ISSN NO. 2320-5407

Journal homepage: http://www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH

RESEARCH ARTICLE

National Symposium On Emerging Trends In Computing & Informatics, NSETCI 2016, 12th July 2016,Rajagiri School of Engineering & Technology, Cochin, India.

A Detailed Study on Public Key Cryptographic Primitives for Securing Publish/Subscribe Systems.

***Antu Raj S and Sangeetha Jose**
Department of Information Technology,Government Engineering College, Idukki.

Manuscript Info *Abstract*

Key words:
Pub/Sub,
Security,
Confidentiality,
Authenticity,
Public key Cryptography

The publish/subscribe (pub/sub) system is one of the most promising communication paradigm for integration of information systems. It is difficult to provide security mechanisms like authenticity and confidentiality in content based publish/subscribe system. Authenticity is hard to achieve in pub/sub system due to one of its characteristics, de-coupling in time between publishers and subscribers. Furthermore, traditional mechanisms used for encrypting whole message and thus provide confidentiality conflicts with content based routing paradigm. This paper investigates the merits and possibility of different types of public key cryptographic primitives for providing security to publish/subscribe systems. Hence we perform detailed study on different types of public key cryptographic primitives.

Introduction:-

Publish/Subscribe system is a communication paradigm which is used for disseminating events or information through the distributed systems on wide area networks. It is one of the most popular communication paradigms in use. There are two types of participants for communication: Publishers and Subscribers. The one who submit information or events to the system is called as publishers where as the one who express their interest in certain type of information is termed as subscribers. The growing attention towards publish/subscribe systems are because of the characteristics of pub/sub system. The main characteristics are decoupling in time, decoupling in flow and anonymity. In pub/sub model subscribers did not receive all the messages published. They only get a subset of published messages. The process of selecting messages for processing called filtering. There are mainly two types of filtering. Content Based and Topic Based. In Topic Based, messages are published to topics or named logical channels. Subscribers in this will receive all messages published to topics which they subscribe and all subscribers in topic will receive same messages. In much pub/sub system, the publisher submits the information to an intermediate message broker which acts as an event bus between publisher and subscribers. Publishers normally submit the events to the broker, and subscribers communicate with the broker for subscribing the messages that is published by the publisher. Broker in a pub/sub paradigm normally perform store and forward function. They store the published events and eventually forward it to the subscribers. In some recent pub/sub systems publishers and subscribers communicate without the help of any intermediate broker. They organize themselves in a routing infrastructure which does not require the support of intermediate broker and thus forms an event forwarding overlay.

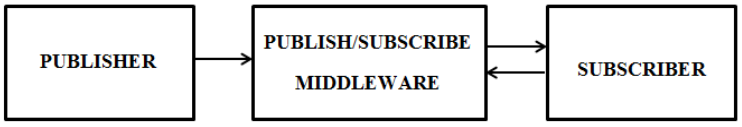

Figure 1. Publish/Subscribe System

Content Based broker less publish/subscribe system is thus an effective communicative paradigm for disseminating information. Content-based publish/subscribe is the most expressive subscription model, where subscriptions define

restrictions on the message content. Since there is wide variety of applications, publish/subscribe needs to provide mechanisms to fulfill the basic security demands of these applications such as access control and confidentiality.

Traditional methods for providing security like public key infrastructure is not applicable in content based publish/subscribe system. Traditional Public Key Infrastructure (PKI) needs end-to-end authentication to provide security to a system. However one of the main characteristics of publish/subscribe system is the loose coupling between publisher and subscriber. Hence end-to-end authentication can't be applied because of these characteristics. Moreover, for encrypting the messages in PKI the publisher need to know the public key of subscribers and subscribers should know the public keys of publishers to verify the authenticity of events which is not possible. Furthermore to provide confidentiality as per traditional mechanisms the whole message should be encrypted. However it conflicts with the content based publish/subscribe paradigm.

Hence a new mechanism is needed to provide security in content based routing paradigm. The mechanism should send encrypted events to subscribers without knowing their subscriptions and it should allow the publishers and subscribers mutually authenticate without knowing each other. A study is conducted based on the mechanisms which addresses the security threats in the broker-less content based publish/subscribe system.

