problems associated with key distribution in public key infrastructure i.e. IBE eliminates the need for public key digital certificates. Therefore, the need for pre-distributed keys before any encrypt/decrypt in traditional cryptography will be illuminated, which gives a great deal of flexibility required in environment such as the cloud. More importantly, IBE link decryption keys with user identities. This enables data owner to be integral part of selecting who can access their encrypted data in cloud environment. Fuzzy IBE (F-IBE) [7], on the other hand, is a further development of IBE in which users are issued with decryption key (private keys) associated with their identities *id* . The user will be able to decrypt a ciphertext that was encrypted with their public keys of their identities *id'* if and only if the overlapping between *id* and *id'* is bigger than an agreed threshold.

This paper proposes a new protocol for Key Exchange using Biometric Identity Based Encryption (KE-BIBE) to enable parties to exchange cryptographic keys securely even an adversary is monitoring the communication channel between the parties. The proposed protocol relies on F-IBE to combine biometrics with IBE in order to provide a secure way to access symmetric keys based on the identity of the users in unsecure environment. In the KE-BIOBE, the message is first encrypted by the data owner using a traditional symmetric key before migrating it to a cloud storage. The symmetric key is then encrypted using public biometrics of the users selected by data owner to decrypt the message. The paper argues that the proposed solution eliminates the needs for a key distribution centre in traditional cryptography. Only the selected users will be able to decrypt the message by providing a fresh sample of their biometric data i.e. it will give data owner the power of fine-grained sharing of encrypted data by control who can access their data.

The rest of the paper is organized as follows. Section 2 presents background materials and literature review. Section 3 introduces the existing work related to biometric IBE. Section 4 gives of the overall structure of the KE-BIOIBE system framework where section 5 presents all the details of the KE-BIOIBE scheme. Conclusion is presented in section 6.

2. BACKGROUND AND LITERATURE REVIEW

This section gives an overview on certain topics that considered as main ingredients of our proposed protocol, and then presents some of IBE's related work.

2.1 Bilinear pairing

Let $\mathbb{G}_0$ and $\mathbb{G}_1$ be two multiplicative cyclic groups of prime order q where $< g >$ is a generator of $\mathbb{G}_0$, and e is a bilinear map such that $e: \mathbb{G}_0 \times \mathbb{G}_0 \rightarrow \mathbb{G}_1$.

The following conditions should be met by e to be bilinear pairing.

- For each element $a, b \in \mathbb{Z}_q^+$ and $< g >$ in $\mathbb{G}_0$ we have $e(g^a, g^b) = e(g, g)^{ab} = e(g^b, g^a)$.
- $e(g, g) \neq 1$ (i.e., non-degenerated).

If the condition are met then the bilinear map $e: \mathbb{G}_0 \times \mathbb{G}_0 \rightarrow \mathbb{G}_1$ can be calculated efficiently [7].

2.2 Threshold secret sharing systems

Shamir sharing secret system was presented in the seventies of the last century in [8] in order to distribute a sensitive information among n parts and reconstruct the information in an easy way from a subset of the n parts. Shamir system works as a threshold model using polynomial interpolation by picking two positive integers α *and* β with $\alpha \leq \beta$. The (α , β) threshold secret sharing allows to distribute a secret value δ over n users $(u_1, u_2, \ldots, u_n)$ in such away that a subset of minimum α users are required to reconstruct the original secret value δ where the polynomial interpolation *f(x)* should be of a degree α-1, and the value of the polynomial at zero is equal to the secret δ i.e., *f(0)* = δ.

2.3 Standard Identity Based Encryption (IBE)

The scheme of IBE was presented by [6] to be as an important development in public key cryptography. The public key associated with IBE is an arbitrary string of unique information that represents a user's identity such as an email address, telephone numbers or driver license number. In IBE, a trusted third party server called a Private Kay Generator (PKG) has the responsibility of generating and publishing master public parameters *PP* of users' identities whereas master secret parameter(s) *msk* are stored and kept securely In order to send an encrypted message from Alice to Bob, IBE works as follows:

- Both Bob's email and the *PP* published by PKG are used to compute Bob's public key *PK.*
- Alice encrypts the message using Bob's *PK* then sends it to Bob.

- Bob needs to get the corresponding private key *sk* of his identity (i.e., his email), so he authenticates himself to PKG, to retrieve the decryhption key.
- Bob decrypts the ciphertext and gets the message.

The construction of IBE offers an effective way that cancel the need for pre-distribution keys stages that associated with traditional public key cryptography. It does also link the keys with individual identities as explained above.

