Hindawi
Security and Communication Networks
Volume 2021, Article ID 5573886, 6 pages
https://doi.org/10.1155/2021/5573886

Research Article

Security Analysis of a Lightweight Identity-Based Two-Party Authenticated Key Agreement Protocol for IIoT Environments

Yuting Li,[1,2] **Qingfeng Cheng**,[1,2] **and Wenbo Shi**[3]

[1]*State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou 450001, China*
[2]*Strategic Support Force Information Engineering University, Zhengzhou 450001, China*
[3]*School of Computer and Communication Engineering, Northeastern University at Qinhuangdao, Qinhuangdao 066004, China*

Correspondence should be addressed to Qingfeng Cheng; qingfengc2008@sina.com

Received 8 January 2021; Revised 2 February 2021; Accepted 22 February 2021; Published 28 February 2021

Academic Editor: Jinbo Xiong

Internet of Things brings convenience to the social life, at the same time, putting forward higher requirements for the security of data transmission and storage. Security incidents based on industrial Internet of Things have occurred frequently recently, which should be given full consideration. The identity-based authenticated key agreement protocol can solve these security threats to a certain extent. Recently, a lightweight identity-based authenticated key agreement protocol for Industrial Internet of Things, called ID-2PAKA protocol, was claimed to achieve secure authentication and meet security properties. In this paper, we show that the ID-2PAKA protocol is insecure in identity authentication and cannot resisting ephemeral key compromise impersonation attack.

1. Introduction

The application field of the Internet of Things is very extensive, especially in the industry [1]. As increasingly more devices such as sensors are connected together [2], related industries are getting closer and integrated with the Industrial Internet of Things (IIoT). IIoT can be regarded as a high degree of integration of industrial automation systems and IoT systems. With the explosive growth of industrial information, the large amount of data generated in the industrial production is a challenge for IIoT. How to effectively process, analyze, and record these data, and extract the results of guiding suggestions for industrial production, is the core difficulty of IIoT [3].

The system architecture of IIoT is shown in Figure 1. The perception layer is composed of widely deployed physical devices (such as sensors, actuators, manufacturing equipment, facility utilities, and other industrial manufacturing and automation related objects) and is responsible for real-time collection of industrial environment and production resource data. The network layer makes short-distance access and long-distance transmission of perception data a reality, while the data processing layer is for fully mining and utilizing the aggregated perception data. The application layer is composed of various industrial applications, including smart factories and smart supply chains. These intelligent industrial applications utilize numerous sensors and actuators to achieve real-time monitoring, precise control, and effective management.

With attendant, incidents based on IIoT security have occurred frequently recently. For intruders, attacks on IIoT systems can attract more attention or get more than attacks on IoT systems in other industries. Attackers have adopted a variety of intrusion methods, such as the leakage of industrial key data, and the illegal hijacking and manipulation of interconnected terminals [4]. The IIoT relies on modern and mature industrial automation systems and integrates a large number of technologies and applications from the fields of communications and computers. The wide application of the IoT puts forward more strict security requirements for data transmission and storage. Therefore, some traditional network attack methods are also suitable for IIoT systems. A large number of attacks have occurred in the past few years. Exposing the various hidden dangers of IIoT in terms of information security is a major obstacle to the rising trend of IoT.