The paper is organized as follows section 2 depicts aboutthe related works. Section 3 discusses about the study on different types of public key cryptographic primitives. The conclusion is given in Section 4.

Related Works:-

Pub/Sub is the most promising application level communication paradigm for integration of information systems. It provides a useful platform for delivering data (events) from publishers to subscribers in an anonymous fashion in distributed networks.

In [30], Jean et al. proposed methods for securing publish/subscribe systems. This is done by specifying and enforcing access control policy at the service API(Application Protocol Interface), and secondly by enforcing the security and privacy aspects of these policies within the service networks itself. Finally, it describesan alternative to whole-message encryption which is appropriate for highly sensitive and long-lived data destined for specific domains with varied requirements. However this system relies on broker network.

Notification as well as subscription confidentiality in publish subscribe systems is addressed by C. Raiciu and S. Rosenblum in [31].It presented a formal security model and analysed the general confidential content based publish/subscribe systems(C-CBPS) problem pointing out its inherent limitations. It provides security techniques that allow content-based routing for the large majority of applications occurring in practice. It describes about two novel protocols that support range mechanisms in C-CB but can also appliedin other areas, such as privacy preserving range matching.

Event Guard - a framework for building secure wide area pub-sub systems is presented in [32]. The Event Guard architecture is comprised of three key components:
1) A suite of security guards that can be seamlessly plugged-into a content-based pub-subsystem
2) A scalable key management algorithm to enforce access control on subscribers
3) A resilient pub-sub network design that is capable of scalable routing, handling message dropping-based denial of service(DoS) attacks and node failures.

The design of Event Guard mechanisms aims at providing security guarantees while maintaining the system's overall simplicity, scalability and performance metrics. Here describes the implementation of the Event Guard pub-sub system to show that Event Guard is easily stackable on any content-based pub-sub core. It also described the two key components of Event Guard. The first component is a suite of security guards that secure the basic publish and subscribe operations from DoS attacks and unauthorized reads and writes. These guards can be plugged-into a wide-area content-based pub-sub system in a seamless manner. The second component is a resilient pub-sub network design that is capable of providing secure and yet scalable message routing, countering message dropping based DoS attacks.

Table I Comparative Study Of Related Works

A unique feature of Event Guard is its unified security framework that meets both security goals for safeguardingthe

Name of Paper	Merits	Demerits
Enabling confidentiality in content based publish-subscribe Infrastructures [C. Raiciu,2006]	• Provide notification confidentiality • Provide Subscription confidentiality • Use coarse-grain epoch based key management	• Traditional Broker Network • Can't provide fine-grain access control
Event Guard: A System Architecture for Securing Publish-Subscribe Networks [M. Srivatsa et al. 2011]	• Developed a frame work for building secure wide area pub-sub system • Maintain system simplicity scalability and performance metrics • Provide notification confidentiality	• Keyword matching of routing events • Traditional broker network • Can't provide fine grain access control
Privacy-Preserving Content-Based Pub-lish/Subscribe Networks [A. Shikta et al. 2009]	• Data confidentiality from point of view of publishers • Achieve privacy of subscribers	• Address security under restricted expressiveness

pub-sub overlay services from various vulnerabilities and threats and performance goals for maintaining the simplicity and scalability of the overall system while providing security guaranty.

Privacy and confidentiality in content based publish subscribe systems(CBPS) can be ensured by a solution based on a commutative multiple encryption scheme[33]. It achieves both data confidentiality from the point of view of the publishers and the privacy of the subscribers with respect to their interests in a potentially hostile model whereby the publishers, the subscribers and the intermediate nodes in charge of data forwarding do not trust one another. The solution relies on a scheme called multi-layer encryption that allows intermediate nodes to manage forwarding tables and to perform content forwarding using encrypted content and based on encrypted subscriber messages without ever accessing the clear text version of those data. This solution further avoids key sharing among end-users and targets an enhanced CBPS model where brokers can also be subscribers at the same time**.**

