IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received January 22, 2019, accepted March 14, 2019, date of publication March 26, 2019, date of current version April 11, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2907599

An IOT-Oriented Privacy-Preserving Publish/Subscribe Model Over Blockchains

PIN LV[1], LICHENG WANG[1], HUIJUN ZHU[2], WENBO DENG[1], AND LIZE GU[1]
[1]State Key Laboratory of Networking and Switching Technology, Beijing 100876, China
[2]Nanyang Institute of Technology, Henan 473000, China

Corresponding author: Huijun Zhu (zhuhj1201@163.com)

This work was supported in part by the National Key R&D Program of China under Grant 2016YFB0800602, in part by the Shandong Provincial Key R&D Program of China under Grant 2018CXGC0701, and in part by the 111 Project under Grant B08004.

ABSTRACT In the Internet of Things (IoT), a cyber physical system (CPS) has achieved great success in a wide range of distributed integration environments. In the cyber physical system (CPS), interconnected sensing devices collect data in the surrounding environment and send data to all interested nodes through the network, thereby sharing all nodes data. This process can be implemented by using a publish/subscribe (pub/sub for short) system. Providing the basic security mechanisms such as authorization and confidentiality is a challenge due to the loose coupling of subscribers and publishers in such a pub/sub system. At the meanwhile, the existing IoT ecosystem mostly relies on a centralized server and thus faces the problem of single point failure. Thus, it is interesting to realize a brokerless or decentralized pub/sub model. Inspired by this motivation, this paper mainly proposes a privacy-preserving publish/subscribe model by using the blockchain technique, which evades the centralized trustroot setting and the problem of single point failure. Another key point of our proposal is that the primitive of public key encryption with equality test (PKEwET) is employed to enable all the required authorization, communication and topics matching can be finished in a confidential manner. Finally, a lightweight prototype of our proposal is implemented by using web3j, and the security and efficiency analysis are also presented.

INDEX TERMS IOT, blockchain, distributed systems, PKEwET, anonymity, pub/sub, CPS.

I. INTRODUCTION

In the last few decades, benefiting from the development of communication technology, wireless sensing technology and big data technology, Internet of Things (IoT) has achieved rocketing development in many fields such as medical care [22], smart city [21] and automatic driving [7]. Data collected from a wide variety of devices can be used in many areas as an important character in IoT world. During the Machine to Machine's (M2M) data exchanging, IoT applications more often use publish/subscribe and request-reply models. The request-reply model is widely used in the traditional Internet. However, it is not suitable for resource-constrained IoT systems. CoAP [24] is a lightweight request-reply protocol targeted for resource-constrained IoT systems. However, because of the lacking the scalability and portability in the large scale of distributed platforms, it is not recommended in such environment. The publish/subscribe is much more practical in such environment because of its low communication overhead and resource efficiency.

Existing pub/sub models for IoT mostly rely on centralized cloud servers such as MQTT [2], LooCI [8], NesC [10]. These lightweight models can work on heavily resource-constrained device hardware and networks with high latency. However, these centralized models may face the following threats:

1) Single point of failure. If the centralized server is down, all services in the network will not be available. For example, these models may suffer from the DoS attacks.
2) Data is easily tampered by the corrupted brokers. Centralized servers are usually exclusive to an organization on the network. If the organization is unreliable, the data in the network will be tampered with or even deleted.
3) The encryption algorithm is heavyweight. The encrypted communication of MQTT usually relies on heavyweight communication protocols such as SSL/TLS [2].

The associate editor coordinating the review of this manuscript and approving it for publication was Macarena Espinilla.

