An Efficient Hop-by-Hop Message Authentication Scheme and Secure Location Privacy in Wireless Sensor Networks

Uma Meena, Anand Sharma

Abstract - Wireless sensor network in recent days affected with two main research problem such as message authentication and location privacy. This paper present an Elliptic Curve ElGamal Signature Algorithm scheme (ECESA) for message authentication and Euclidean Zigzag Bidirectional Tree (EZBT) for location privacy of both source and sink. ECESA involves three phase: (i) private and public key generation using Elliptic Curve Cryptography (ECC), (ii) ElGamal signature arrangement for effective message encryption and (iii) matching the decrypted result with MD5 hash value for authentication of the authorized person. The most important privacy preserving techniques are the EZBT to send the messages either sink to source or from source to sink with the location privacy scheme. On account of this, the proxy source and sink is selected while using the Euclidean distance technique. Finally, the efficiency of the work has been demonstrated through the simulation results of location privacy and message verification. Then the performance are validated in terms of quality of service (QoS).

IndexTerms - Elliptic curve cryptography, ElGamal encryption, MD5 hash algorithm, location privacy, Euclidean distance, Zigzag bidirectional tree

1. INTRODUCTION

The message authentication scheme plays an important role in the sensor network, in which the modified messages are detected through the receiver side and then send a message to the sender [1]. This can be otherwise named by data origin authenticity, where the integrity of the message is checked out with the corresponding scheme. While doing this, any extra characters and changes bits are not included in this [2]. Location privacy is the major defects in the sensor networks, and it is classified as source and sink location privacy. Both these schemes can prevent from the adversaries of source and sink.23yj

The distinctive features of wireless sensor networks (WSN) is the low bandwidth, energy, and computational complexities, the foremost constraints of security because of safe the private information [3-6]. By this way the huge amount of sensor nodes may deploy the attacks, and those can be prevented by numerous way which is explored. The WSN domain can claims for suitable applications such as military, and health monitoring system, for that lightweight authentication schemes are explored along this [7]. To provide security, and special authorization of receiver or sender through the encryption [8].

Due to the nature of WSN have numerous security task such as resource, lack of static infrastructure, communication, topology for deployment, sensor node limitation and unknown network [9]. Although this authentication scheme can avoid the unwanted messages, and provide the secured messages. Though these can offer declarations about the original messages, validate the type of messages, and integrity [10-13]. The message legitimacy, and the integrity is provided through the projection of various authentication schemes. The mechanism of cryptography have certain limitations alike communication overhead, scalability, computational task, and compromise attacks [14].

Authentication comes into the problem for the reason that through security codes in each node will authenticate with the additional node [15]. As WSN, in this surveying region where most of the surveying regions were deployed. We consider it as a mesh topology because it is difficult to authenticate every mote [16, 17].The efficient ways of public key cryptography is included in this section to secure the vulnerable data.So much of encryption schemes alike Ron Rivest, Adir Shamir, Das protocol,anddiffie-helman algorithm. The smart card and the hashing functions are the dynamic user authentication protocols, which is obtained through the gate way [18].

The authentication schemes play very well to compromise the nodes, access the data and from corrupt the data. The systematic symmetric and public key approaches are used to solve the problems of encryption, and provide efficiency in terms of memory and the computation. The messages are able to pass from one node to another with the inadequate energy, and memory, in which the safe regarding problems may be rectified through hop- hop- message authentication protocols.Elliptic Curve ElGamal Signature Algorithm (ECESA) is established to solve scalability and computation complexity.So the major issue in WSNs is location privacy of both the source and sink. In order to concurrently overcome the security threat occurrences and location privacy of both source and sink, the Euclidean Zigzag Bidirectional Tree (EZBT) algorithm is currently used.

2. RELATED WORKS

Some of the recent works related to the message authentication and location privacy wireless sensor networks is listed below,

Revised Manuscript Received on December 22, 2018.