A Survey on Different Types of Public KeyCryptographic Primitives:-

In [2] Doukas et al. proposed a system based on Gateways(GW) that aggregate sensor data and also resolve security issues through digital certificates and PKI data encryption. It addresses the security problems in IoT(Internet of Things) health care devices. In people's personal as well as community lives, the IoT plays an important role. A prototype cloud-based system is proposed to address the security issues in IoT. The proposed system manages the collected data and then forwards it to gateways and then to the cloud infrastructure. IoT gateways used to apply appropriate encryption techniques to collected data and thus provide securetransmission techniques. These gateways ensure security and privacy of health care devices by applying encryption. PKI provides an effective way for information exchange over insecure environment like IoT. IoT gateways are used to reduce the computational and memory constraints of PKI encryption. In [3] Reimair et al. proposed a method whichuses the centralized key storage solutions for bringing the functions of ID based encryption systems to traditional PKI systems. It addresses the problem of key authentication in PKI. The proposed approach brings identity based encryption and attributes based encryption approach to PKI with-out compromising security. It emulated the identity based encryption approach for PKI infrastructure. Centralised key access and management is possible by using crySIL.

In [4] J. Lokesh et al. proposed a light weight implementation of public key infrastructure for providing security in wireless sensor networks. Authenticity of base station was ensured by the application of public key cryptography.Proposed system used for the session key set up between base station and sensors. It provided confidentiality andauthentication to the wireless sensor network. In [5] Dolgovet al. proposed a chameleon-signature in the prototype of ukrainian combined PKI. A combination of chameleon hashand PKI used to improve the performance of electronic document management systems. The implementation of chameleon hash along with PKI provides security for electronic commerce systems.

A new scheme for the implementation of PKI infrastructure in adhoc network was proposedin [6]. The proposed method distributes the functionality of PKI between network nodes by using two methods. First technique provides full Certificate authority functionality to the cluster heads in the network. And the second technique manages the distribution of certificates among nodes in the networks. A multi signature mechanism is also proposed to increase the trust of the certificates which are signed by more than one cluster head. The proposed method is based on the

clustering and cluster head election. There are also mechanisms to support mobility. The proposed method isindependent of routing protocol.

In [7] Wei Ren et al. studied the possibility of achieving the optimized user revocation cost with respect to variousrevocation approaches in privacy aware PKI. Privacy and security of services can be ensured using Privacy awarePKI. Privacy aware PKI used to provide access control and privacy in wireless networks. The proposed method focused on group signature which is based in privacy aware PKI. It designed an optimised user revocation scheme Delta-RL. It addressed user revocation in group signature based privacy-aware PKI from the view point of performance evaluation and optimization. Delta-RL provides revocation by using periodic revocation, timely revocation or revocation list approach. Delta-RL provides high performance and less communication overhead. In [8] Fagen Li et al. proposed efficient signcryption scheme to solve the communication problems between heterogeneous systems. It can achieve confidentiality, integrity, authentication and non-repudiation. The proposed signcryption method used to send message to receiver in identity based encryption system. The user in identity based encryption system also uses the signcryption algorithm to send the message to receiver which is in PKI system. Two signcryption schemes are proposed for this purpose. These schemes are secure against insider attacks. The results proved that these two schemes are secure in the random oracle model.

In [9] P.R.Karla proposed a method for encrypting ontological meta-models built using semantic web technologies.The proposed method uses a combined approach of identity based encryption and elliptic curve cryptography to achieve this. The Elliptic Curve Cryptography (ECC) is a public key encryption technique based on elliptic curve theory. Faster, smaller, and more efficient cryptographic keys can be created using elliptic curve cryptography. Keys are generated through the properties of elliptic curve. In the proposed approach ontological models are encrypted using ECC combined with Identity-Based Encryption (IBE). Encryption of metamodels developed using semantic web technology in theproposed approach. TinyIBE which is a complete identity-based encryption scheme for sensor networks is proposed in [10]. It proved that Identity based encryption scheme is possible in sensor networks and it is very efficient approach to provide security in sensor networks. This method exploits the capabilities if higher end cluster heads. The TinyIBEreduces key storage space and communication overhead. It also provides a higher level of security and stronger resilience against node capture attack. This study proved that identity based encryption is an effective way to provide security in heterogeneous networks.