3. EXISITING WORK ON BIOMETRIC IDENTITY BASED ENCRYPTION

Fuzzy identity based encryption was introduced by [7]. A Set of descriptive attributes is adopted to represent an identity. The scheme's idea bases on a private key of an identity *x* has a capability to decrypt a ciphertext was encrypted by a public key of an identity *x'* in case of *x* and *x'* are closely enough i.e., the distance between *x* and *x'* be less than or equal to certain value (or threshold value). Shamir sharing secret was nice exploited through distribute and reconstruct master secret value over and from set of attributes, which construct the identity. Two interesting application were derived from using fuzzy identity based encryption scheme: biometric identity based encryption *BIO-IBE* and attribute based encryption *ABE*. In BIO-IBE, the identity *x* is a feature vector $(f_1, f_2, \ldots, f_n)$ of size *n* that extracted from biometric data using particular feature extractor technique and then stored in template database. Whereas, the identity x' represents a feature vector $(f'_1, f'_2, \ldots, f'_n)$ extracted from fresh query biometric. A $(d$ -1)-degree of polynomial is used to distribute and reconstruct the secret value over set of overlapping feature between x and x' in such away $|x \cap x'| \geq d$. Interpolating subset of d-features be enough to reconstruct the secret value, then decrypts the ciphertext using a private key components of identity x' a ciphertext was encrypted by public key of identity *x*. In second application, a descriptive attributes use to encrypt/decrypt a message *M*. A certain set of descriptive attributes such {Dept =Applied computing, staff, age >=40, computer science} are used in encryption phase. While, anyone has *d*- attributes should be capable to decrypt the encrypted message. The *d* value is decided by a dealer for instance, if *d*=3, then a person with {Dept =Applied computing, staff, age 42} be able to decrypt the encrypted message.

IBE in [9] was developed to build a new scheme of digital signature basing on an identity called identity based signature IBS [10]. As in [7] two interesting applications of fuzzy identity based signatures were presented which were secured against adaptive chosen attack. They exploited parameters are used to construct fuzzy identity based encryption to construct both applications.

Others, such in [11] relayed on Sakai-Kasahara scheme [12] in private keys generation stage. The scheme states that, to encrypt a message M, the recipient's biometric template beforehand need to be at the hand of the sender. Thereafter, the signature σ of the *PKG* upon the public parameter *PAR* of the recipient need to be verified. In case of σ be valid, a fuzzy extraction is used to compute the biometric identity ID. Four algorithms are used with an assumption that, if and only if $|w \cap w'| \geq d$, then $ID = ID'$. Two hash functions H_a and H_b are selected whereas $H_a: \mathbb{Z}_p{}^* \times \{0,1\}^*$ and $H_b: \mathbb{G}_T \rightarrow \{0,1\}^m$. Besides, hash function $H: b \rightarrow \{0,1\}^*$ is selected by PKG in addition to an encoding C_e and decoding C_d functions along with a certain feature extractor F_e technique that is implemented over biometric data b. The ID is computed by hashing template b i.e., $ID = H(b)$. Then after, depending on w and ID, the PKG outputs the private key components $g^{1/(x+H_a(\mu_i,ID))} = g^{1/(x+h_i^{ID})}$ for each feature (or attribute) $\mu_i \in w$. An encryption algorithm is applied by making a receipt's biometric data (Bob's biometric) at the hand of the sender (Alice) along with the related PAR. A re-produce algorithm *Rep* uses to compute an identity *ID'* by adopting $ID' = Rep(b', PAR)$, where b' represents a biometric data of w' identity. Therefore, $ID = ID'$ only in case of the distance dis between b and b' are within a threshold t scope.

4. THE PROPOSED KEY EXCHANGE BASED ON BIOMETRIC IBE

In general, the proposed KE-BIOIBE system provides a new protocol for keys exchanging that enables two parties Alice and Bob to securely exchange cryptographic keys even an adversary is monitoring the communication channel between them. Assume Alice has encrypted data (or message) and store it in a cloud environment and she would like to give Bob access to the encrypted data. Typical PKI solutions do not only require pre-distributed key management and a trusted third partly (e.g. certificate authority), but also they do not offer a clear link between data owner and the encryption keys. Therefore, the proposed KE-BIOIBE protocol offers a practical solution that gives data owner (Alice) the power of fine-grained sharing of here encrypted data by control who can access their data.

