IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 11, November 2015

A Review on Functional Encryption Schemes and their usage in VANET

Sandhya Kohli [1], Kanwalvir Singh Dhindsa [2], Ravinder Khanna [3]

Research Scholar, Punjab Technical University, Kapurthala, Punjab, India[1]

Associate Professor (CSE & IT Department), B.B.S.B. Engineering College, Fatehgarh Sahib, Punjab, India[2]

Dean R & D, MM University, Sadopur, Ambala[3]

Abstract: A vehicular Ad–hoc network (VANET) is an important component of intelligent transport system (ITS), and provides an eminent way to communicate with other nodes while driving. For vehicular communications (VC) a secure method must be employed for message and data dissemination. Various encryption and decryption schemes have been devised so far for message communication in VANET. Earlier symmetric and asymmetric encryption techniques were employed in VANET for secure communication but it has many inherent shortcomings so a new encryption standard known as functional encryption scheme has been used in VANET. In this paper a comparison of various encryption schemes i.e. symmetric/ asymmetric and various functional encryption schemes has been done to reveal the utility of functional encryption in VANET. Although functional encryption scheme has many subgroups but in this paper two major subgroups of functional encryption i.e. predicate encryption (PE) and Attribute based encryption (ABE) are compared to reveal the benefits of each scheme.

Keywords: VANET, Encryption, Security, Vehicular Communication.

I. INTRODUCTION

Vehicular Ad-hoc Networks (VANET) is the future generation networking technology that provides an enhanced transportation system known as intelligent transport system (ITS). Vehicular ad-hoc networks is the enhancement of mobile ad-hoc networks (MANET). In VANET each participating vehicle acts like a node. For ITS system each vehicle participates in vehicular communication act as a node. Each node can send, receive and broadcast the information in the vehicular network. The main components of vehicular network are Road Side Units (RSU), On Board Unit (OBU) and GPS system, a vehicle must be equipped with it to allow vehicular communication. VANET system is used for variety of applications like **i.** ***Entertainment/Comfort Applications*** These applications are also known as non safety applications as they enhance the driver and passenger's comfort level. This category of applications provide various facilities like weather information, traffic detail, location of nearest restaurant, petrol station and hotels, thereby assisting the drivers[1]. **ii.** ***Safety Applications*** These applications are aimed to provide safe driving conditions and avoid congestion and accidents. So this category of application enables safe and clean driving. The deployment of a comprehensive security system in VANET is very challenging, as the VANET exhibits high mobility and dynamicity. Variety of security schemes/protocols have been proposed for vehicular communication. The security paradigm in VANET propose that security scheme should exhibits following parameters **i.** ***Authentication*** it is the process of verification of identity between vehicle and RSU, to validate the information exchange[2]. The authentication ensures that legitimate vehicles are communicating in vehicular network ***ii. Confidentiality*** is an important security requirement for VANET as it ensures that data and messages will be read by authorized nodes only**.** ***iii. Integrity*** ensures that data received by nodes and RSU is same as send by the original sender, means it is not being tampered during communication**.** ***iv. Non Repudiation Property*** ensures that sender and receiver of the messages cannot deny their entitlement.

II. STATE OF THE ART

In vehicular networks using public key encryption with digital signatures although provides both security and data integrity against most of the attacks but it still has limited functionality. The public key encryption lacks the articulation needed to protect data in a open system like VANET, due to following reasons i. Public key encryption allows "all or nothing " access, partial and selected access and computation is not possible with public key encryption. ii. The traditional public key encryption does not provide fine grained access to encrypted data; it only provides coarse grained access. These shortcomings in public key encryption form the basis for the development of functional encryption schemes. Function encryption is an offbeat exemplar of public key encryption that enables both fine grained access control and selective computation on encrypted data. So Functional encryption is the recent demand for security paradigm in VANET**.**

Functional encryption is a technique in which the decryption key permits a user to know a specific function of the encrypted data and nothing else. In Functional encryption technique there is a trusted authority that holds