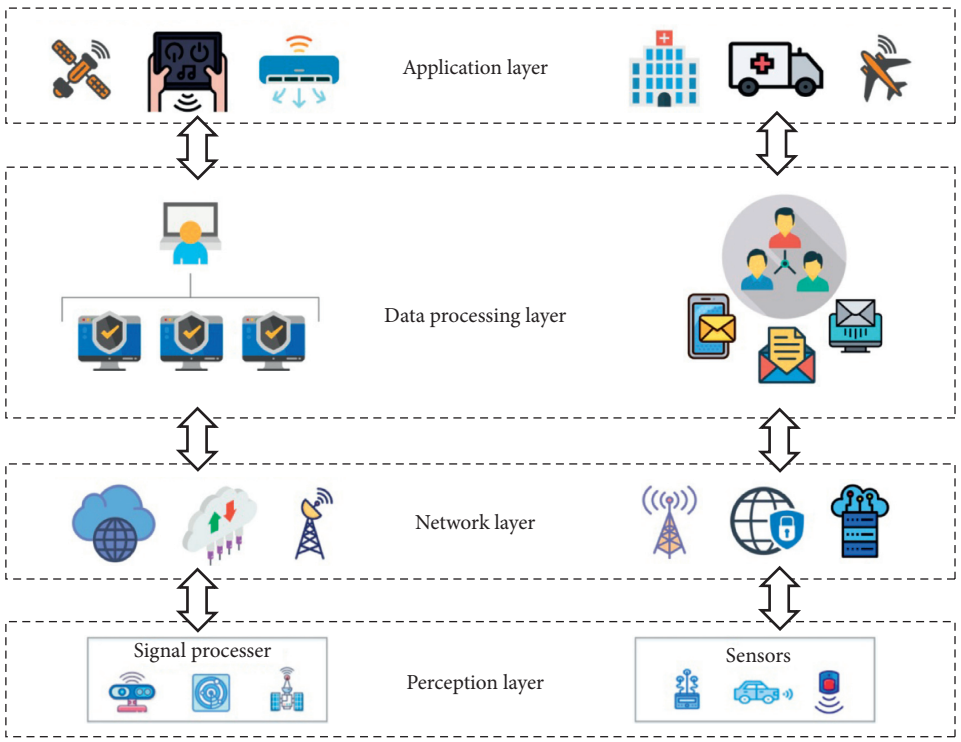

Figure 1: IIoT system architecture.

Specifically, the security threats faced by IIoT can be divided into two categories, namely, the hidden dangers of the internal structure of IIoT and the hidden dangers of external network attacks. Among them, attacks against external networks have the characteristics of wide coverage, multiple levels, and diverse attack methods. The solutions to these security problems usually use a mixture of computing, encryption, image processing, and identity authentication.

Applying cryptography to network communication can solve these security threats to a certain extent. Cryptography realizes the encryption, decryption, user identity authentication, key agreement, and privacy protection of important information through strict mathematical theories. It is one of the important means to protect communication security. The key agreement protocol is an important branch of cryptography, which refers to the rule that two or more parties in communication negotiate a symmetric encryption key on a common channel before formal communication. The key agreement protocol determines the security of the symmetric encryption key and thus determines the information security of the communication participants. Therefore, the study of session key agreement protocol can strengthen the security of the network to a certain extent, and it is of great significance to the protection of personal privacy and commercial interests.

Traditional key agreement protocols use certificates to authenticate the participants of the protocol, which are easy to be forged and tampered with. Therefore, the traditional session key agreement protocol still has certain deficiencies in security. The identity-based authenticated key agreement (ID-AKA) protocol integrates identity authentication into the key agreement process, avoiding the use of digital certificates and improving the security of the key agreement protocol [5, 6]. According to whether bilinear pairing is used in the ID-AKA protocol, it can be divided into the ID-AKA protocol based on bilinear pairing and the ID-AKA protocol without bilinear pairing. Although the ID-AKA protocol without bilinear pairing has an advantage over the ID-AKA protocol based on bilinear pairing in terms of computational efficiency, the ID-AKA protocol without bilinear pairing is not satisfactory in terms of security [7]. Bilinear pairing operation is a computationally intensive operation, so ID-AKA protocol based on bilinear pairing has obvious shortcomings in computational efficiency. This affects the comprehensive performance of the ID-AKA protocol based on bilinear pairs and also seriously affects its practical application range [8].