Uma Meena, Research Scholar, College of Engineering and Technology, MUST, Lakshmangarh, Rajasthan, India. (e-mail:umameenaphd@gmail.com)

Anand Sharma, Assistant Professor, College of Engineering and Technology, MUST, Lakshmangarh, Rajasthan, India

The authentication scheme plays a vital role of WSN to protect the data being from corrupted, and unauthorized. Various systematic approaches had been established over past years. The scalability, and the reliability of the nodes are maintained through the authentication schemes, and it is computationally high, communication overhead. Recent days, the polynomial based approach has been evaluated, to rectify the degree of polynomial, in which the threshold is set. The amount of transmitted messages is above the threshold value then the adversary nodes can catch the messages, it should be within the limits of threshold level.

The scalable authentication based elliptic curve cryptography (ECC) is proposed by Li et al. [19]. If the entire network is suffered by the intermediate nodes, then the proposed approach was able to withstand the condition and transmit much more information in the unpredictable manner. By theoretical and the simulation analysis, the proposed approach has the greater confidence in terms of communication overhead, and computational. In addition, the message source privacy is delivered by this scheme.

The hop by hop message authentication schemes are vulnerable for the privilege attacks such as accelerating, and Denial of service (DoS). The vulnerability of the authentication haddevelopedby Ren et al. [20]. The location aware end to end security was the outline of the work and each nodes were store the secret keys. The key management frame work establish the route for authentication alike node-to- node or node- to- sink. This was the most attractive way to focus on the Daniel of service attack.

The WSN is used for the purpose of monitor the environmental condition such as humidity, and temperature etc. The cost and the power is the major complication in the presence of work, where the broad casting based protocols, and public key cryptosystem is not applicable. The source-location based information leakage beyond the limits are proposed by Li et al. [21].The routing was provided through the Network Mixing Ring (NMR) and Randomly Designated Intermediate Node (RSIN). The obtained results from the simulation environment tells that the packet delivery ratio, which is highly efficient.

The major concept behind the wireless sensor network was the communication overhead, and it were satisfied through some sensor resource constraints. The network lifetime along with the communication overhead was highly demonstrated through the data aggregation. The final results of that techniques was the crucial way to establish those kind of methods in efficient manner. The data protection was enhanced through the developed method of Energy-Efficient and High-Accuracy (EEHA), and it had been established by Li et al. [22].

The open challenges in the sensor networks was the severe threat, error at upper level, and energy wastage, this was done at the side of sink, and end of the nodes. The false data had been analysed by Lu et al. [23]. The above problems were rectified by bandwidth-efficient cooperative authentication (BECAN) scheme. The small portion of the error data was checked out through the sink in order to protect the sink from diminishing.

3. PROPOSED ECESA-EZBT METHODOLOGY

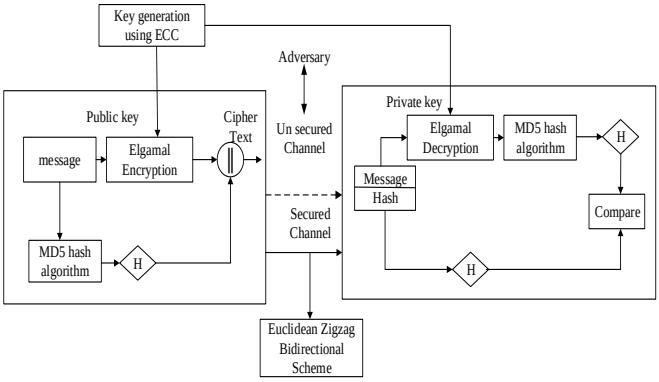

Figure 1:Schematic representation of the proposed method

The Elliptic Curve ElGamal Signature Algorithm scheme (ECESA) based on Euclidean Zigzag Bidirectional Tree (ZBT) is proposed to transfer the text information along with the cipher key. Thesystematic way of the proposed methodology is shown in fig.1, in which H signifies the hash function and embodies the concatenation operator. The ECESA includes three main features alike Elliptic Curve Cryptography (ECC), MD5 hash algorithm for confirming the authorized person and effective message encryption using ElGamal signature method. The location privacy, i.e., the concealment of the location of either source or sink, or otherwise both, is a kind of contextual privacy. To deliver messages from source to sink, the projected method introduces Euclidean Zigzag Bidirectional Tree (EZBT) to address the prominence of location privacy of both the source and sink, in which it can protect the end-to-end location against from eavesdropper. However, in this zigzag bidirectional tree arrangement, either proxy source or proxy sink are adopted in which location of the source or sink easily prevents from the challenger. Zigzag bidirectional scheme is not possible while it is selected randomly and even if the proxy source and sink are near to source and sink. By using Euclidean distance method, we can overcome the drawback of selection process of the proxy source and sink.