In 2008, Nakamoto [11] first applied the blockchain technology to a point-to-point cash system. The system records all transactions on all nodes in a distributed consensus manner. The blockchain technology adopted by the system has rapidly attracted the attention of the academic community with its advantages in decentralization, anonymity, record not tampering and smart contracts. The advantages of blockchain in IoT mainly reflect in:

1) Decentralization: The blockchain uses distributed consensus to jointly maintain data consistency on the chain. The entire process does not require the participation of trusted centers. Because of the decentralized nature of the blockchain, all nodes on the blockchain can easily resist attacks such as DoS.
2) No tampering: Once the data is stored in the blockchain, no one has the permissions to modify the data. This feature provides a safe and reliable storage environment for the data on the blockchain.
3) Anonymity: Currently there are already many mechanisms for the anonymity of membership transactions on the blockchain such as RingCT2.0 [17], Mixcoin [4], zkSnark [14], etc. These mechanisms are well protected for the identity privacy of blockchain users.
4) Smart Contract: This technology enables the blockchain to automatically execute Turing complete code in order to meet the needs of multiple application scenarios besides cryptocurrency.

In order to solve the aforementioned problems faced by the traditional pub/sub models, a privacy-protected blockchain-based pub/sub model is proposed in this paper. The model consists of three entities, publishers, subscribers, and blockchain-based broker. The publisher is primarily responsible for publishing contents. The subscriber registers interest with the publisher and receives the corresponding contents. The blockchain-based broker records the subscription and forwards the contents from the publisher to the subscriber. In this secure pub/sub model, all data stored in the model cannot be changed, which solves the problem that the data of the traditional centralized publish/subscribe model is easily falsified. In terms of multi-node synchronization, all nodes' data is synchronously replicated in a distributed consensus manner, so the data of all nodes is relatively ordered. For the privacy protection of model users, the model is based on public key encrypt with equality test (for short PKEwET) [23] and ElGamal [6] provides effective protection for publishers and subscribers' privacy.

A. CONTRIBUTIONS

The main contributions of this paper are summarized as follows.

1) We propose a privacy-preserving blockchain based secure publish/subscribe scheme for IoT systems. The proposed scheme enables publishers to control the data access and subscribers to selectively receive data. The model proposed by us can effectively protect data privacy and interests of subscribers.
2) The proposed model is based on the blockchain technology. The blockchain enable the data to be replicated across multiple blockchain nodes in a large scope. Since the data, recorded on the blockchain, is immutable, anyone can't modify or delete the data. The publishers and subscribers' real identities are also well protected by the Ethereum platform.
3) A prototype system is implemented to evaluate the feasibility of the proposed model. We also give the security analysis of the secure pub/sub model at the end of paper, and prove that the proposed blockchain-based pub/sub can well protect the publishers and the subscribers' privacy.

B. PAPER ORGANIZATION

The rest of this article is organized as follows. In Section II, some related works are analyzed. In Section III, some basic concepts and techniques are recalled briefly. In Section IV, we present a privacy-preserving pub/sub model by using the technique of blockchain and the PKEwET. The analysis of the security, and the performance based on a lightweight prototype implementation of our proposal are given in Section V. Finally, concluding remarks are presented in Section VI.

II. RELATED WORK

Most of the previous research in the publish/subscribe system has focused on improving the expressiveness and the scalability of the pub/sub system [20]. Very few works concentrate on improving the security of pub/sub system.

In [5], Borcea et al. propose PICADOR, a secure topic-based pub/sub system based on the use of a proxy-reencryption scheme. The authors apply a lattice-based proxy re-encryption scheme that allows partial homomorphic operations. The brokers have to re-encrypt the publications such that the authorised subscribers could recover the plaintext of these publications in their system. However, this re-encryption increases the computation overhead significantly on the broker end. The topic of each publication is sent to the broker in plaintext, which can not meet the privacy-preserving requirements of the participants.