In [11] Yang et al. considered the problem of constructing proxy re-encryption based on SK identity based encryption. A proxy re-encryption scheme based on secret key identity based encryption is constructed with the help of PKG. In this scheme only PKG generates the re-encryption key. This method is applicable to small Identity based encryption(IBE) systems because the PKG should be online every time. The proposed proxy re-encryption scheme is unique because it is chosen cipher text attack type2(CCA2) secure. In [12] an identity based proxy signature scheme is proposed. The security of the scheme is proved in standard model. The proposed ID based proxy signature scheme is proven to be secure under computational Diffie-Hellman assumption. An ID based secret signature scheme is proposed in [13]. This ID based implementation of secret signature reduces the key management load. ID based signature scheme and ID based key management scheme are combined together to implement the ID based secret signature scheme. The proposed ID based secret signature scheme is secure in the random oracle model under standard computational Diffie-Hellman (CDH) and decisional Diffie-Hellman (DDH) assumptions. Signature proving and receiver proving protocols are also provided. An ID based blind signature is proposed in [14]. Blind signature allows a signer to sign a message without revealing the identity. Identity based blind signature scheme is proposed. The scheme is based on the hess ID-based signature scheme. The scheme is secure under the computational Diffie-Hellman assumption. As the number of blind signature verifications is considerably large theproposed scheme is efficient.

An efficient Identity based signcryption scheme is proposed in [15]. Signcryption combines the functionalities of signature and encryption. Two schemes are proposed here. Among that only one recipient is there in the first scheme and there are multiple receivers in the second scheme. The proposed ID basedsigncryption methods are based on elliptic curve cryptography. Single recipient signcryption scheme and multi receiversigncryption scheme are proposed. The multi receiver approach reduces the communication overhead. Signcryption and unsigncryption stages didn't involve the support of bilinear pairings. The schemes support the confidentiality, unforgeability, public verifiability,non-repudiation, integrity and forward secrecy. Two users are there in single recipient signcryption scheme whereas more than two users are there in multi receiver signcryption scheme. This method is more efficient since there is less communication overhead. In [16] Fagen Li et al. proposed an identity-based(t, n)threshold proxy

signcryption scheme using bilinear pairings. The use of identity based cryptography reduces the problem of key management. The construction of ID based proxy signcryption was based on pairing-based verifiable secret sharing scheme and ID-based signcryption scheme. The proposed scheme is also suitable for multi agent systems.
An Identity Based Korean Certificate-based Digital Signature Algorithm(KCDSA) Signcryption was proposed in [17]. The semantic security, public verifiability or the forward secrecy can be achieved using this signcryption scheme. The proposed approach is based on the standardized digital signature scheme. Korean Certificate-based Digital Signature Algorithm was extended by using the idea of ID based cryptography. The proposed ID based KCDSA signcryption scheme provide the semantic security under the decisional bilinear Diffie-Hellman assumption. In [18]Yong Yu et al. proposed an ID-based mediated signcryption which solves the problem of the fast revocation of a user's identity in IDBased signcryption schemes. This scheme is proven to be secure under random oracle model. However the system is not secure without random oracle which is an open problemto address. A Scalable revocable certificate less encryption (RCLE) scheme was proposed in [19]. This scheme is provably secure in standard model. The proposed system can resist the threat of decryption key exposure. Decryption key exposure-resistant revocable certificateless encryption (RCLE) scheme with a very short decryption key is also proposed which is provably secure under random oracle model. This scheme addresses the key revocation problem in the public key cryptography. The proposed scheme has less communication overheads and less resource consumption.