Problem definition and Objective

WSN is embraced of many sensor nodes and a sink node among which the packets are delivered from the source to sink node. It is the major role for the location privacy of sources and sink concurrently since the adversary pursues to breach the location privacy of a source or sink in the network and the WSN is hypothetically endangered by a particular adversary. The adversary cannot admittance the content for the motive that we assume that each message conveyed in the network is encrypted. To detect either source (or sink) by examining the traffic flow and tracing back (or forth) hop-by-hop and thus local opponent is condensed. So the main impartial of our work is to afford well-organized computational and communication overhead for plentiful equivalent security levels while providing message concealment and to attain a high security period with a low end-to-end latency and energy consumption.

3.1. ECESA Message Authentication

The authentication of hop-by-hopmechanism is held on with the Elliptic curve ElGamal signature (ECESA) For sending a message from source to destination there are three phases or steps are present

Step 1: ECC Key Generation Phase

For the message authentication, the first step of key generation phase is to be an elliptic curve cryptography, which says that the real numbers over the elliptic field (E) is said to be $y^2 = x^3 + sx^2 + t^2$. The curve along with the point P holds the value of prime integer. If the elliptic condition alike $4s^3 + 27t^2 \neq 0$ is satisfied by the terms of s and t then the roots replica is avoided. The curve depend equation are proposed to find out the elliptic curve elements over the prime field. The equations are now modified as $\left(y^2 = x^3 + sx^2 + t^2\right)_{\mathrm{mod}\,P}$ and $\left(4s^3 + 27t^2\right)_{\mathrm{mod}\,P} \neq 0$.

$$R = \left\{(x, y) : \left(y^2 = x^3 + sx^2 + t^2\right)_{\mathrm{mod}\,P}\right\} \cup \{\infty\} \quad (1)$$

An elliptic group $E_P(s,t)$ is formed for quadratic residues $Z_p = 1, \cdots p-1$.

There are some of the basic operations which can be used in the ECC using the scalar multiplication can be given as,

Addition

Assume $X(j_1, k_1), Y(j_2, k_2) \in R(k)$ and the point on the elliptic curve is E, where $X \neq Y$ .Then $Z + W = (j_3, k_3)$ In which $j_3 = \left(\frac{k_2 - k_1}{j_2 - j_1}\right)^2 - j_1 - j_2$ and $k_3 = \left(\frac{k_2 - k_1}{j_2 - j_1}\right)^2 (j_1 - j_3) - k_1$

Doubling

Assume $X(j_1, k_1) \in R_Q(s,t)$ and the point on the elliptic curve is E, where $X \neq -X$. Then $2X = (j_3, k_3)$ In which $j_3 = \left(\frac{3j_1^2 + s}{2k_1}\right)^2 - 2j_1$ and $k_3 = \left(\frac{3j_1^2 + s}{2k_1}\right)^2 (j_1 - j_3) - k_1$

Multiplication

Let the point on the elliptic curve (X) be Q. Then, the point multiplication of the point Q is represented as repeated addition. $XQ = Q + Q + \cdots Z\,times$.

Public, private keys generation

The communication from the sender side to the receiver over the communication channel is provided through the elliptic curve and it is to be $E_p(s,t)$ where p is a prime number and a random point Z on the elliptic curve. From the range [1, p-1], the sender chooses a large random number α. Sender computes $\beta = \alpha X$ as their public key. The public key are (P, X, β) and the private key as α. While conveying the message the sender sends the public key along with the cipher text.

Step 2: ElGamalEncryptionand Decryption phase

An objective of this segment is to designate how we can change this hard problem (the ECDLP) into a Public Key Cryptography system. It was self-sufficiently extended from the standard ElGamal system by Neal Koblitz and by Victor Miller and the scheme obtainable here is recognized as the Elliptic ElGamal arrangement.