The key stages of the proposed solution can be summarised as follows:

- Alice encrypts her data using traditional encryption (symmetric/ asymmetric) techniques such as AES or RSA.

$$\mathcal{E}_M \longleftarrow Enc(\, sk, M) \tag{1}$$

- She stores the encrypted data in a cloud environment.
- Now, if Alice wants to allow Bob to decrypt the message, she encrypts the encryption key *sk* using a public key of Bob's unique identity *w'* (i.e., Bob's biometric such as a photo of his face) to produce $\mathcal{E}_{sk}$.

$$\mathcal{E}_{sk} \longleftarrow Enc(\, pk_{id}, sk) \tag{2}$$

- Alice sends the output $\mathcal{E}_{sk}$ to Bob.
- To get the *sk*, Bob needs to provide a fresh biometric sample *w*
- If and only if the overlap between *w* and *w'* is greater than a threshold value, Bob will retrieve the corresponding private key of his identity and decrypt the ciphertext to get the *sk*.

$$sk \longleftarrow Dec(\, sk_{id}, sk) \tag{3}$$

- Bob brings the encrypted data stored in the cloud environment to his local device, and uses *sk*, to retrieve the original message/data.

$$M \longleftarrow Dec(\, sk, \mathcal{E}_M) \tag{4}$$

The paper argues that since the face biometric data, for example, is a public between parties who knows each other, it can be obtained from many resources such as social media resources (e.g., Facebook, Instagram, etc.). Hence, face recognition is ideal biometric trait for our proposal.

The above key stages are illustrated in figure 1, which shows the overall framework of the KE-BIOIBE system to bind traditional encryption key *sk* with user's biometric data to provide effective access control mechanisms for cloud storage.

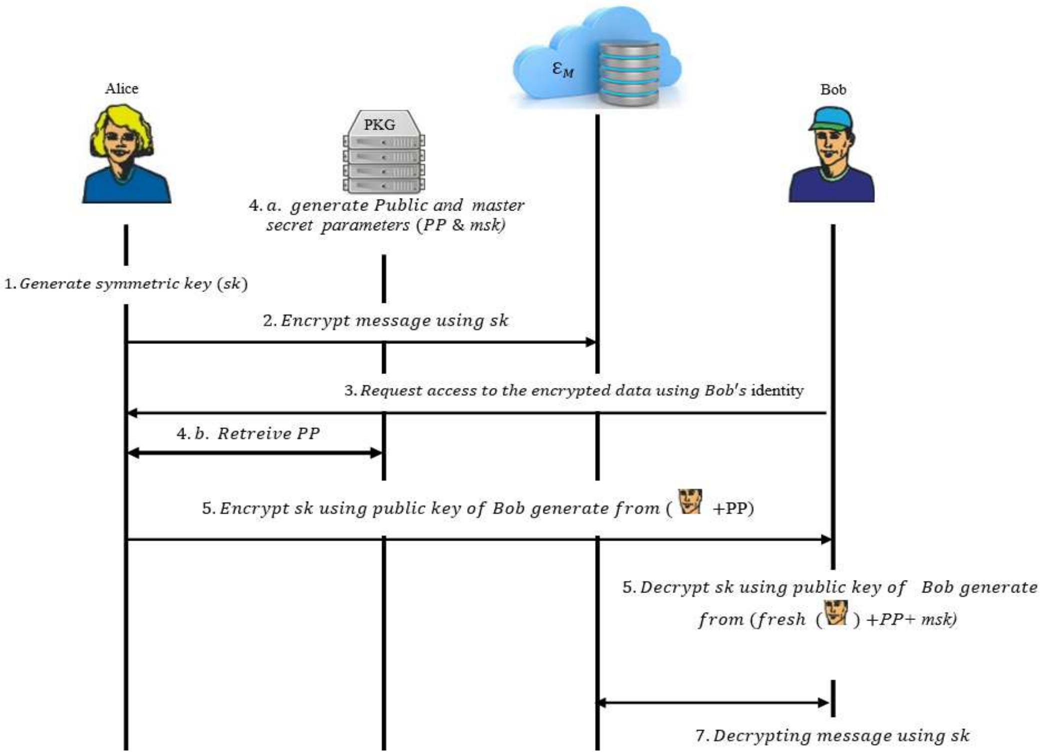
$\mathcal{E}_M$
Alice
PKG
Bob
4.a. generate Public and master secret parameters (PP & msk)
1. Generate symmetric key (sk)
2. Encrypt message using sk
3. Request access to the encrypted data using Bob's identity
4.b. Retreive PP
5. Encrypt sk using public key of Bob generate from (+PP)
5. Decrypt sk using public key of Bob generate from (fresh ( ) +PP+ msk)
7. Decrypting message using sk

Figure1. An overview of general KE--BIOIBE framework

5. KE-BIOIBE DESCRIPTION

Our protocol relies on the concept of fuzzy identity based encryption scheme proposed [7] to bind the encryption keys with users' identity instead of using certificate authorities. The proposal has four main stages (*setup, Key extraction, Encryption and Decryption*) to implement the key exchange KE-BIOIME explained in the previous section.