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 11, November 2015

a master secret key, which is known only to the authority. When input is give to authority as a description of some function f, then the authority generate a secret key with respect to that function sk[f] . Anyone having sk[f] can compute f[x] from encryption of any x. If E(pk,x) symbol is used for encryption of x then for decryption symbols will be E(pk,x) and sk[f] and the decryption output will be f(x), here pk is master key and x is the input function and sk[f] is the secret key . A functional encryption scheme consist of four algorithms they are

- A setup algorithm which generates a Master key (MK) and a public key (PK). Using the PK anyone can encrypt the message but only the Master key holder (MK) can decrypt it.
- Keygen algorithm takes MK and description of some function f as input, it produces a key called secret key (SK) which is specific to the function f and it is denoted by SK[f].
- An encryption algorithm E takes public key and message as input and outputs a ciphertext
- A decryption algorithm D takes secret key SK and ciphertext C as input and outputs a message i.e D(sk[f],c) outputs f(x).

In this algorithm SK[f] does not fully decrypt the ciphertext , it only produces a function f , to fully decrypt a ciphertext one can use a secret key SK[g] , where g is the identity function, where g(x) = x for all x .

III.LITERATURE RE VIEW ON VARIOUS ENCRYPTION SCHEMES

A. *Symmetric Key Encryption*

This was the oldest and first encryption technique. It is a technique that uses shared secret key to encrypt and decrypt data. The symmetric key algorithms are very efficient in processing large amount of information but computationally less intensive than asymmetric encryption algorithm. Various symmetric key algorithms were proposed namely AES, DES, 3DES, RC2, Blowfish and RC6. Experimental comparison of these algorithms is done by D.S Abdul et al. [3] on various parameters like execution time of encryption/decryption algorithm with different packet size, throughput of each encryption/decryption algorithm, effect of changed key size on power consumption and time consumption for encrypting/decrypting different types of files. D.S Abdul et al.[3] concluded through experimental results that Blowfish symmetric key algorithm has better performance than other algorithms. ***Drawbacks*** the symmetric key encryption suffers from many drawbacks like ***i.*** the shared secret key is required to be exchanged between sender and receiver. For sharing the key high level of trust process is required. ***ii.*** Key distribution and key storage is also crucial factor to achieve. ***iii.*** In symmetric encryption scheme there is no provision for authentication of sender, receiver and data integrity.

B. *Asymmetric Key Encryption*

Asymmetric key encryption comprises a set of well established techniques used for secure communication. In this encryption scheme there is a separate encryption and decryption keys. User can decrypt the message only if he had the appropriate decryption key. In this method public keys of the user will be exchanged, the release of public key does not cause any harm to the security of messages. Due to the unique public/private key of user, a secure communication is possible without key exchange. Various asymmetric key encryption algorithms have been proposed so far, but the most commonly used are RSA and Elliptic Curve Cryptography (ECC). Shahzadi Farah et al.[4] and M. Ali Mohammadi et al. [5] does an experimental evaluation of asymmetric key algorithms (RSA and ECC).Functionally RSA and ECC algorithms are quite similar, but the key size in ECC is much smaller than RSA. The key size in ECC is 571 bits where as in RSA the key size is 15360 bits. Nicholas Jansma et al. [6] perform the comparison of RSA and Elliptic Curve digital signatures and proposed that performance of RSA is comparable to ECC when used for digital signatures, for signature generation ECC takes less time of (3.07 sec), RSA takes (9.20 sec), whereas in signature verification RSA takes less time of (0.03 sec) while ECC takes more time (4.53 sec). So the applications which require message verification more often than the signature generation can use RSA asymmetric key algorithm than ECC algorithm. ***Drawbacks*** Following are the drawbacks of asymmetric key encryption ***i***. the length of keys are large and costly. ***ii***. Asymmetric keys are more susceptible to brute force attacks. Asymmetric encryption system also suffers from non repudiation problem as the public key assigned by this system are just the random numbers which does not reveal the identity of user. ***iii.*** In asymmetric key encryption there is involvement of third party known as public key infrastructure (PKI). PKI is vulnerable to many attacks like man in the middle attack etc.