In [20] Certificateless Public Key Encryption with Keyword Search model is proposed. The proposed model doesn't need a secure channel. This provides security against chosen keyword attack and keyword guessing attack. This method removes the key escrow problem and it is very efficient method. Since it doesn't need any certificates the complexity will be low and it is more applicable to DaaS (Data as a service) environment in cloud computing. A practical certificateless signature (CLS) scheme based on bilinear pairings was proposed in [21]. In the verification algorithm three pairing computations can be used. Only one precomputable pairing is used in signing process. The security of the proposed system is provably equivalent to Inverse Computational Diffie-Hellman problem and q-Strong Diffie-Hellman problem in the random oracle model. The proposed method is more efficient as compared to other methods.

In [22] Miao et al. done the cryptanalysis of a certificateless signature scheme. They proved that it is not secure against type II adversary who models a malicious-but-passive key generation center (KGC). An attack used to describe the capability of type II adversary to forge certificateless signature of signer by getting the two valid signature of the signer. That is if the adversary gets two valid signature of user, he can forge the valid signatures on behalf of the original user. Thus they proved that the certificateless signature scheme they considered failed to achieve the security. In [23] Bo Yang et al. studied certificateless strong designated verifier signatures (CLSDVS) based on bilinear pairings by combining CLPKC with the strong designated verifier signatures. An efficient CLSDVS scheme was proposed with supporting security proofs and efficiency analysis. This work provided the security proof of the proposed system under random model. The security of the proposed CLSDVS scheme is based on the intractability of the Computational Bilinear Diffie-Hellman Problem and the Computational Diffie-Hellman Problem. The proposed scheme satisfies all the requirements of the strong designated verifier signatures in the certificate less public key cryptography.

In [24], an efficient CL-PKC signcryption scheme was proposed. The proposed scheme supports publicly verifiable signatures. The proposed one is an efficient one than the first concrete and secure CL-PKC signcryption scheme. Byusing signcryption confidentiality, authentication and non-repudiation can be achieved in a single step. Since certificateless approach is used, there is no key escrow problem and also cost can be reduced significantly. A certificateless blind signcryption scheme with partial message recovery is proposed in [25]. The proposed method is based on certificateless based blind signcryption scheme and identity-based signature scheme with partial message recovery. The dishonest behavior of KGC can be detected by the proposed method. It is used to sign messages which have limited bandwidth environments. It is proven that the scheme provides confidentiality, verifiability, unforgeability, high security, and high efficiency. Non repudiation can be achieved by preventing the KGC from framing. The communication as well as computational costs is reduced by usingthe proposed scheme. This scheme shortens the length of message for signcryption to meet the constrained bandwidth requirements.

A certificateless broadcast signcryption scheme is constructed in [26]. The proposed scheme is secure under theDiffie-Hellman assumptions in the random oracle. Broadcast signcryption, allows the broadcaster to encrypt and sign the message in a single logical step. This provides confidentiality and authentication to the messages. The forward secrecy security attributes are satisfied by the proposed scheme. The proposed scheme has a comparatively

lowcommunication overhead. So that the proposed system is suitable for broadcast system devices with low computational capabilities. Since it is certificateless there is no key escrow problem. In [27] Han Yiliang et al. proposed an Identity-based certificateless aggregate signcryption scheme. The proposed scheme makes use of the multilinear maps and it eliminates the key escrow problem. The scheme is provably secure under standard model. The proposed scheme provides unforgeability and confidentiality. The Route Map of public Key Cryptographic Primitives is given in Figure.2