CCNx [13] is an advanced research project on Content-centric Networking, now termed Named Data Networking (NDN). The communication architecture in CCNx is also based on pub/sub system. The data content in CCNx is organized using hierarchical naming [9]. Traditional pub/sub system is based on end-to-end delivery. However, CCNx employs a broadcast-based mechanism for information transmission, rather than brokers. Rather than using self-certified identities, publishers in CCNx use a recognizable tag label for their publications. Then publishers attach their publication with their digital signature. This digital signature is produced by encrypting the publication data and the label with the publisher's public key. Once a subscriber receives the publication message, he can verify whether the publication comes from the right source by checking the label within the message. However, if a malicious publisher uses forged labels and

public keys of other publishers, subscribers in CCNx might get the wrong publication.

Trinity [12] is a novel distributed pub/sub broker with blockchain-based immutability by integrating the broker system with a blockchain framework. Trinity supports the smart contract, which is used for validating the published data against the agreement made by all the participants in the framework. If a publisher violates the agreement, the data which is published by him/she will not be registered in the blockchain ledger. Trinity also addresses the issues of ordering by employing the blockchain-based broker system. However, since the published data stored on the blockchain is plaintext, the privacy issue is a much more critical in such system.

Tariq et al. [19], [20] propose a novel approach to provide confidentiality and authentication in a broker-less content-based publish/subscribe system. The authentication of publishers and subscribers as well as confidentiality of events is ensured by adapting the pairing-based cryptography mechanisms. They adapted identity-based encryption (IBE) [3] mechanisms to ensure the encrypted published content to be decrypted by the authorized subscribers. However, by using of the IBE mechanisms, the anonymity of the publishers and subscribers can't be protected in such system.

Anusree and Sreedhar [1] propose a secure broker-less publish/subscribe system with forward secrecy and unforgeability security. The proposed scheme uses an Elliptic Curve Identity Based Signcryption Algorithm. So this scheme reduces the computational cost and the communication overhead effectively. However, the problem of anonymity also exists in such mechanism.

III. BACKGROUNDS

In this section, we review the pub/sub system, PKEwET primitive, and blockchain related concepts.

A. PUB/SUB SYSTEM

The pub/sub system is a middleware solution that decouples publishers and subscribers. It is often used to solve the problem of communication between IoT devices [16]. As shown in Figure.1, there are three entities in a traditional pub/sub system namely the publisher, the subscriber and the broker cluster. This system is characterized by two types of processes: Publishers, which produce messages, and/or Subscribers, which consume the messages they are interested in, where such an interest is indicated by means of subscriptions.

B. PUBLIC KEY ENCRYPTION WITH EQUALITY TEST

The public key encryption with equality test (PKEwET) is mainly used in the field of cloud computing, which allows to determine whether two ciphertexts encrypted by different public keys are equal without decrypting the ciphertext. As shown in Figure. 2, the system has three entities: a cloud and two data owners referred to as Alice and Bob. Alice and Bob encrypt their private data, denoted by M_A and M_B, using their respective public key, transfer the resulting ciphertexts

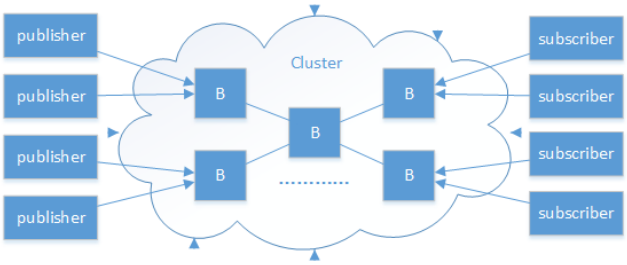


FIGURE 1. General framework of pub/sub systems.

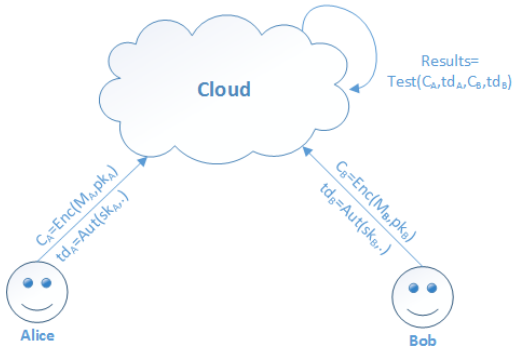


FIGURE 2. Public key encryption with equality test in cloud.

to the cloud. The resulting ciphertexts is denoted by C_A and C_B, and authorize the cloud to execute the equality test on M_A and M_A but without giving it the capability to decrypt C_A and C_B.