In this paper, we analyze the ID-2PAKA protocol for IIoT environments from [9] in terms of a security perspective and discover some insecure threats. When the protocol is analyzed, it is insecure in terms of identity authentication. Moreover, there were some threats in resistance to ephemeral key compromise impersonation attack.

The organization of this paper is arranged as follows. Related works are firstly introduced in Section 2. Then, we briefly review the ID-2PAKA protocol in Section 3. Furthermore, Section 4 points out the weaknesses of the ID-2PAKA protocol. Conclusion will be given in Section 5.

2. Related Work

In recent years, cyberattacks against industrial IoT systems have emerged one after another, showing a continuous upward trend. The security issues of industrial IoT systems

have attracted great attention in the information security industry.

In view of the security issues of the IoT, a large number of security mechanisms have been proposed [10, 11], especially the wireless sensor network as an important supporting technology of IoT. In [12], in response to the vulnerability of wireless sensor network nodes and limited resources, Zhou and Xiong propose a lightweight smart card-based wireless sensor network user authentication scheme, which is based on random values as temporary keys. Through the request-response handshake mechanism to ensure the two-way authentication between the user and the gateway node, this solution avoids the problem of asynchrony between the smart card and the gateway node. The literature [13] presents a two-factor authentication protocol that provides a powerful authentication and session key establishment process. The protocol resists the threat of multiple users logging in with the same identity. The authentication process does not require public key operations, and it uses a cryptographic hash function to achieve higher efficiency.

The literature [14] proposes a new method adapted to resource-constrained wireless sensor networks. Only legitimate users can access node resources, and illegal users are denied access. The solution is based on ID technology and elliptic curve cryptosystem (ECC), which provides mutual authentication and key agreement processes between users and nodes. In [15], Liu et al. analyze the wireless sensor network in the perception layer of the IoT and propose an identity authentication scheme for the wireless sensor network. The scheme uses ECC, protecting the data confidentiality and integrity of the perception layer of the IoT. However, this scheme only protects the data security of the perception layer of the IoT system and does not protect the IoT terminal devices at the perception layer.

At present, many key agreement protocols for the IoT environment pay more attention to lightweight requirements [16, 17]. In 2016, Farash et al. [18] improved the key agreement protocol based on heterogeneous sensor network proposed by Turkanovic. The improved version can strengthen the security level. Srinivas et al. [19] proposed a chaotic mapping-based key agreement protocol for IIoT environment. However, the author uses a weaker model to prove the protocol; thus, there is still room for further improvement in the security of the protocol.

In addition to the traditional key agreement protocol, some other methods have also been introduced into the field of IIoT security protection. Recently, Xiong et al. [20] combined data encryption with game theory, designing a personalized privacy protection framework. The advantage is to find a reasonable balance between retaining quality of crowdsensing services and privacy. Besides, in order to solve the key management problem of dynamic wireless sensor networks in IIoT, Tian et al. [21] presented a key management scheme based on blockchain. This scheme used stake blockchain to replace the base station to implement key management, avoiding the security threats of untrusted base stations. The summary of literature studies is given in Table 1.

3. Review of ID-2PAKA Protocol

A brief introduction of ID-2PAKA protocol will be given in this section. It consists of three phases: setup phase, private-key generation phase, and session key agreement phase. The notations and the corresponding meanings used in ID-2PAKA protocol are shown in Table 2.

There are three entities participating in ID-2PAKA protocol: the initiator P_1, the responder P_2, and the PKG. Among them, the PKG is only responsible for generating the identity-based private key of $P_i\,(i = 1, 2)$. Other details can be depicted in the following subsections.

3.1. Setup Phase. In setup phase, the PKG generates the system parameters according the security parameter k:

(1) With a given security parameter k, the PKG chooses a prime number q greater than 2^k, then generates an additive cyclic group G_1, and a multiplicative group G_2 of order q. The generator of G_1 is P.

(2) The PKG chooses a bilinear map e: $G_1 \times G_1 \longrightarrow G_2$.

