2nd INTERNATIONAL CONFERENCE ON ELECTRICAL, COMMUNICATION, COMPUTER, POWER AND CONTROL ENGINEERING **ICECCPCE19**, 13-14 February, 2019 | Mosul, Iraq

Security and Privacy in the Internet of Things (IoT): Survey

Rana S. Mohammed
Computer Science Department
Education College
Mustansiriyah University
Baghdad, Iraq
drranasaad@uomustansiriyah.edu.iq

Ahmed H.Mohammed
Computer Science Department
Education College
Mustansiriyah University
Baghdad, Iraq
dr.ahmedh@ uomustansiriyah.edu.iq

Farah N. Abbas
Computer Science Department
Education College
Mustansiriyah University
Baghdad, Iraq
far1983ah@uomustansiriyah.edu.iq

2019 2nd International Conference on Electrical, Communication, Computer, Power and Control Engineering (ICECCPCE) 978-1-7281-0781-3/20/$31.00 ©2020 IEEE 10.1109/ICECCPCE46549.2019.203774

***Abstract*—Internet of things becomes important and its applications have widely used in the last years. These applications need a protection system against different attacks. This paper study the recent IoT Security researches and classifies them into the following tends Cryptography, Authentication, Blockchain, and data privacy preserving. And at last of this paper gives the conclusions and future work.**

Keywords —Internet of Things (IoT), Industrial Internet of Things (IIoT), Cryptography, Authentication, Blockchain, and data privacy preserving.

I. INTRODUCTION

The internet of things (IoT) has rapid development in our everyday life. It is one of the new technologies that attract a lot of academic researchers and industrial companies. It aims to combine physical things (i.e. sensors, actuators, and chips) with digital worlds into one smart system to do a specific application without any human intervention such as healthcare, smart home, smart building, smart cities, smart grids, transport manufacturing, etc.[1].

For more, it means as the internet of objects will including the set of devices which communicate with each other over the network. This cause a big challenge for the administration of a huge amount of connections. Since a new technology then it suffers from several issues. One of most challenges is IoT security issues compared with other issues (i.e. resource constraints, complex environment, mobility, heterogeneity, and scalability) [1] [2].

The security problems in IoT are different from the security problems on the internet (World Wide Web). IoT security issues are privacy, authorization, verification, access control, system configuration, information storage, and management. The recent tends about a secure architecture for smart cities, security protocol, lightweight cryptography, lightweight authentication, the blockchain, and data privacy preserving [3].

This paper focuses on the last four tends (cryptography, authentication, the blockchain, and data privacy-preserving). It shows the recent papers in encryption and privacy in IoT compared with previous survey works. And also it shows the benefits of new approaches based on blockchain to provide the encryption and privacy of big data in the IoT environment.

The remainder of this paper is organized as follows: section two presents IoT cryptography. Section three presents the IoT authentication. Section four presents the IoT blockchain. Section five presents IoT data privacy preserving. Finally, the section of a conclusion is presented.

II. SECURITY TECHNIQUES USED IN IOT

A. Crypto- Techniques

This part will show a brief of recent researches of the encryption/decryption techniques in the IoT environments.

Kumar et al. [4] proposed a scalar point multiplication based on elliptic curve cryptography (ECC) to fast the encryption/decryption and saves the battery life in android mobile devices. The results of this research show that it reduces the number of scalar addition and doubling compared with conventional ECC algorithms.

Mimi et al. [5] designed a searchable public key encryption with multiple keywords (SCF-MCLPEKS) scheme for IIoT deployment against chosen keyword attacks. The results of this work show that it has an efficient computational and low cost of communication.

Hana et al. [6] proposed a scheme for encryption the attribute to support the access policy in IoT. This method consists of six steps to do the encryption and decryption. The future work of this research is to improve the security and efficiency of a dynamic environment.

Libing et al. [7] proposed a protocol of searchable encryption using the trapdoor permutation function (TPF) for cloud based IoT (Cloud of Things-CoT) environment.

Bai et al. [8] proposed a security framework based on elliptic curve cryptography (ECC) for a smart card in IoT. The analysis results of this research ensured that ECC gave good security to implement a smart card.