In the Elliptic ElGamal scheme, a point which has large order, publicly indicate an Elliptic Curve and a Finite Field demonstration is elected to communicate in a secure manner. Only the person with the private key α will be capable of regaining the original message and in the encryption procedure in Elliptic ElGamal consists of generating a pair of cipher texts, which is a point on the chosen elliptic curve. In order to calculate $C_1 = M + k\beta$, the first cipher text C_1 is created by taking the message point M that one would like to send and taking a random large value k. The receiver must be able to deduct $k\beta$ from C_1 to recuperate the message M. The foremost problem is eavesdropper would be able to decode the message easily therefore k cannot be sent by itself. For decoding C_1, the receiver actually wants $k\beta$ value and $k\beta = k(\alpha P) = \alpha(kP)$. The receiver could use their secret value α to calculate $\alpha.C_2$ and subtract this from C_1 then they will recover the value M, that's why we sent the value $C_2 = kP$ (which we are assuming does not reveal k).

In summary, encryption is done by randomly generating k and then calculating:

$$C_1 = M + k\beta \quad (2)$$

$$C_2 = kP \quad (3)$$

At the same time of encryption, the sender able to find the signature for message using MD5 hash functions as H. Then the cipher text can be obtained as,

$$CT = (C_1, C_2) \| H \quad (4)$$

When the sender wants to transmit the message to the receiver, it will send the cipher text CT and the public key (P, Z, β).

After the receiver has the values c1 and c2, receiver may undo the decryption by calculating:

$$M = C_1 - \alpha C_2 = M + k\beta - \alpha kP = M + (k\alpha)P - (k\alpha)P$$

Thus, we can decrypt the cipher text to plain text.

Step 3: Verification phase

Finally to validate the authorized person, the hash function for the decrypted message is compared with the original message.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

3.2. Euclidean Zigzag Bidirectional Tree (EZBT) based location privacy

Due to the open nature of wireless communication, privacy is one of the most significant complications and it creates very easy for adversaries to eavesdrop. Mechanisms must be in place to secure a WSN when organized in critical applications. The source-location privacy problem is how to secrete a source of messages from an eavesdropper, which is serious for applications where the position of an event is significant. For example, we consider enemy troops in battlefields and a sensor network monitoring our troops. They can locate and attack our troops by when enemy troops can assay the location of our troops from the wireless signals of the sensor network. The significant matter for sensor network is the sink-location privacy difficult is how to secrete the destination (a sink node in general) of messages from an eavesdropper where survival of the network is significant. For example, the physical attacks of the network are limited by a sensor network monitoring. Enemies can try to abolish the sink node to break down the complete network whether they can estimate which node is a sink node.

If the proxy sink is adjacent to the source then the zigzag bidirectional arrangement [24] will be unacceptable and that proxy source will also away from the sink then it also necessary. Eavesdropper cannot identify the exact location of original source when the presence of difficulties over the distance between source and proxy sink. In this paper, the problem of an existing method is avoided by the Euclidean distance based method to find the proxy source and proxy sink.

Proxy node (Source, sink) selection

In the proposed scheme, first we have to estimate the average distance per hop in the network dhop, then the proxy source and sink nodes can be selected based on the distance using Euclidean distance method.

The objective of the selection of proxy source and proxy sink is given as,

$$F(x) = \max(D(X,V)) \qquad (6)$$

The Euclidean distance given in eqn. (7) used to calculate the distance of the specific node to its all neighbouring nodes.

$$D(X,V) = \|X - V\|^2 \qquad (7)$$

In the above equation is the source or the destination node and is the neighbouring of all the other nodes.

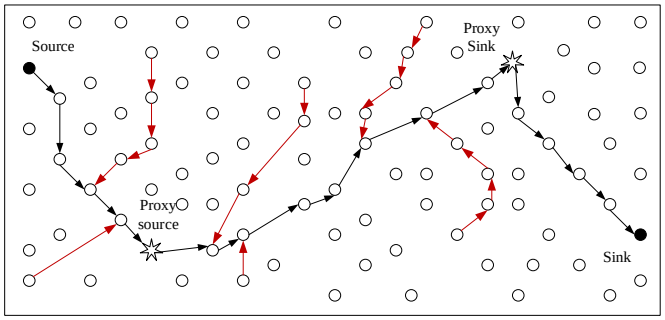

Figure 2:Euclidean Zigzag Bidirectional Tree (EZBT) method

The pictorial illustration of the Euclidean Zigzag Bidirectional Tree scheme is given in fig.2. The message travel in three segments based on the EZBT in which both proxy nodes are added between the source and sink. The methods are given below.