(3) The PKG chooses two one-way hash functions $H_i\,(i = 1, 2)$: $\{0,1\}^* \longrightarrow \{0,1\}^q$.

(4) The PKG randomly chooses a master private key $s_0 \in Z_q^*$ and computes the master public key $P_0 = s_0 P$.

(5) The system parameters are set as $\{q, G_1, G_2, P, e, H_1, H_2, P_0\}$, public to all entities.

3.2. Private-Key Generation Phase. In this phase, the identity-based private keys and the corresponding public keys of $P_i\,(i = 1, 2)$ are generated by the PKG. The main details are shown in Figure 2:

(1) $P_i\,(i = 1, 2)$ submits the identity $\mathrm{ID}_i\,(i = 1, 2)$ to the PKG.

(2) The PKG first authenticates the legality of $\mathrm{ID}_i\,(i = 1, 2)$, then computes the public key $q_i = H_1(\mathrm{ID}_i)$ and the identity-based private key $\mathrm{Pr}_i = (s/(s + q_i))$.

3.3. Session Key Agreement Phase. This phase is executed between the initiator P_1 and the responder P_2. The details are described in Figure 3:

(1) The initiator P_1 chooses a random number $r_1 \in Z_q^*$, then computes $\psi_1 = r_1 P$ and $\sigma_1 = r_1 \mathrm{Pr}_1$. Then, P_1 sends the tuple $\{\psi_1, \sigma_1\}$ to the responder.

(2) After receiving $\{\psi_1, \sigma_1\}$ from P_1, the responder P_2 chooses a random number $r_2 \in Z_q^*$, then computes $\psi_2 = r_2 P$ and $\sigma_2 = r_2 \mathrm{Pr}_2$. Finally, P_2 sends the tuple $\{\psi_2, \sigma_2\}$ to P_1.

(3) After receiving response of P_2, P_1 first verifies whether the equation $e(\sigma_2, P_0 + q_2 P) = e(\psi_2, P_0)$ holds, where $q_2 = H_1(\mathrm{ID}_2)$. If verified, P_1 computes $X = r_1 \psi_2$ and sets the session key as $sk_1 = H_2(\mathrm{ID}_1 \| \mathrm{ID}_2 \| \psi_1 \| \psi_2 \| X)$.

Table 1: The summary of literature studies.

Literature studies	Description	Application
[10, 11]	Security mechanisms	For wireless sensor networks
[12]	A lightweight smart card-based authentication scheme	For wireless sensor networks
[13]	A two-factor authentication protocol	For wireless sensor networks
[14]	Uses ID technology and elliptic curve cryptosystem	For resource-constrained wireless sensor networks
[15]	Protects the data security	For the perception layer
[16, 17]	Key agreement protocols	For lightweight IoT environment
[18]	An improved key agreement protocol	For heterogeneous sensor network
[19]	Uses chaotic mapping	For IIoT environment
[20]	Combines data encryption with game theory	For privacy protection in IIoT
[21]	Uses stake blockchain	For dynamic wireless sensor networks

Table 2: The notations.

Notations	Meanings
k	Security parameter
G_1	An additive cyclic group
G_2	A multiplicative group
q	The prime order of G_1 and G_2
p	The generator of G_1
s_0	The master private key
P_0	The master public key
$H_i (i = 1, 2)$	The secure hash functions
$P_i (i = 1, 2)$	The users

(4) In the same way, P_2 first verifies whether the equation $e(\sigma_1, P_0 + q_1 P) = e(\psi_1, P_0)$ holds, where $q_1 = H_1(\mathrm{ID}_1)$. If verified, P_2 computes $X = r_2\psi_1$ and sets the session key as $sk_1 = H_2(\mathrm{ID}_1 \| \mathrm{ID}_2 \| \psi_1 \| \psi_2 \| X)$.