Thiyagarajan et al. [9] proposed a scheme of HEVC encryption depend on the energy of structure, texture, and motion for each frame of video by calculating quantized coefficients and classify the energy level by used adaptive threshold values. If the result was high then all the elements were encrypted while the low energy was alternated using correlating with its neighboring coefficients and then it encrypted.

Zhou et al. [10] proposed a system of file-centric multi-key aggregate keyword searchable encryption (Fc-MKA-KSE) for IIoT data. The analysis results of this research show that this system can satisfy the security requirement and can resist against indistinguishable selective-file chosen keyword

attack (IND-sF-CKA) and the indistinguishable selective-file keyword guessing attack (IND-sF-KGA).

Elhoseny et al. [11] used a cryptographic model with optimization strategies to get secure of medical data in the IoT environment. The optimal key was chosen by using a hybrid of swarm optimization in elliptic curve cryptography (ECC). The analysis results of this research show that the medical images are secured.

Liu et al. [12] Implemented elliptic curve cryptography on 32 bit32-bit ARMv6-M series platform to propose MAC and 2-way carry catcher method.

Albalas et al. [13] Proposed a lightweight protocol of secure constrained application (CoAP) using elliptic curve cryptography (ECC). The results of this research show that the energy saving of authentication = 75.3%, the energy saving of data integrity=55.7%, and energy saving of confidentiality= 47%.

Debiao et al. [14] proposed a scheme of Certificateless Public Key Authenticated Encryption with Keyword Search (CLPAEKS) against IKGA (Inside Keyword Guessing Attack) by encrypting the data before uploading to the cloud using the public key.

B. Authentication Techniques

This part will show a brief of recent researches of the authentication techniques in the IoT environments.

Alamr et al. [15] proposed a protocol of radio-frequency identification based on elliptic curve cryptography (ECC). This proposed was implemented in real RFID system using Omnikey 5421 and NXP Java (J3A040) smartcards. The results of this research show it requires less number of operations and it has time complexity.

Xiong et al. [16] presented a protocol of biometrics based authentication with ECC for WSNs in IIoT. The analysis tests used NS-3 for simulation. The results show this protocol was secure and efficient in the IIoT environment.

Xiong et al. [17] proposed a scheme of authentication for fingerprint identification for WSN in the IoT environment by adapted of fuzzy to handle the biometric information. The future work of this research is simulating the scheme using NS-2 tool.

Jangirala et al. [18] proposed a scheme of the user authenticated key agreement in the IIoT environment by enhanced Chebyshev polynomial. And also apply the fuzzy extractor for biometric authentication by the user's smart card. The analysis of this research used AVISPA software tool and NS2 simulation on network performance then the results show that it had security against several attacks and also it had performance in the network.

Afifi et al. [19] proposed an authentication protocol by using a single hash function for the output of one or a set of M on-chip self-power timers which had a synchronized phenomenon. This design provided a dynamic authentication.

Shen et al. [20] showed the method of previous work RFID authentication suffered from the replaying and the server spoofing attacks so it proposed a scheme of RFID authentication using elliptic curve cryptography (ECC). The results show that it had security and it did not require extra cost.

Yang et al. [21] proposed a lightweight access control for healthcare IoT with two access control modes (attribute based access mode and break glass access mode). The results of this research show that the 2nd mode was lightweight and suitable for healthcare IoT networks.

Gritti et al. [22] proposed a secure mechanism of bootstrap for device identification as well as a mechanism of message attestation for validation. By assigning the local identities to devices based on their role and by generating a unique response for the environment.

Sheni et al. [23] proposed a protocol of key agreement to achieve authentication by using hash functions and XOR operations. The results show that the scheme was secure against different types of attacks.

Cui et al. [24] presented the construction of SA-ABSR based on a standard ABS scheme. It generated and verified the signatures for users and also it enabled the user for cancellation by had the server immediately stop signature generation for canceled signers.

Ammari et al. [25] presented slimIoT as informative lightweight scalable attestation scheme. The results show that it was compatible with all IoT devices and provided security against the physical attacker.

Bamasag et al. [26] utilize lightweight authentication of the internet of things (IoT) devices for a sequence of message transmissions in a specific time – frame.