(i) From the proxy source to the proxy sink,
(ii) From the source to the proxy source,
(iii) From the proxy sink to the real sink.

In this outline the adversary deliberates the proxy sink as original sink and the proxy source as original source. To safeguard the original sender and receiver, we deliberate the proxy adversary as source and proxy servers as sink. Thus the security of source and sink as the active technique.

4. SIMULATION RESULTS

The location privacy is maintained through the hop-by-hop authentication scheme which is works under the basis of elliptic curve cryptography, and the developed methods are implemented in the working platform of MATLAB. Finally the comparison results are made over the performance, metrics such as computational overhead, packet delivery ratio, and communication overhead. Overall the proposed approach has been compared with the existing Zigzag bidirectional scheme to show the proposed scheme is the look forward one than from others.

4.1. Simulation Environment

The simulation environment has the 100 nodes which is dispersed in the entire network, in which the nodes contain certain frequency range of B = 1 Mbit/s, and firmware character energy consumption x_{elec} and energy dissipation during transmission λ_{amp} is set as 10×10^{-9} J/bit and 130×10^{-12} J/bit/m^2, correspondingly. Additional simulation parameters are listed in Table 1.

Table 1: Simulation Parameters

Parameter	Value
Total number of nodes	100
Deployment Area	50m×2500m
Source and sink Node	1
Transmission distance	100m
Packet Sending Rate	1 packet/sec
Size of the packet	160 bit
Initial energy of the node	50mJ

4.2. Performance Evaluation

Packet delivery ratio (PDR)

It is the ratio of total number of packets transmitted by the transceiver, and it is matched by the receiver.

End-to-end delay:

End-to-end delay is denoted as the time taken for a packet to be transmitted across a network from source to destination.

Communication overhead:

The proportion of energy dissipated to the sum of transmitted and received energy as the communication overhead.

Computational overhead:

It is referred as the proportion of sum of transmitted time and received time to the total computational time.

Transmission delay:

It is deliberated as the distance and the time taken for the transmission between the hop.

Energy consumption:

Energy consumption is mentioned as the quantity of energy taken for the processing and transmission of packets.

The experimental results of the proposed method in terms of end to end delay, communication overhead, computational overhead, packet delivery ratio, transmission delay and energy consumption is given in fig. 3-8.