Remark. The consistency of the computation is verified as

$$\begin{aligned} e(\sigma_1, P_0 + q_1 P) &= e\left(r_1 \frac{s}{s+q_1} P, (s+q_1)P\right), \\ &= e(r_1 sP, P), \\ &= e(r_1 P, sP), \\ &= e(\psi_1, P_0), \\ e(\sigma_2, P_0 + q_2 P) &= e\left(r_2 \frac{s}{s+q_2} P, (s+q_2)P\right), \\ &= e(r_2 sP, P), \\ &= e(r_1 P, sP), \\ &= e(\psi_1, P_0). \end{aligned} \tag{1}$$

4. Security Analysis of ID-2PAKA Protocol

There are some security vulnerabilities in the proposed ID-2PAKA protocol that cannot be ignored, which will be introduced in detail in this subsection. The security analysis of ID-2PAKA protocol in this paper is based on the theory of eCK model, which is mainly composed of Ephemeral Key Compromise Impersonation Attack and Secure Authentication.

In the idea of eCK model, we can consider the security of the scheme from the perspective of leaking any two keys, except for leaking the long-term private key and temporary private key of a communicating party at the same time. The security analysis of ID-2PAKA protocol is given as follows.

4.1. Ephemeral Key Compromise Impersonation Attack. After analysis, when the ephemeral keys r_1 and r_2 of both communicating parties are leaked, the adversary $\mathcal{A}$ can recover the corresponding session key according to the leaked messages. Thus, ID-2PAKA protocol cannot resist ephemeral key compromise impersonation attack. The details are described in the following.

In the case that r_1, r_2 are known to $\mathcal{A}$ and $\{q, G_1, G_2, P, e, H_1, H_2, P_0\}$ are public to all entities, so that $\mathcal{A}$ can compute $\psi_1 = r_1 P$, $\psi_2 = r_2 P$ and $X = r_1 r_2 P$. The session key is computed as $sk_1 = H_2(\mathrm{ID}_1 \| \mathrm{ID}_2 \| \psi_1 \| \psi_2 \| X)$. In this way, the adversary can easily compute the vital session key without having to do any modification or insertion operations.

4.2. Secure Authentication. In addition to the ephemeral key compromise impersonation attack, the ID-2PAKA protocol is also insecure in terms of identity authentication. The verification of either party to the other is based on the equation $e(\sigma_1, P_0 + q_1 P) = e(r_1(S/(s+q_1))P, (s+q_1)P)$. However, the equation is essentially established by relying on the ephemeral key r_1. The processes of disguising P_1 and P_2 and completing the session key agreement phase are described below.

If $\mathcal{A}$ pretends to be P_1, she first chooses $r_1' \in Z_q^*$, then computes $\psi_1' = r_1' P_0 + r_1' q_1 P$ and $\sigma_1' = r_1' P_0$, finally sends the tuple $\{\psi_1', \sigma_1'\}$ to the responder. The responder P_2 verifies the equation $e(\sigma_1', P_0 + q_1 P) = e(\psi_1', P_0)$. The correctness is as follows:

$$\begin{aligned} e(\sigma_1', P_0 + q_1 P) &= e(r_1' P_0, P_0 + q_1 P), \\ &= e(r_1' sP, (s+q_1)P), \\ &= e(r_1'(s+q_1)P, sP), \\ &= e(\psi_1', P_0). \end{aligned} \tag{2}$$

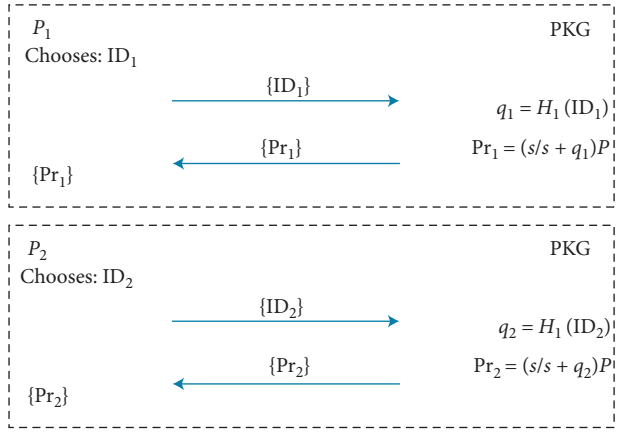

Figure 2: Private key generation phase.