C. ETHEREUM AND SMART CONTRACTS

Ethereum is a public chain based distributed ledger similar to the Bitcoin system. But unlike the Bitcoin system, it provides a decentralized virtual machine that can perform the smart contract which is written by turing complete scripting language. The so-called smart contract is a series of commitments that cryptographer Nick Szabo [18] first proposed in digital form in 1994. In Ethereum, all the participants can execute the above contract. Once a smart contract is appointed, it can be executed automatically without the involvement of an intermediary and no one can stop it from running.

Whether it is the execution of smart contracts or the value transfer in the blockchain, transactions play an important role in these processes. As shown in Figure. 3, the structure of the transaction is (txHash, from, to, payload, VRS), which represents the transaction hash, the sender's address, the recipient's address, the message's additional information, and the transaction initiator's signature. A transaction can be thought of as a message sent from one account to another, which can contain a binary data and an ether coin. If the target account contains a code, the code will execute and use the payload as the input parameter. If the target account is a zero account, the transaction will create a new contract and the payload used to create the transaction will be converted to the virtual machine's bytecode and executed.

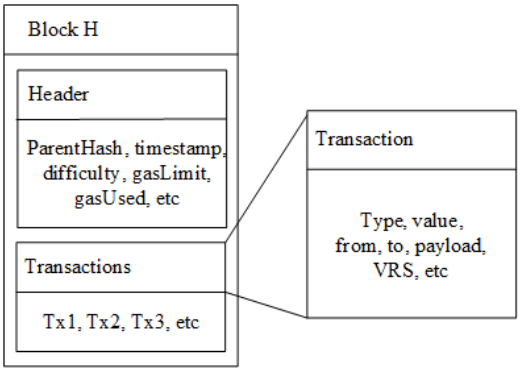


FIGURE 3. Ethereum's block and transaction structure.

IV. BLOCKCHAIN-BASED SECURE PUB/SUB MODEL

A. SECURITY GOALS AND REQUIREMENTS

The goal of our pub/sub protocol is to protect the privacy of subscribers and publishers against the third-party platform. Just as [20] did, there are three security requirements in our design:

Authentication: To avoid noneligible subscriptions, only authorized subscribers should be able to publish events in the system.

Scalability: The secure pub/sub system should scale with the number of subscribers in the system. Two aspects are important to preserve scalability: 1) the performance of the system can not decline obviously by the increasing number of the node. 2) The number of keys maintained by each participant is small enough.

Confidential: In a broker-less environment, two aspects of confidentiality are of interest: 1) the contents are only visible to authorized subscribers and are protected from illegal modifications, and 2) the subscriptions of subscribers are confidential and unforgeable.

B. BLOCKCHAIN-BASED SECURE PUB/SUB MODEL

The secure pub/sub model of this paper is based on the PKEwET scheme proposed by Zhu *et al.* [25]. The dynamics of the secure Publish/subscribe model is shown in Figure. 4. This model mainly includes the following procedures, Setup, Publish, Subscribe, Match, and Receive. The specific scheme is as follows.