C. *Functional encryption*

Functional encryption is a public key encryption in which decryption key allows a user to learn a function of the encrypted data. Functional encryption allows fine grained access control of data and causes less communication complexity, so it becomes the choice of researchers working in the area of encryption. As shown in figure 1 functional encryption is broadly classified into Attribute based encryption (ABE) and Predicate encryption (PE).

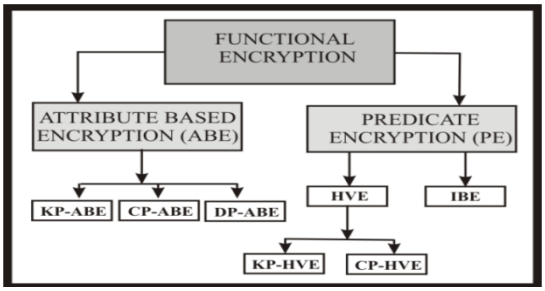

Fig 1: Functional Encryption classification

1) *Attribute based Encryption (ABE)*

Sahai and waters in 2005 [7] proposed an improved IBE scheme and called it *fuzzy IBE* (FIBE). FIBE is the first concept of ABE. In FIBE the message sender can encrypt

DOI 10.17148/IJARCCE.2015.41142

the message to only those users which have certain attributes. Attributes are the crucial entities in ABE scheme. Many versions of ABE scheme have been proposed like KP-ABE, CP-ABE and DP-ABE they are described below.

a. *Key policy attribute based encryption (KP-ABE)*

KP-ABE scheme was proposed by Goyal et al.[8] in 2006. This scheme allows fine grained access on any monotone structures. This scheme is based on decisional bilinear Diffie-Hellmon (DBDH) assumption[9]. In this scheme the secret key is associated with pre accessed structure, user can decrypt the cipher text if attribute set satisfies the access structure given in secret key. KP-ABE scheme is best suited for application like sharing audit log information. As this scheme is designed for monotone access structure so the data owner cannot express the negative attributes to remove the participants with whom the data owner does not want to share. Later on KP-ABE is also designed for non monotone access, in which the secret keys are labelled with a set of attributes using positive and negative attributes. This non monotonic KP-ABE scheme is used to make complex access policies, but this scheme suffers with drawback that the cipher text size grows linearly with the no. of cipher text attributes. Another major drawback in KP-ABE scheme is that the access policy is specified in the secret key, so even the data owner cannot decide who can decrypt the cipher text, he can only set the attributes to control the access of cipher text.

b. *Cipher Policy Attribute based encryption (CP-ABE)*

Bethencourt et al.[10] in 2007 proposed the first CP-ABE scheme. In CP-ABE scheme the user secret key is associated with attributes expressed as strings, whereas the cipher text contains the access structure. So the user will be able to decrypt the cipher text only if his attributes satisfies the access structure criteria. Many versions of CP-ABE scheme has been proposed to make flexible access control policies. Cheung and Newport[11] creates a secure CP-ABE scheme which uses positive and negative attributes with AND gate. This was the first CP-ABE secure scheme developed using DBDH assumption, but it suffers from two drawbacks first it is not sufficiently expressive and second the size of cipher text and secret key increases linearly with no. of attributes. Further improvements were made by Goyal et al.[12] and liang[13], they designed a CP-ABE scheme based on DBDH assumptions and have flexible access structure. They proposed bounded CP-ABE known as BCP-ABE scheme. This scheme supports any access formula in which size is bounded by "and", "or" and "threshold" operation. This scheme also suffers with the limitation that only limited depth access tree structure can be defined. In the year 2011 a new CP-ABE scheme was proposed by Waters [14] using non interactive cryptographic assumptions. In this scheme access structure is expressed by using linear secret sharing scheme (LSSS). The cipher text size and encryption, decryption overhead increases linearly with the access structure. So the scheme does not performed well. Almost all the CP-ABE schemes are constructed from bilinear pairing. Later J. Zhang and J.F. Zhang [15] developed a CP-ABE scheme using q-ary lattices without using bilinear pairing. This scheme provides strong security proofs and it opens the way to create CP-ABE using other assumptions rather than using bilinear pairing. A new CP-ABE scheme was proposed by Zhibin Zhou et al.[16], using a constant size cipher text known as CCP-ABE and attribute based broadcast encryption (ABBE). ABBE has significantly reduces the storage and communication overhead to the order of O(log N), where N is the system size .