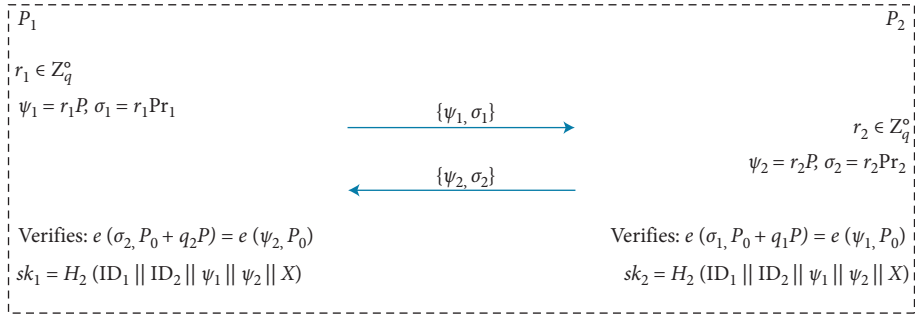

Figure 3: Session key agreement phase.

In the same way, $\mathcal{A}$ can pretend to be P_2. First, $\mathcal{A}$ chooses $r_2' \in Z_q^*$, then computes $\psi_2' = r_2' P_0 + r_2' q_2 P$ and $\sigma_2' = r_2' P_0$, finally sends the tuple $\{\psi_2', \sigma_2'\}$ to the initiator. The initiator P_1 verifies the equation $e(\sigma_2', P_0 + q_2 P) = e(\psi_2', P_0)$. The correctness is as follows:

$$\begin{aligned} e(\sigma_2', P_0 + q_2 P) &= e(r_2' P_0, P_0 + q_2 P), \\ &= e(r_2' sP, (s + q_2)P), \\ &= e(r_2'(s + q_2)P, sP), \\ &= e(\psi_2', P_0). \end{aligned} \tag{3}$$

5. Conclusions

Secure communication is a vital point in IIoT environment, which should be given full consideration. There are many ID-AKA protocols for IIoT environments suffer from a variety of attacks. ID-AKA protocols based on bilinear pairing have advantage in terms of security. In this paper, we analyze the ID-2PAKA protocol, which is a lightweight identity-based authenticated key agreement protocol for industrial Internet of Things proposed by Gupta et al. recently. The analysis results show that the ID-2PAKA protocol cannot obtain the secure identity authentication or resist ephemeral key compromise impersonation attack. The main reason for this situation is that there are some security flaws in the misusage of ephemeral key and long-term private key.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was supported in part by the National Natural Science Foundation of China (grant nos. 61872449 and 62072093).

References

[1] D. Kiel, C. Arnold, and K.-I. Voigt, "The influence of the Industrial Internet of Things on business models of established manufacturing companies-a business level perspective," *Technovation*, vol. 68, pp. 4–19, 2017.

[2] A. Nauman, Y. A. Qadri, M. Amjad, Y. B. Zikria, M. K. Afzal, and S. W. Kim, "Multimedia Internet of Things: a comprehensive survey," *IEEE Access*, vol. 8, pp. 8202–8250, 2020.

[3] K. Tange, M. De Donno, X. Fafoutis, and N. Dragoni, "A systematic survey of industrial Internet of Things security: requirements and fog computing opportunities," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 4, pp. 2489–2520, 2020.

[4] R. Ande, B. Adebisi, M. Hammoudeh, and J. Saleem, "Internet of Things: evolution and technologies from a security perspective," *Sustainable Cities and Society*, vol. 54, p. 101728, 2020.