1) Setup: Select a k as a security parameter and generate the system public parameter sp by the following procedure. First select the group G whose order is prime q, then randomly select $g \in G_q$, and finally select the hash function:

$$H_1 : G^4 \to Z_q^4, H_2, H_3, H_4, H_5 : \{0,1\}^k \to Z_q \quad (1)$$

2) Publish: The publisher randomly selects $x \in Z_q$ and computes $X = g^x$, and finally publishes X and T_{Topic} to the blockchain system.
3) Subscribe: When the subscriber queries the publisher's transaction by reading the blockchain ledger, the subscriber initiates a subscription transaction to

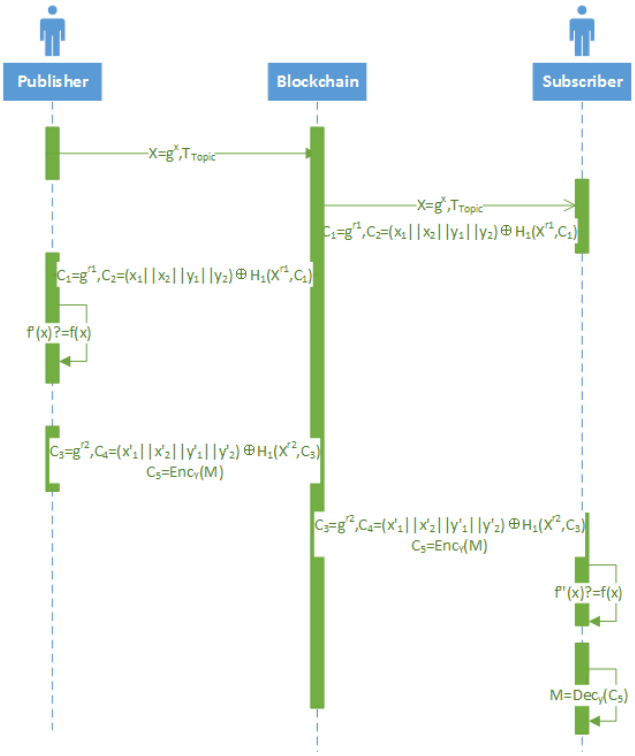


FIGURE 4. Interactive time sequence of the proposed model.

the publisher. The specific process is as follows: randomly select $y \in Z_q$ and calculate $Y = g^y$, the subscriber first uses H_2, H_3, H_4, H_5 generate two points:

$$p_1 = (H_2(T_{Topic}), H_3(T_{Topic})),$$
$$p_2 = (H_4(T_{Topic}), H_5(T_{Topic})) \quad (2)$$

The subscriber constructs a straight line $f(x)$ by using p_1 and p_2. He or she brings x_1,$x_2 \in 0, 1^l$,which is selected by randomly, to $f(x)$ and computes (x_1, y_1),(x_2, y_2). Then the subscriber generate $r_1 \in Z_1^*$.

$$C_1 = g^{r_1}, C_2 = ((x_1||x_2||y_1||y_2) \oplus H_1(X^{r_1}, C_1)) \quad (3)$$

Finally, the subscriber sends C_1, C_2, Y and the token which is paid for the publisher to his transaction address.

4) Match: When the publisher receives the subscriber's transaction information, the subscriber uses H_2, H_3, H_4, H_5 to generate two points

$$p_1 = (H_2(T'_{Topic}), H_3(T'_{Topic})),$$
$$p_2 = (H_4(T'_{Topic}), H_5(T'_{Topic})) \quad (4)$$

Use p'_1, p'_2 to construct a straight line $f'(x)$. Then the publisher recovers the information from the transaction on the ledger as follow:

$$x'_1||x'_2||y'_1||y'_2 = C_2 \oplus H_1((C_1^x), C_1) \quad (5)$$

If (x'_1, y'_1), (x'_2, y'_2) both on the $f'(x)$, it means $T_{Topic} = T'_{Topic}$.The publisher choose $r_2 \in Z_q^*$ randomly.

TABLE 1. The comparison with other schemes.