c. *Dual Policy ABE (DP-ABE)*

Attrapadung and Mai [17] in 2009 develop a new ABE scheme known as Dual Policy ABE. KP-ABE specifies policies over data attributes and it is useful for content based access control. CP-ABE specifies policies over receiver attribute and useful for access control that directly specifies receiver policies. Advantages of both techniques are combined to form a new approach known as dual policy ABE (DP-ABE).

2) *Predicate Encryption (PE)*

PE *is* a new branch of encryption. The traditional public key or asymmetric key encryption is coarse grained, in which sender encrypt the message with Public Key (PK) and only the owner of unique Secret Key (SK) can decrypt the message. Predicate encryption allows fine grained access control over the decryption keys. In this scheme the owner of the master secret key (Msk) can obtain secret key (Sk*p*) for any predicate *P* from a specified class of predicates P[18]. For encrypting a message m the sender specify an attribute and the resulting cipher text *X* can be decrypted only by using keys Sk*p* such that P($\vec{x}$) = 1[18]. Predicate encryption scheme is an instance of functional encryption. The functional encryption supports restricted secret keys that enable a key holder to learn a specific function of encrypted data but reveal nothing else about data. For example in a given encrypted program the secret key enable the key holder to know only the output of program with specific inputs without telling anything else about the program[19]. Functional encryption is classified into HVE and IBE.

a. *Hidden Vector Encryption (HVE)*

HVE belongs to the class of predicate encryption. HVE scheme allows the use of wildcards in the attributes associated with cipher text [20]. In HVE scheme the cipher text attributes are vectors $\vec{x}$ = (x_1…..x_l) of length l over alphabet $\sum$. keys are associated with $\vec{y}$=(y_1 ….y_l)of length l over alphabet $\sum U \{*\}$ and match($\vec{x}$, $\vec{y}$) predicate is true if and only if for all i, $y_i \neq *$ means $x_i=y_i$[18]. Several HVE schemes have been proposed, most commonly used are key policy based HVE (KP-HVE) scheme and cipher text policy based HVE (CP-HVE) scheme. In KP-HVE wildcard appears in decryption attribute vector in the user secret key, while in CP-HVE

wildcard appears in the encryption attribute vector in cipher text. Jong Hwan Park et al. [20] propose fully secure HVE under standard assumptions and conclude that their scheme requires only O(1) sized private keys and O(1) pairing computations for decryption, as compared to other HVE schemes in which the pairing overhead increases linearly with the access control structure

b. *Identity Based Encryption (IBE)*

In this encryption scheme sender encrypt a message to an identity without accessing his public key certificate, this process simplifies the certificate management procedure and thereby reduces the transmission overhead. In IBE scheme character strings are used as identities. IBE scheme does not require public key encryption certificates, this makes IBE suitable for many practical applications. IBE scheme has an advantage over public key encryption as there is no need of certificate, so recipient's public key can be obtained from user's identity. Key revocation is also not required after the expiry of keys. ***Drawbacks*** IBE scheme requires a centralized server where keys and identities of users are stored. A secure channel is also required between sender and receiver.