Let $\mathbb{G}_0$ be a bilinear group of prime order p, and $< g >$ be a generator of $\mathbb{G}_0$. Let also e be a bilinear map such that: $e: \mathbb{G}_0 \times \mathbb{G}_0 \rightarrow \mathbb{G}_1$. In our proposal, each identity consists of a set of n strings of an arbitrary length. The collision resistant hash function [7]is selected to convert each string in the identity into the corresponding integer in $\mathbb{Z}_p$. Eventually, the Lagrange coefficient $\Delta_{i,S}$ is defined for $i \in \mathbb{Z}_p$ and a set of element S in $\mathbb{Z}_p$ as follows:

$$\Delta_{i,S}(x) = \prod_{j \in S, j \neq i} \frac{x - j}{i - j}$$

As explained above, Alice generates an encryption key *sk* in order to encrypt her message *M* before storing it in a public cloud computing, then the following four stages are applied:

- ***Setup (n, d).***

In the beginning, we assume that Alice has Bob's public identity of (i.e., Bob's face image), then she sends request to a PKG to generate public and private parameters.

- The elements $g_1 = g^y, g_2$ are chosen from $\mathbb{G}_\mathbf{1}$
- Uniformly at random from $\mathbb{G}_\mathbf{1}$ **,** we choose $t_1, \ldots, t_{n+1}$ where *n* is the length of the identity.
- Uniformly at random from $\mathbb{Z}_p$, we choose y.
- Let *N* be the set $\{1, \ldots, n+1\}$ and we define a function *T* as:

$$T(x) = g_2^{x^n} \prod_{i=1}^{n+1} t_i^{\Delta\, i,N(x)}$$

The public parameters will be $g_1,\ g_2, t_1, \ldots, t_{n+1}$ while *y* represents the master secret key *msk.*

- ***Key extraction.***

The key extraction algorithm uses to generate a private key sk_{id} of Bob's identity *w* in order to decrypt the *sk.* The process of extracting the private key components for identity *w* is as follows:

A random (d-1)-degree polynomial *p* is chosen with constraint that all values at point zero equal to *msk*, i.e., $p(0) = y$. The private key consists of two parts $\{D_i\}$ and $\{d_i\}$ for each $i \in w$:

$D_i = \ g_2^{p(i)}\ T(i)^{r_i}$, and
$d_i = g^{r_i}$ where r_i is randomly chosen from $\mathbb{Z}_p$ for each $i \in w$.

- ***Encryption.***

Alice encrypts the *sk* before sending it to Bob. To encrypt the $sk \in \mathbb{G}_2$using the public key of Bob's identity *w'*, choose random $k \in \mathbb{Z}_p$. The ciphertext will consists of four parts:

$$CT = (w', E' = sk.e(g_1, g_2)^k, E'' = g^k, \{E_i = T(i)^k\}_{i \in w'})$$

- ***Decryption.***

Now, Bob needs to present his identity *w* (i.e., his fresh biometric) to get the corresponding private key of *w*. The decryption algorithm includes the following procedure:

Assume the $\mathcal{E}_{sk}$ represents the encrypted *sk* was encrypted using the public key of identity *w'*. Then, another key of identity *w* could be able to decrypt the $\mathcal{E}_{sk}$ if and only if $|w \cap w'| \geq d$. If the overlapping between w and w' satisfying the threshold value *d*, then an arbitrary subset *S* of *d-elements* would be enough to decrypt *CT*, where *S is a subset of* $w \cap w'$. Following steps will despite the decryption algorithm.

$$sk \; = E' \prod_{i \in S} (\frac{e(d_i, E_i)}{e(D_i, E'')})^{\Delta \; i,s(0)}$$

In order to prove a correctness:

$$sk \; = E' \prod_{i \in S} (\frac{e(d_i, E_i)}{e(D_i, E'')})^{\Delta \; i,s(0)}$$

$$= sk. e(g_1, g_2)^k \prod_{i \in S} (\frac{e(g^{r_i}, T(i)^k)}{e\big(g_2^{p(i)} \; T(i)^{r_i}, g^k\big)})^{\Delta \; i,s(0)}$$

$$= sk. e(g_1, g_2)^k \prod_{i \in S} (\frac{e(g^{r_i}, T(i)^k)}{e(g_2^{p(i)}, g^k). e(\; T(i)^{r_i}, g^k)})^{\Delta \; i,s(0)}$$