Scheme	Confidentiality	Encrypted Matching	Anonymous	No Trust	Light Weight
Tariq et al. [20]	✓	✓	–	–	–
Anusree et al. [1]	✓	✓	–	–	–
Shitole et al. [15]	✓	✓	–	–	–
Our scheme	✓	✓	✓	✓	✓

And then compute

$$C_3 = g^{r_1}, C_4 = (x_1'||x_2'||y_1'||y_2') \oplus H_1(Y^{r_2}, C_3),$$
$$C_5 = Enc_Y(M) \quad (6)$$

Enc represents the ElGamal public key encryption algorithm, and finally the publisher sends C_3, C_4, C_5 as transaction to the blockchain system.

5) Receive: Finally, the subscriber receives the publisher's published message, and the subscriber first calculates

$$x_1''||x_2''||y_1''||y_2'' = C_4 \oplus H_1(C_3^y, C_3) \quad (7)$$

Then, the subscriber uses (x_1'', x_2''), (y_1'', y_2'') to construct a straight line $f''(x)$. If $f''(x) = f(x)$, the subscriber gets the message $M = Dec_y(C_5)$

V. SECURITY AND PERFORMANCE ANALYSIS

A. SECURITY ANALYSIS

1) CONFIDENTIALITY

For the Pub/Sub scheme, the publisher encrypts the message body M using a public key cryptosystem to generate ciphertext $C = Enc_Y(M)$. Then, the subscriber decrypts the ciphertext using $M = Dec_y(C)$ to obtain the message plaintext M. The confidentiality guarantee of the message body is based on the security of the encryption system, that is, as long as the public key encryption system is secure, we can assume that the confidentiality of the message is guaranteed. Since this scheme uses the ElGamal public key cryptosystem with IND-CPA security, satisfying this security means that ciphertext will not reveal any useful information about the corresponding plaintext to any adversary whose computing power is polynomial bounded. The confidentiality of the message of this program is guaranteed.

2) PRIVACY PRESERVATION

The pub/sub model effectively protects subscribers' Topic privacy information from being accessed by third parties other than the publisher. During the subscription phase of the subscriber, if the adversary wants to obtain the subscriber's subscribed Topic, it must crack the determined Diffie-Hellman problem in a finite polynomial time. So he must have the ability to calculate $h = g^{r_1 x}$ under the premise of given (g, g^x, g^{r_1}, h) in polynomial time. However, it is difficult to solve the Diffie-Hellman problem. This scheme effectively protects the subscriber's subscription to Topic privacy.

In addition, the anonymity of this model is guaranteed by the pseudo anonymity of the Ethereum platform. By using this platform, the addresses of the publishers and the subscribers are obtained by hashing the corresponding public key, and no one can associate the address of the publishers and the subscribers with their real identity. The model provides anonymity for publishers and subscribers, effectively ensuring the identity privacy of publishers and subscribers.

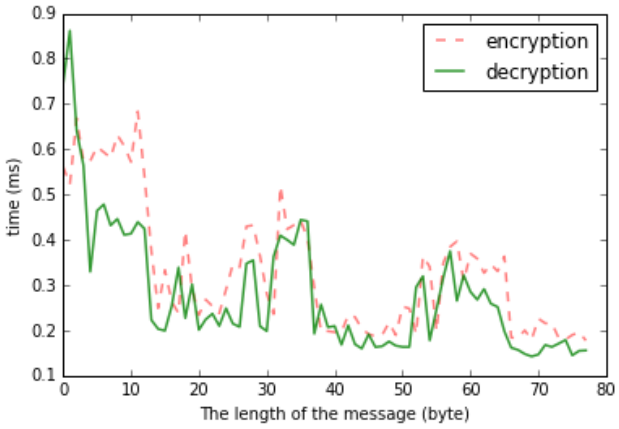


FIGURE 5. Encryption/decryption runtime.

TABLE 2. The performance analysis of our secure pub/sub.

Algorithm	runtime(ms)
Publish	0.519
Subscribe	15.144
Match	4.165
Receive	1.796

3) RESISTANCE TO DDOS ATTACKS

Because Ethereum runs under the assumption where most nodes are honest, it is difficult for an attacker to launch a DDos attack on the network. In fact, if you want to launch 51% attacks in the Ethereum network, you need a lot of computing power. So as long as you retain enough honest nodes in the network, this model can resist DDos attacks.