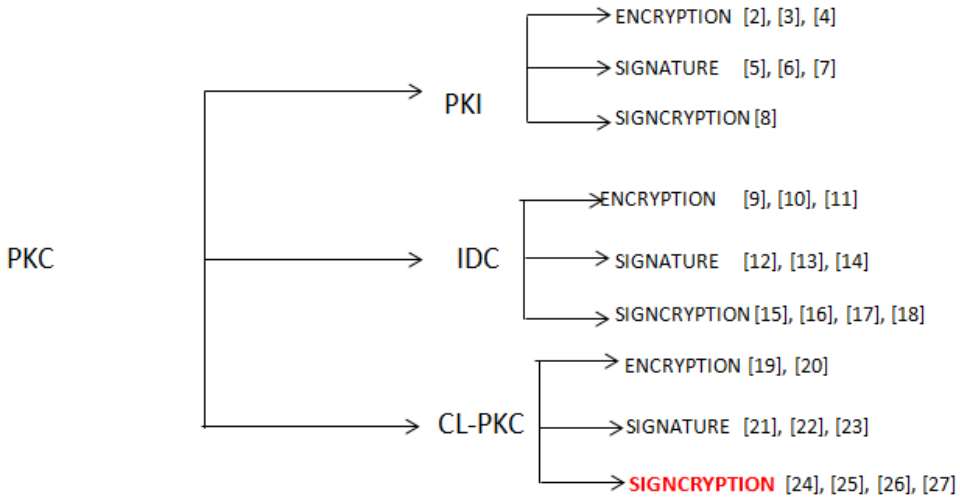

Figure 2. Route Map of public Key Cryptographic Primitives

A. Analysis of the Detailed Study:-

From the detailed study of different types of public key cryptographic primitives, it is found that certificate-less signcryption is an efficient approach to provide security to publish/subscribe systems. Certificate-less signcryption can solve the security problems in publish/subscribe systems with high performance. Hence we highlighted the term signcryption in Figure.2.

Conclusion:-

Publish/Subscribe messaging paradigm is an important method for communication in distributed systems. Many applications make use of the content based publish/subscribe messaging paradigm. Hence it is necessary to meet the security demands of publish/subscribe systems. Various methods can be used to address the security issues of public subscribe system. A survey is conducted based on different types of public key cryptographic primitives which can be applied to secure publish/subscribe systems. From the detailed study, it is clear that certificateless signcryption approach can solve the security issues with high performance and low communication overhead.

References:-

1. **Muhammad Adnan Tariq, Boris Koldehofe, and Kurt Rother-mel**, Securing Broker-Less Publish/Subscribe Systems Using Identity-Based Encryption, IEEE Transactions on parallel and
2. distributed systems, February 2014
3. **CharalamposDoukas, IliasMaglogiannis ,VassilikiKoufi, Flora Malamateniou, and George Vassilacopoulos** , EnablingData Protection through PKI encryption in IoT m-Health Devices, IEEE 12th International Conference on Bioinformaticsand Bioengineering (BIBE), November 2012
4. **Florian Reimair, Johannes Feichtner, Peter Teufl**, Attribute-Based Encryption goes X.509, IEEE 12th International Conference on e-Business Engineering, 2015
5. **J.Lokesh and E.Munivel**, DesignofRobustandSecure EncryptionScheme for WSN using PKI(LWT-PKI), COMSNETS'09 Proceedings of the First international conference on Communication Systems And Networks, Pages 586-587
6. **Viktor Dolgov, IuliiaIshchenko**, Proposals of using chameleon-signature in Ukrainian prototype of combined
7. PKI , TCSET, February 2010
8. **KadriBenamar, Feham Mohammed, M'hmedAbdallah**, A new management scheme of cluster based PKI for ad hoc networks using multi-signature, IEEE Transactions on parallel and distributed systems, June 2010