$$= sk. e(g_1, g_2)^k \prod_{i \in S} (\frac{e(g,T(i))^{r_i k}}{e(g_2^{p(i)},g^k).e(g,T(i))^{r_i k}})^{\Delta \; i,s(0)}$$

by canceling $e(g, T(i))^{r_i k}$

$$= sk. e(g_1, g_2)^k \prod_{i \in S} \frac{1}{e(g_2^{p(i)}, g^k)^{\Delta \; i,s(0)}}$$

by interpolating the exponents, and since $p(0) = y$ using *d* points, the result be:

$$= sk. e(g, g_2)^{ky} \prod_{i \in S} \frac{1}{e(g_2, g)^{ky}} = sk$$

Where the *sk* uses to decrypt the encrypted data stored in public cloud computing.

Fuzzy Selective-ID is a model defined by Sahai and Waters in [7] to proof the security of fuzzy identity based encryption. In our protocol, the same model will be followed. Fuzzy Selective-ID states that, any scheme is secure if all polynomial-time of adversaries have at most a negligible advantage in the following game [7]:

1) Adversary $\mathcal{A}$ declares an identity I to be challenged upon.
2) *Setup:* The challenger $\mathcal{C}$ executes the setup algorithm described in the previous section then publishes the public parameters *PP*, *which can be accessed by* the adversary $\mathcal{A}$.
3) $\mathcal{A}$ issues queries for private keys of several identities δ_i, where $|\delta_i \cap ID| < \; d$ for all i.
4) Two equal length messages $|\mathcal{M}_0| = |\mathcal{M}_1|$ are issued by $\mathcal{A}$. Afterwards, $\mathcal{C}$ flips a random coin, α, then encrypts $\mathcal{M}_\alpha$ with ID and sends the ciphertext to $\mathcal{A}$.
5) Repeat the step 3.
6) $\mathcal{A}$ outputs guess α' of α.

$\mathcal{A}$ wins the game if and only if $\alpha' = \; \alpha$. The advantages ϵ of an adversary $\mathcal{A}$ will be defined as the following:

$$\Pr[\alpha' = \; \alpha] - \frac{1}{2}$$

6. Conclusion

This paper proposed a new protocol for Key Exchange using Biometric Identity Based Encryption (KE-BIBE) that enables parties Alice and Bob to securely exchange cryptographic keys even an adversary is monitoring the communication channel between the parties. We showed that the proposed protocol combines biometrics with IBE in order to provide a secure way to access symmetric keys based on the identity of the users in unsecure environment. In the proposed KE-BIOBE protocol, the message is first encrypted by the data owner (Alice) using a traditional symmetric key before migrating it to a cloud storage. The symmetric key is then encrypted using public biometrics of the users selected by data owner to decrypt the message based on Fuzzy Identity-Based Encryption. We showed that only selected users (Bob as example) was able to decrypt the message by providing a fresh sample of their biometric data. We argued that the proposed solution could eliminate the needs for a key distribution centre in traditional cryptography but more importantly is gives Alice as a data owner the power of fine-grained sharing of encrypted data by control who can access her data.

References

[1] D. Chen and H. Zhao, "Data security and privacy protection issues in cloud computing," in *Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on*, 2012.

[2] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," *Journal of network and computer applications,* vol. 34, no. 1, pp. 1-11, 2011.

[3] M. Co., "Key Distribution Center," 2016. [Online]. Available: https://msdn.microsoft.com/en-us/library/windows/desktop/aa378170%28v=vs.85%29.aspx. [Accessed 05 05 2017].

[4] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE transactions on Information Theory,* vol. 22, no. 6, pp. 644-654, 1976.

[5] K. S. Vicente REVUELTO, "Weaknesses in Diffie-Hellman Key (Whitepaper)," 2016.

[6] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Workshop on the Theory and Application of Cryptographic Techniques,* 1984.

[7] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, 2005.

[8] A. Shamir, "How to share a secret," *Communications of the ACM,* vol. 22, no. 11, pp. 612-613, 1979.

[9] B. Waters, "Efficient identity-based encryption without random oracles," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, 2005.

[10] P. Yang, Z. Cao and X. Dong, “Fuzzy Identity Based Signature.,” *IACR Cryptology EPrint Archive*, vol. 2008, p. 2, 2008.

[11] N. D. Sarier, “A new biometric identity based encryption scheme secure against DoS attacks,” *Security and Communication Networks,* vol. 4, no. 1, pp. 23-32, 2011.

[12] R. Sakai and M. Kasahara, “ID based Cryptosystems with Pairing on Elliptic Curve.,” *IACR Cryptology ePrint Archive,* vol. 2003, p. 54, 2003.