B. PERFORMANCE ANALYSIS

In this section, we discuss the efficiency of our protocol. The prototype system is written by web3j, which is a lightweight Java SDK of Ethereum. The performance of our protocol is shown in table 2. It is executed on intel(R) Core(TM) i7-6700 CPU 3.40GHz, 16.00GB of RAM. As shown in table 2, we make the message to be encrypted one byte by using our scheme. In figure 5, we make the experiment about its runtime with increasing length of the message. We can

see that our scheme have a good efficiency. We also compare our scheme with others in table 1. All of the schemes realize protection of the confidentiality of data and support encrypted matching of the topic. However, they don't consider the anonymity of the subscriber and the trust problem in IoT system. Our scheme solves these problems by using the Ethereum platform.

VI. CONCLUSION

In this paper, we propose a secure light-weight pub/sub scheme by using the blockchain. In order to protect the subscribers' privacy, we use the light-weight PKEwET to encrypt topics. We also solve the single point of failure and the anonymity of the participants by using the Ethereum. At the end of the paper we give the experiments to verify the rationality of our scheme.

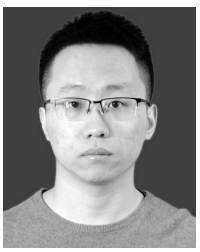
REFERENCES

[1] P. Anusree and S. Sreedhar, "A security framework for brokerless publish subscribe system using identity based signcryption," in *Proc. Int. Conf. Circuits, Power Comput. Technol.*, Mar. 2015, pp. 1–5.
[2] A. Banks and R. Gupta, "Mqtt version 3.1 1," *OASIS*, to be published.
[3] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Proc. IEEE Symp. Secur. Privacy*, 2007, pp. 321–334.
[4] J. Bonneau, A. Narayanan, A. Miller, J. Clark, J. A. Kroll, and E. W. Felten, "Mixcoin: Anonymity for bitcoin with accountable mixes," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.* Berlin, Germany: Springer, 2014, pp. 486–504.
[5] G. D. Crescenzo *et al.*, "Efficient and private three-party publish/subscribe," in *Proc. Int. Conf. Netw. Syst. Secur.*, 2013, pp. 278–292.
[6] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Trans. Inf. Theory*, vol. IT-31, no. 4, pp. 469–472, Jul. 1985.
[7] S. H. Hashemi, F. Faghri, P. Rausch, and R. H. Campbell, "World of empowered iot users," in *Proc. IEEE 1st Int. Conf. Internet*, Apr. 2016, pp. 13–24.
[8] D. Hughes *et al.*, "Looci: a loosely-coupled component infrastructure for networked embedded systems," in *Proc. 7th Int. Conf. Adv. Mobile Comput. Multimedia*, Dec. 2009, pp. 195–203.
[9] V. Jacobson, D. K. Smetters, J. D. Thornton, M. F. Plass, N. H. Briggs, and R. L. Braynard, "Networking named content," *Proc. 5th Int. Conf. Emerg. Netw. Exp. Technol.*, May 2009, pp. 1–12.
[10] P. Levis *et al.*, "The emergence of networking abstractions and techniques in tinyos," *Proc. NSDI*, vol. 4, 2004, p. 1.
[11] S. Nakamoto. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System.* Accessed: Mar. 30, 2019. [Online]. Available: https://goo.gl/MqyCW7
[12] G. S. Ramachandran, K.-L. Wright, and B. Krishnamachari. (2018). "Trinity: A distributed publish/subscribe broker with blockchain-based immutability." [Online]. Available: https://arxiv.org/abs/1807.03110
[13] B. Saadallah, A. Lahmadi, and O. Festor, "CCNx for contiki: Implementation details," INRIA, Tech. Rep. RT-0432, Nov. 2012.
[14] E. B. Sasson *et al.*, "Zerocash: Decentralized anonymous payments from bitcoin," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2014, pp. 459–474.