Zhe et al. [27] described two hardware architectures. The 1st architecture was implemented a small processor in 0.13 _m CMOS ASIC that is useful for constrained devices in IoT applications. The 2nd was designed for signature verification by using FPGA.

Sani et al. [28] presented a scheme of key establishment that contains a mechanism of identity – based credentials (IBC) in IoT application and lightweight security. The results of this research show that it did not require high communication and communication costs.

C. Blockchain Techniques

The blockchain is a growing list of records which are linked using cryptography. Each block contains a cryptographic hash of the previous block. So the blockchain is resistant to modification of data. In cryptocurrency, blockchain is new technologies which consist of a secure database that contains all transactions are created by the participating entities.

The blockchain validation process of the transaction as follow steps: 1st step, the entity (A) broadcasts the transaction (T_1) to the network. 2nd step, Each node gathers a set of transactions into one block (B_t). 3rd step, One node broadcasts the block (B_t) to all the peers in the network. 4th step, Validation of the block (B_t) by all the peers in the network. 5th

step, Each node add the block (B_t) to the blockchain. At last 6th step, the transaction (T_1) is done between A and B [1].

This section shows a brief of recent researches of the blockchain techniques in the IoT environments.

Zhetao et al. [29] proposed a secure system of energy trading based on blockchain technology. This research designed a method of credit based payment and also proposed a strategy of optimal pricing using Stackelberg game for loans.

Sagirlar et al. [30] introduced the mechanism of detection and prevention based on blockchain named as AutoBotCatcher. Blockchain was exploited to perform botnet community detection based on the dynamic network by snapshots of the contact graph between IoT devices.

This research puts the future work to make AutoBotCatcher resistance against threats and also to generate contacts graphs and manage any changes.

Ruinian et al. [31] proposed the secure and protection method for data storage based on blockchain by combining an edge computing, certificateless public key cryptography, and blockchain in the IoT environment. The future work of this research is to improve the authentication method for the system.

Olivier et al. [32] proposed an architecture that combines the elements of OSCAR and the ACE framework to provide secure access to resources in IoT. A blockchain was used rather than a single ACE authorization server to handle the authorization requests through smart contracts. This research put the future points to implement different application by this architecture.

Gupta et al. [33] proposed a model by applying a blockchain to provide an authentication and authorization service in IoT networks. The analysis tests of this research show that this model had scalability and efficient properties.

D. Data Privacy Preserving Techniques

Databases and data mining become a great deal by business and companies. These databases become large and large with the evolving of the time and technology so it needs privacy preserving to keep the security [34].

This section shows a brief of recent researches of the data privacy-preserving techniques in the IoT environments.

Yin et al. [35] proposed a location privacy method to protect location data in IIoT. It added the noises by Laplace scheme to accessing frequency of the data. The selected data could be by using the index mechanism that depends on the tree node of accessing frequency.

Ren et al. [36] proposed a thing-fog-cloud architecture to investigate secure real-time queries. And also it described the challenges and limitation with future opportunities to develop private query protocols in the IoT environment.

Du et al. [37] described the architecture of MEC for H-IoT. Machine learning for privacy-preserving was a case study to apply MEC. The simulation results show that this architecture can protect data privacy. At last this research open issues for future works.

Ikram et al. [38] proposed a technique of location information privacy, the enhanced semantic obfuscation technique (ESOT), to preserve this user information in the IoT environment.

Zhang et al. [39] proposed a model called a privacy-preserving double-projection deep computation model

(PPDPDCM) was based on the BGV homomorphic encryption method to protect the private data.

Mai et al. [40] proposed a privacy-preserving of meter data in smart grid by using a homomorphic asymmetric key cryptosystem. Smart meter device encrypts and sends a reading to the cloud and the grid operator every 15 minutes. Grid operator performs homomorphic computation on the cloud and also it sends the aggregation results to a retailer for billing purposes. The customer can access to the cloud using the public key. The future work of this research that reduces the computation time of the homomorphic to get more efficient and scalable cloud services for encrypting the data.

III. BENEFITS AND CHALLENGES

Table I shows the benefits and challenges of cryptography/authenticity, the blockchain, and data privacy preserving in IoT.

The comparison takes care by computation, memory, bandwidth, energy consuming, time – latency, scalability, and architecture [1].