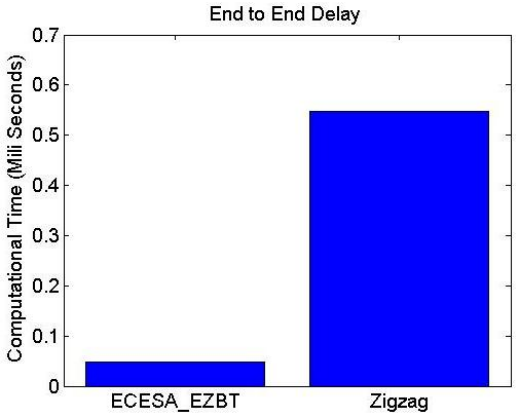

Figure 3: comparison of End-to-end delay

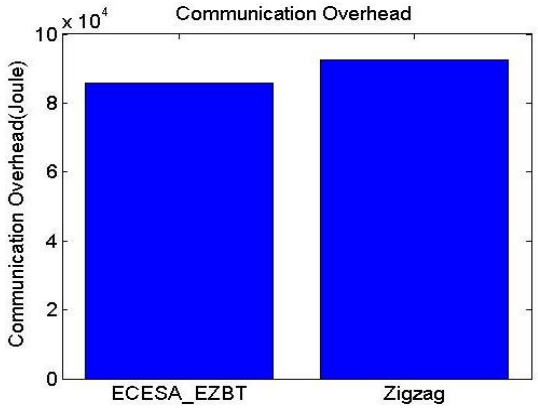

Figure 4:comparison of communication overhead

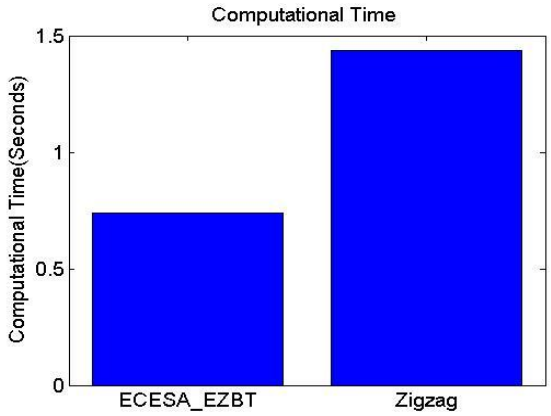

Figure 5: comparison of computational overhead

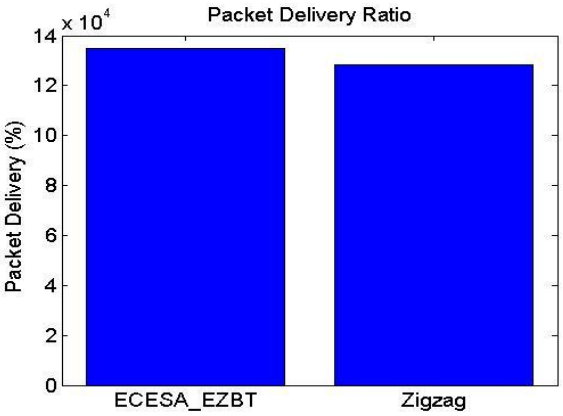

Figure 6: comparison of packet delivery ratio

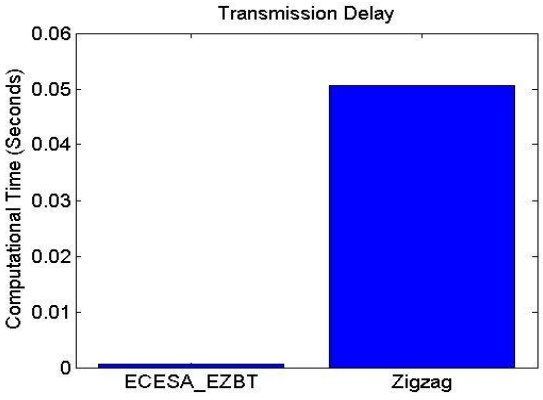

Figure 7: comparison of transmission delay

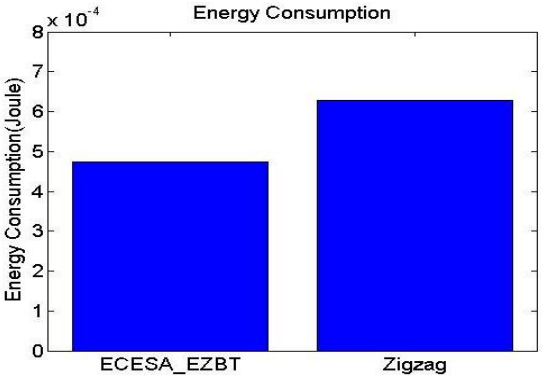

Figure 8: comparison of energy consumption

The comparison results in the figure 3, 4, 5, 7 and 8 reveals that the end-to-end delay, communication overhead, computational overhead, transmission delay and energy consumption of our proposed method get reduced. Then the packet delivery ratio in figure 6 will get increased for the proposed technique when compared with the conventional Zigzag. Thus the experimental results from the comparison chart shows the improved performance for the proposed ECESA_EZBT than the ZBT.

5. CONCLUSION

In this paper, a new authentication scheme is developed using the Elliptic Curve ElGamal Signature Algorithm based on Euclidean Zigzag Bidirectional Tree (ECESA_ EZBT). ECESA method is more efficient with the key size and more secure to security threat attacks. Then, Location privacy is a critical issueover the source and sink nodes. The spate location privacy (Either source or sink) is the Previous research. In this paper, Euclidean zigzag bidirectional tree is used to overcome the security threat attacks and location privacy of both source and sink simultaneously. Hence our proposed method simulation result provides improved performance.