[15] S. Shitole and A. Gujar, "Securing broker-less publisher/subscriber systems using cryptographic technique," in *Proc. Int. Conf. Comput. Commun. Control Automat. (ICCUBEA)*, Aug. 2016, pp. 1–6.
[16] M. Singh, M. Rajan, V. Shivraj, and P. Balamuralidhar, "Secure MQTT for internet of things (IoT)," in *Proc. 5th Int. Conf. Commun. Syst. Netw. Technol.*, Apr. 2015, pp. 746–751.
[17] S.-F. Sun, M. H. Au, J. K. Liu, and T. H. Yuen, "Ringct 2.0: A compact accumulator-based (linkable ring signature) protocol for blockchain cryptocurrency monero." in *Proc. Eur. Symp. Res. Comput. Secur.*, Aug. 2017, pp. 456–474.
[18] N. Szabo, "Smart contracts: Building blocks for digital markets," *EXTROPY, J. Transhumanist Thought*, no. 16, 1996.
[19] M. A. Tariq, B. Koldehofe, A. Altaweel, and K. Rothermel, "Providing basic security mechanisms in broker-less publish/subscribe systems," in *Proc. 4th ACM Int. Conf. Distrib. Event-Based Syst.*, May 2010, pp. 38–49.
[20] M. A. Tariq, B. Koldehofe, and K. Rothermel, "Securing broker-less publish/subscribe systems using identity-based encryption," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 2, pp. 518–528, Feb. 2014.
[21] E. Theodoridis, G. Mylonas, and I. Chatzigiannakis, "Developing an iot smart city framework," in *Proc. IISA*, Jul. 2013, pp. 1–6.
[22] R. J. Krawiec *et al.*, "Blockchain: Opportunities for health care," in *Proc. NIST Workshop Blockchain Healthcare*, Aug. 2016, pp. 1–16.
[23] G. Yang, C. H. Tan, Q. Huang, and D. S. Wong, "Probabilistic public key encryption with equality test," in *Topics in Cryptology—CT-RSA*. New York, NY, USA: Springer, 2010, pp. 119–131 .
[24] Z. Shelby, K. Hartke, C. Bormann, "The constrained application protocol (COAP)," Fremont, CA, USA, 2014.
[25] H. Zhu, L. Wang, H. Ahmad, and X. Niu, "Pairing-free equality test over short ciphertexts," *Int. J. Distrib. Sensor Netw.*, vol. 13, no. 6, 2017, Art. no. 1550147717715605.

PIN LV received the B.S. degree in software engineering from Jilin University, China, in 2016. He is currently pursuing the M.S. degree in computer science with the Beijing University of Posts and Telecommunications. His current research interests include blockchain technology and privacy, and cryptography.

LICHENG WANG received the Ph.D. degree from Shanghai Jiao Tong University, in 2007. He is currently an Associate Professor with the Beijing University of Posts and Telecommunications, Beijing, China. His current research interests include modern cryptography, network security, and trust management.

HUIJUN ZHU received the B.S. degree from Luoyang Normal University, in 2007, the M.S. degree from Henan Polytechnic University, in 2010, and the Ph.D. degree from the Beijing University of Posts and Telecommunications, in 2018. She is currently an Associate Professor with the Nanyang Institute of Technology. Her research interests include modern cryptography, network security, and cloud computing.



WENBO DENG is currently pursuing the B.S. degree in computer science with the Beijing University of Posts and Telecommunications. His research interests include blockchain technology and privacy, and cryptography.

LIZE GU received the Ph.D. degree from the Beijing University of Posts and Telecommunications, Beijing, China, in 2005, where he is currently a Professor. His current research interests include modern cryptography and blockchain technology.