IV. COMPARISON OF VARIOUS ENCRYPTION SCHEMES

A. *Comparison of symmetric key encryption and asymmetric key encryption is done on following parameters and shown in table 1*

Sr. no.	***Parameters***	***Symmetric key encryption***	***Asymmetric key encryption***
1	***Avg execution time taken by encryption algo***	Blowfish algo takes min exec time (60.3 ms)	ECC algo takes min time (1.44 sec, 3.07 sec) for key gen and sig gen
2	***Avg execution time taken by decryption algo***	Blowfish algo takes min decryption time (83.4ms)	RSA algo takes min time(0.03 sec) for sig verification
3	***Key size in bits***	256 bits	RSA- 15360 bits ECC- 521 bits

Table 1: A Tabular Comparison of Symmetric and Asymmetric encryption schemes.

1) *Average execution time taken by encryption/decryption algorithm with diff packet size*

In symmetric key encryption blowfish algorithm takes minimum average time for encryption 60.3ms and 83.4ms for decryption as compared to other symmetric key algorithms. In asymmetric key encryption average time taken by ECC algorithm for key generation and signature generation is minimum (1.44 sec, 3.07 sec), whereas for signature verification RSA algorithm takes minimum time of 0.03 sec as compared to ECC algorithm which takes 4.53 sec for signature verification.

2) *Key size in bits*

In symmetric key encryption the key size is 256 bits, whereas in asymmetric key encryption scheme ECC algorithm has key size of 521 bits whereas RSA algorithm has key size of 15360 bits.

B. *Comparison of predicate encryption (IBE & HVE) and Attribute based encryption is done on following parameters and shown in table 2.*

1) *Access Structure*

Previous IBE schemes lack fine grained access control, later on it is provided in hierarchical identity based encryption (HIBE). Still the access control in IBE scheme is limited as the character strings are used as identifiers. In HVE scheme fine grained access control is provided on decryption keys. HVE scheme also allows the use of wild cards, thereby provides much flexible access control. A secure and flexible HVE is also developed which provide security from unrestricted queries and thereby preventing the misuse of wildcards in queries. ABE scheme is developed with both monotone and non monotone access structure, so it provides very flexible environment to the users for fine grained access.

2) *DBDH assumption*

DBDH means decisional bilinear Diffie - Hellman assumption. IBE scheme is not based not DBDH assumption, whereas both the HVE and ABE schemes are build on DBDH assumption.

3) *Key size and Cipher text complexity*

In the earlier IBE schemes key size and cipher text was a critical problem. As user identity is used as a major attribute, so the key size and cipher text increases linearly with increase in identity string. Later on this problem is solved by development of Hierarchical IBE with constant cipher text (HIBE). HVE scheme is better than IBE as it has been proposed with constant decryption key size and short cipher text. So size of the key is not much problematic in HVE scheme. ABE scheme has two main subgroups called KP-ABE and CP-ABE. Key size and cipher text size is a major problem in KP-ABE. Although KP-ABE scheme with non monotonic access structure with constant cipher text size is developed, but the key size is still a challenge as it grows linearly with no of attributes. Many versions of CP-ABE have been proposed to improve the key size and cipher text size. Bounded CP-ABE (BCP-ABE) scheme is one of the subclass of CP-ABE. It has comparatively small key size and cipher text as compared to other proposed schemes.

4) *Computation overhead during encryption, key gen and decryption phases*

Most of the IBE schemes proposed are based on ECC algorithm, which has maximum computational overhead of O ($\log^3 p$). Attribute based broadcast encryption

(ABBE) which is the subgroup of ABE scheme has lowest computational complexity of the order of O (logN), where N is the system size. Secure HVE which is the subset of HVE requires minimum O (1) pairing computations for decryption as compared to other HVE scheme, so HVE has least computational overhead than IBE & ABE.