REFERENCES

1. D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in In proceedings of Eurocrypt, 2004, pp. 506–522.
2. B. Waters, D. Balfanz, G. Durfee, and D. K. Smetters, "Building an encrypted and searchable audit log," in Network and Distributed System Security Symposium, 2004.
3. M. Ding, F. Gao, Z. Jin, and H. Zhang, "An efficient public key encryption with conjunctive keyword search scheme based on pairings," in IEEE International Conference onNetwork Infrastructure and Digital Content, 2012, pp. 526–530.
4. F. Kerschbaum, "Secure conjunctive keyword searches for unstructured text," in International Conference on Network and System Security, 2011, pp. 285–289.
5. C. Hu and P. Liu, "Public key encryption with ranked multi-keyword search," in International Conference on Intelligent Networking and Collaborative Systems, 2013, pp. 109 113.
6. Z. Fu, X. Sun, N. Linge, and L. Zhou, "Achieving effective cloud search services: multi-keyword ranked search over encrypted cloud data supporting synonym query," IEEE Transactions on Consumer Electronics, vol. 60, pp. 164–172, 2014.
7. C. L. A. Clarke, G. V. Cormack, and E. A. Tudhope, "Relevance ranking for one to three term queries," Information Processing and Management: an International Journal, vol. 36, no. 2, pp. 291–311, Jan. 2000.
8. H. Tuo and M. Wenping, "An effective fuzzy keyword search scheme in cloud computing," in International Conference on Intelligent Networking and Collaborative Systems, 2013, pp. 786–789.
9. M. Zheng and H. Zhou, "An efficient attack on a fuzzy keyword search scheme over encrypted data," in International Conference on High Performance Computing and Communications and Embedded and Ubiquitous Computing, 2013, pp. 1647 1651.
10. S. Zittrower and C. C. Zou, "Encrypted phrase searching in the cloud," in IEEE Global Communications Conference, 2012, pp. 764– 770.
11. Y. Tang, D. Gu, N. Ding, and H. Lu, "Phrase search over encrypted data with symmetric encryption scheme," in International Conference on Distributed Computing SystemsWorkshops, 2012, pp. 471–480.
12. H. Poon and A. Miri, "An efficient conjunctive keyword and phrase search scheme for encrypted cloud storage systems," in IEEE International Conference on Cloud Computing, 2015.
13. "A low storage phrase search scheme based on bloom filters for encrypted cloud services," to appear in IEEE International Conference on Cyber Security and Cloud Computing, 2015.
14. H. S. Rhee, I. R. Jeong, J. W. Byun, and D. H. Lee, "Difference set attacks on conjunctive keyword search schemes," in Proceedings of the Third VLDB International Conference on Secure Data Management, 2006, pp. 64–74.
15. K. Cai, C. Hong, M. Zhang, D. Feng, and Z. Lv, "A secure conjunctive keywords search over encrypted cloud data against inclusion-relation attack," in IEEE International Conference on Cloud Computing Technology and Science, 2013, pp. 339–346.
16. Y. Yang, H. Lu, and J. Weng, "Multi-user private keyword search for cloud computing," in IEEE Third International Conference on
17. Cloud Computing Technology and Science, 2011, pp. 264–271.
18. C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, "Secure ranked keyword search over encrypted cloud data," in International Conference on Distributed Computing Systems, 2010, pp. 253–262.
19. M. T. Goodrich, M. Mitzenmacher, O. Ohrimenko, and R. Tamassia, "Practical oblivious storage," in Proceedings of the Second ACM Conference on Data and Application Security and Privacy, 2012, pp. 13–24.
20. B. Chor, O. Goldreich, E. Kushilevitz, and M. Sudan, "Private information retrieval," in Proceedings of the 36th Annual Symposium on Foundations of Computer Science, 1995, pp. 41–50.
21. S. Ruj, M. Stojmenovic, and A. Nayak, "Privacy preserving access control with authentication for securing data in clouds," in Proceedings of the 2012 12th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing, 2012, pp. 556 563.