9. **Wei Ren, KuiRen, Wenjing Lou**, Optimized User Revocation for Group Signature Based Privacy-aware PKI, The 28thInternational Conference on Distributed Computing Systems Workshops, June 2008
10. **Fagen Li, Hui Zhang, and Tsuyoshi Takagi**, Efficient Signcryption for Heterogeneous Systems , IEEE Systems Journal, Vol. 7, No. 3, September 2013
11. **Pramukh R. Karla, Sang C. Suh, and Varadraj P. Gurupur**, Encrypting Ontological Meta-Model Using Elliptic Curve Cryptography with Identity Based Encryption , 8 th International Conference on Computing Technology and Information Management, April 2012.
12. **PiotrSzczechowiak and Martin Collier**, TinyIBE: Identity-Based Encryption for Heterogeneous Sensor Networks, ISS-NIP, December 2009
13. **Xuan Wang and Xiaoyuan Yang**, Proxy Re-encryptionScheme Based on SK Identity Based Encryption, Fifth International Conference on Information Assurance and Security, 2009
14. **Feng Cao and Zhenfu Cao**, An Identity Based Proxy Signature Scheme Secure in the Standard Model, IEEE International Conference on Granular Computing, 2010
15. **Byoungcheon Lee, Jin Li, Kwangjo Kim**, Identity-Based Secret Signature Scheme, Fourth International Conference on Computer Sciences and Convergence Information Technology, 2009
16. **Reza Shakerian, Touraj11ohammadPour, SeyedHosseinKamali, MaysamHedayati**, An Identity Based Public Key Cryptography Blind Signature Scheme from Bilinear Pairings,IEEE Transactions on Emerging Topics in Cloud Computing, February 2008.
17. **Hassan Elkamchouchi, EmanAbouElkheir, and YasmineAbouelseoud**, An Efficient Identity-Based Signcryption Scheme Without Bilinear Pairings , ISSNIP, December 2009.
18. **Fagen Li, YupuHu,Shuanggen Liu**, ID-Based(t, n)Threshold Proxy Signcryption for Multi-Agent Systems, Lecture Notes in Computer Science, Volume 4456, pp 406-416
19. **Jong-Ho Ryu, Youn-SeoJeong, DongilSeo**, Identity Based KCDSA Signcryption, The First International Symposium on Data, Privacy, and E-Commerce, 2007.
20. **Yong Yu ,Bo Yang, Ying Sun**, A Provably Secure ID-Based Mediated Signcryption Scheme, ACIS International
21. Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, 2007.
22. **Yinxia Sun, Futai Zhang, LiminShen, Robert H. Deng**, Efficient revocable certificateless encryption against decryption key exposure, ISSN, September 2013.
23. **PengYanguo, Cui Jiangtao, PengChanggen, Ying Zuobin**, Certificateless Public Key Encryption with Keyword Search,International conference on Network Technology and Applications, November 2014.
24. **LifengGuo, LeiHu, Yong Li**, A Practical Certificateless Signature Scheme, First International Symposium on Data, Privacy and E-Commerce, 2010
25. **Songqin Miao, Futai Zhang, Lei Zhang,** On the Security of a Certificateless Signature Scheme, 2nd International Conference on Signal ProcessingSystems (ICSPS), 2010
26. **Bo Yang, Zhengming Hu, Zibi Xiao**, Efficient Certificateless Strong Designated Verifier Signature Scheme, International Conference on Computational Intelligence and Security, 2009
27. **Diego Aranha, Rafael Castro, Julio L'opez, Ricardo Dahab**, Efficient Certificateless Signcryption, 8th Brazilian Symposium in Information and Human Language Technology, March 2011.
28. **Qin Hai-sheng, Zhang Lei, Feng Yan-qiang,**CertificatelessBlind Signcryption Scheme with Message Recovery Design, International Conference on Computer Science and Service System, 2012.
29. **Ming Luo, Chun-huaZou, JianfengXu**, CertificatelessBroadcast Signcryption with Forward Secrecy \, Seventh
30. International Conference on Computational Intelligence and Security, 2011.
31. **Han Yiliang, Chen Fei**, The Multilinear maps based Certificateless Aggregate Signcryption Scheme , International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, 2015.
32. **William stallings**, Cryptography and Network Security Principles and Practices, Fourth Edition, Prentice Hall, 2005
33. **J. Bacon, D.M. Eyers, J. Singh, and P.R. Pietzuch**, Access Control in Publish/Subscribe Systems, Proc. Second ACM Int'l Conf. Distributed Event-Based Systems (DEBS), 2008
34. **C. Raiciu and D.S. Rosenblum,** Enabling Confidentiality in Content-Based Publish/Subscribe Infrastructures, Proc. IEEE Second CreatNet Int'l Conf. Security and Privacy in Comm. Networks (SecureComm), 2006.
35. **M. Srivatsa, L. Liu, and A. Iyengar**, EventGuard: A System Architecture for Securing Publish-Subscribe Networks, ACM Trans. Computer Systems, vol. 29, article 10, 2011.

36. **Shikfa, M. O nen, and R. Molva**, Privacy-Preserving Content-Based Publish/Subscribe Networks, Proc. Emerging Challenges for Security, Privacy and Trust, 2009.