Sr. no	***Parameters***	***PE***		***ABE***
		IBE	***HVE***	
1	***Access structure***	Fine grained access control is not provided	Fine grained access control is provided	Fine grained access control is provided
2	***DBDH assumption***	IBE is not based on DBDH assumption	HVE is based on DBDH assumption	ABE is based on DBDH assumption
3	***Key size and cipher text complexity***	key size is large but constant cipher textQ is found in HIBE	HVE has Constant decryption key size and short cipher text	ABE has Small key size and cipher text
4	***Computation overhead during encryption, key gen and decryption phases***	Computational overhead is more in IBE than HVE & ABE $O(\log^3 p)$	Secure HVE has minimum computational overhead of O(1)	ABBE has computational overhead of O(logN)
5	***Efficiency***	Efficiency of IBE is good, as both bilinear pairing operation and lattice theory is used.	HVE is less efficient, as only bilinear pairing operation is used.	Efficiency of ABE is good, as both bilinear pairing operation and lattice theory is used.

Table 2: A Tabular Comparison of PE and ABE Scheme

5) *Efficiency*

IBE and ABE scheme are proposed using bilinear paring operation and lattice theory also, so efficiency of IBE and ABE is better than HVE which is proposed only using bilinear pairing operation.

V. CONCLUSION

In vehicular networks so far a lot of work is being done on authentication using public key encryption and functional encryption techniques. Previously public key encryption was used widely but it suffers with the problem of *key revocation and non repudiation*, so functional encryption is used in vehicular communication to avoid these problems. So two separate comparison tables has been made which draws following conclusions

- A comparison of symmetric and asymmetric key encryption reveals that asymmetric encryption using RSA algorithm, can be used for authentication in vehicular communications (VC). In VANET authentication process is required more often, therefore during vehicular communication signature verification algorithm is used quite frequently than key generation and signature generation algorithms. As RSA algorithm takes less time (0.03 sec) than ECC algorithm (4.53 sec), so RSA algorithm is well suited for authentication process in VANET.

- IBE and HVE are subclasses of Predicate encryption (PE). Earlier for authentication in VANET IBE scheme is used, but it suffers with many vulnerabilities which has been discussed in the paper. HVE scheme which is another subclass of PE is never used in VANET for authentication and it has properties comparable to ABE, so instead of IBE HVE can be used for authentication in VC.

REFERENCES

[1] S. Al-Sultan, M. M. Al-Doori, A. H. Al-Bayatti, and H. Zedan, 'A comprehensive survey on vehicular Ad Hoc network', *J. Netw. Comput. Appl.*, vol. 37, no. 1, pp. 380–392, 2014.

[2] M. N. Mejri, J. Ben-Othman, and M. Hamdi, 'Survey on VANET security challenges and possible cryptographic solutions', *Veh. Commun.*, vol. 1, no. 2, pp. 53–66, 2014.

[3] D. S. A. Elminaam, H. M. A. Kader, and M. M. Hadhoud, 'Performance Evaluation of Symmetric Encryption Algorithms', *Commun. IBIMA*, vol. 8, no. 8, pp. 58–64, 2009.

[4] S. Farah, M. Y. Javed, A. Shamim, and T. Nawaz, 'An experimental study on Performance Evaluation of Asymmetric Encryption Algorithms', in *Recent advaces in information science*, 2012, vol. 8, pp. 121–124.

[5] M. Alimohammadi and A. A. Pouyan, 'Performance Analysis of Cryptography Methods for Secure Message Exchanging in VANET', *Int. J. Sci. Eng. Res.*, vol. 5, no. 2, pp. 911–917, 2014.

[6] N. Jansma and B. Arrendondo, 'Performance comparison of elliptic curve and RSA digital signatures', 2004.

[7] A. Sahai and B. Waters, 'Fuzzy Identity-Based Encryption', *EUROCRYPT 2005, Proc. 24th Annu. Int. Conf. Theory Appl. Cryptogr. Tech.*, pp. 457–473, 2005.

[8] V. Goyal, O. Pandey, A. Sahai, and B. Waters, 'Attribute-based Encryption for Fine-grained Access Control of Encrypted Data', *Proc. 13th ACM Conf. Comput. Commun. Secur.*, pp. 89–98, 2006.

[9] J. Bethencourt, A. Sahai, and B. Waters, 'Ciphertext-Policy Attribute-Based Encryption', in *2007 IEEE Symposium on Security and Privacy (SP '07)*, 2007, pp. 321–334.