[5] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Advances in Cryptology–CRYPTO 1984*, pp. 47–53, Springer, Berlin, Germany, 1984.

[6] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," in *Proceedings of the Annual International Cryptology Conference*, pp. 213–229, Santa Barbara, CA, USA, August 2001.

[7] S. Kumari, M. Karuppiah, A. K. Das, X. Li, F. Wu, and N. Kumar, "A secure authentication scheme based on elliptic curve cryptography for IoT and cloud servers," *The Journal of Supercomputing*, vol. 74, no. 12, pp. 6428–6453, 2018.

[8] A. Karati, S. H. Islam, M. Karuppiah et al., "Provably secure and lightweight certificateless signature scheme for IIoT environments," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3701–3711, 2018.

[9] D. S. Gupta, S. H. Islam, M. S. Obaidat, P. Vijayakumar, N. Kumar, and Y. Park, "A provably secure and lightweight identity-based two-party authenticated key agreement protocol for IIoT environments," *IEEE Systems Journal*, pp. 1–10, 2020.

[10] X. Miao, P. Fan, and D. Mu, "The study on wireless sensor networks security access scheme," in *Proceedings of the 2009 3rd International Conference on Teaching and Computational Science (WTCS 2009)*, pp. 233–241, Shenzhen, China, December 2009.

[11] M. L. Das, "Two-factor user authentication in wireless sensor networks," *IEEE Transactions on Wireless Communications*, vol. 8, no. 3, pp. 1086–1090, 2009.

[12] X. Zhou and Y. Xiong, "An efficient and lightweight user authentication scheme for wireless sensor networks," in *Information Computing and Applications*, pp. 266–273, Springer, Berlin, Germany, 2011.

[13] K. S. Arikumar and K. Thirumoorthy, "Improved user authentication in wireless sensor networks," in *Proceedings of the 2011 International Conference on Emerging Trends in Electrical and Computer Technology*, pp. 1–15, Nagercoil, India, March 2011.

[14] A. Mnif, O. Cheikhrouhou, and M. B. Jemaa, "An ID-based user authentication scheme for wireless sensor networks using ECC," in *Proceedings of the 2011 International Conference on Microelectronics (ICM)*, pp. 1–9, Hammamet, Tunisia, December 2011.

[15] J. Liu, Y. Xiao, and C. P. Chen, "Authentication and access control in the Internet of Things," in *Proceedings of the 2012 32nd International Conference on Distributed Computing Systems Workshops*, pp. 588–592, Macau, China, June 2012.

[16] M. E. S. Saeed, Q.-Y. Liu, G. Tian, B. Gao, and F. Li, "AKAIoTs: authenticated key agreement for Internet of Things," *Wireless Networks*, vol. 25, no. 6, pp. 3081–3101, 2019.

[17] X. Jia, D. He, N. Kumar, and K.-K. R. Choo, "Authenticated key agreement scheme for fog-driven IoT healthcare system," *Wireless Networks*, vol. 25, no. 8, pp. 4737–4750, 2019.

[18] M. S. Farash, M. Turkanović, S. Kumari, and M. Hölbl, "An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment," *Ad Hoc Networks*, vol. 36, no. 1, pp. 152–176, 2016.

[19] J. Srinivas, A. K. Das, M. Wazid, and N. Kumar, "Anonymous lightweight chaotic map-based authenticated key agreement protocol for industrial Internet of Things," *IEEE Transactions on Dependable and Secure Computing*, vol. 17, no. 6, pp. 1133–1146, 2018.

[20] J. Xiong, R. Ma, L. Chen et al., "A personalized privacy protection framework for mobile crowdsensing in IIoT," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 4231–4241, 2020.

[21] Y. Tian, Z. Wang, J. Xiong, and J. Ma, "A blockchain-based secure key management scheme with trustworthiness in DWSNs," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 9, pp. 6193–6202, 2020.