[10] L. Cheung and C. Newport, 'Provably secure ciphertext policy ABE', in *Proceedings of the 14th ACM conference on Computer and communications security CCS 07*, 2007, pp. 456–465.

[11] V. Goyal, A. Jain, O. Pandey, and A. Sahai, 'Bounded ciphertext policy attribute based encryption', *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 5126 LNCS, no. PART 2, pp. 579–591, 2008.

[12] X. Liang, Z. Cao, H. Lin, and D. Xing, 'Provably secure and efficient bounded ciphertext policy attribute based encryption', in *Proceedings of the 4th International Symposium on Information, Computer, and Communications Security - ASIACCS '09*, 2009, pp. 343–352.
[13] B. Waters, 'Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization', *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 6571 LNCS, no. subaward 641, pp. 53–70, 2011.
[14] J. Zhang and Z. Zhang, 'A Ciphertext Policy Attribute-Based Encryption Scheme without Pairings', in *Information Security and Cryptology (ISC '12)*, 2012, pp. 324–340.
[15] Z. Zhou and D. Huang, 'On Efficient Ciphertext-Policy Attribute Based Encryption and Broadcast Encryption', *Proc. 17th ACM Conf.*, pp. 753–755, 2010.
[16] N. Attrapadung and H. Imai, 'Dual-Policy Attribute Based Encryption', in *Applied Cryptography and Network Security*, 2009, pp. 168–185.
[17] A. De Caro, V. Iovino, and G. Persiano, 'Fully Secure Hidden Vector Encryption', in *Pairing-Based Cryptography – Pairing 2012*, 2012, pp. 102–121.
[18] D. Boneh, A. Sahai, and B. Waters, 'Functional encryption: Definitions and challenges', *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 6597 LNCS, no. subaward 641, pp. 253–273, 2011.
[19] T. V. X. Phuong, G. Yang, and W. Susilo, 'Efficient Hidden Vector Encryption with Constant-Size Ciphertext', in *Computer Security - ESORICS*, 2014, pp. 472–487.
[20] J. H. Park, K. Lee, W. Susilo, and D. H. Lee, 'Fully secure hidden vector encryption under standard assumptions', *Inf. Sci. (Ny).*, vol. 232, pp. 188–207, 2013.

BIOGRAPHIES

Ms. Sandhya Kohli obtained her M.Tech (IT) from MM University Mulana in 2009. She has attained second position in merit during her M.Tech in university. She has worked in many reputed colleges and having 9 years of teaching experience. She has authored many research papers in various journals. She has participated in many conferences FDP's and STC's. Presently she is doing her Ph.D(CSE) from Punjab Technical University. Her areas of interest are: Ad-hoc networks, Linux, Simulation, DBMS and Cloud computing.

Dr. Kanwalvir Singh Dhindsa is working as Associate Professor in the department of CSE & IT at Baba Banda Singh Bahadur Engg. College, Fatehgarh Sahib (Punjab). He obtained his Ph.D in Computer Engg. (In the field of Information Systems and Mobile Computing), and also M.Tech. degree from Punjabi University, Patiala (Pb). He has been awarded with the 'Best Ph.D. Thesis Award' in International conference held in association with Computer Society of India (CSI) at COER, Roorkee (Uttarakhand) in Nov. 2014. He has guided more than 20 M. Tech. students and is currently guiding 8 PhD scholars. He has authored more than 50 publications in various esteemed International journals and proceedings of national and international conferences. He has reviewed several referred journals of national and international repute such as IJCSIS (USA), JECR (USA), IJCTE(Singapore), JAIT of Academy Publisher (Finland), IJCA (USA) and IAENG International Journal of Computer Science

Dr. Ravinder Khanna studied his B.Tech, M.Tech and Ph.D. in Electronics and Communication Engineering from Indian Institute of Technology Delhi. He served in the Indian Air Force for twenty

DOI 10.17148/IJARCCE.2015.41142