TABLE I BENEFITS AND CHALLENGES IN IOT

The technique	benefits	challenges
Cryptography/ Authenticity	- fast - Storage - Bandwidth	- Scalability - Heterogeneity - Mobility
Blockchain	- Security - Decentralization architecture - Scalability - Heterogeneity	- Energy consuming - Time – latency - Anonymity attacks - Scalability in case increase the number of IoT objects
Data privacy preserving	Secure of big data	- Confidentiality - Authenticity - Integrity

IV. CONCLUSION

The internet of things (IoT) now considers as an important research topic. It provides different communicates between different objects over a smart network. This paper presents a review of the IoT security intends cryptography, authentication, the blockchain, and data privacy preserving.

The conclusions of this review that the techniques of encryption and authentication must have a lightweight property compared with traditional encryption and authentication methods. The algorithms in software are weighted by the time complexity, latency, and memory complexity. While the algorithms in hardware are weighted by the consumption of physical devices and power in addition to the time complexity and latency.

So most researchers used the elliptic curve cryptography (ECC) in their encryption algorithms. The reason for choosing the ECC that it has smaller key sizes for encryption/decryption or for authentication to reduce the power consumption of the IoT network. We hope from the researchers in the future use other encryption and authentication methods and show their efficient.

The blockchain tend is a recent work and solve some problems in the conventional security system of the specific IoT application. This tends to need more works to ensure the security and verification for any IoT application using blockchain.

Another tends is big data privacy preserving in IoT. The researcher must take the issues of confidentiality, authenticity, and integrity of data in the IoT environment.

REFERENCES

[1] D.l E. Kouicem, A. Bouabdallah, Hicham Lakhlef. "Internet of things security: A top-down survey. Computer Networks". Elsevier 2018.

[2] S. Oza, D. Mathpal, "A Study on Internet of Things Security and Lightweight Cryptography". IJSRCSEIT. 2018.

[3] D. Puthal ; N. Malik ; S.. Mohanty ; E. Kougianos ; Ch. Yang. "The Blockchain as a Decentralized Security Framework [Future Directions]". IEEE Consumer Electronics Magazine .Volume: 7 , Issue: 2 , March 2018 .

[4] K. S.Kumar and R. Sukumar. ."Achieving energy efficiency using novel scalar multiplication based ECC for android devices in Internet of Things environments. Springer. 2018.

[5] M.Ma, et al., "Certificateless Searchable Public Key Encryption Scheme for Industrial Internet of Things". 1551-3203 (c) 2016 IEEE.

[6] Q. Hana, Y. Zhangb, and H. Lia. "Efficient and Robust Attribute-based Encryption Supporting Access Policy Hiding in Internet of Things". Elsevier. Future Generation Computer Systems December 3, 2017.

[7] L. Wu , B. Chen, K. R. Choo, D. He. "Efficient and Secure Searchable Encryption Protocol for Cloud-based Internet of Things". Elsevier. J. Parallel Distrib. Comput. 2017.

[8] T. Bai, K. M. Raj, S. A. Rabara, "Elliptic Curve Cryptography based Security Framework for Internet of Things (IoT) Enabled Smart Card". IEEE. World Congress on Computing and Communication Technologies (WCCCT). 2017.

[9] K.Thiyagarajan, R. Lu, K. El-Sankary, and H. Zhu. "Energy-Aware Encryption for Securing Video Transmission in Internet of Multimedia Things". IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, VOL. XX, NO. X, MAY 2018.

[10] R. Zhou, et al., "File-centric Multi-Key Aggregate Keyword Searchable Encryption for Industrial Internet of Things". 1551-3203 (c) 2017 IEEE.

[11] M. Elhoseny, K. Shankar, S. K. Lakshmanaprabu, A. Maseleno, and N. Arunkumar. "Hybrid optimization with cryptography encryption for medical image security in Internet of Things". Springer. Neural Computing and Applications. 2018

[12] Z. Liu, et al., "Memory-Efficient Implementation of Elliptic Curve Cryptography for the Internet-of-Things". IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING1545-5971 (c) 2018 IEEE.

[13] F. Albalas, M. Al-Soud, O. Almomani, and A. Almomani. "Security-aware CoAP Application Layer Protocol for the Internet of Things using Elliptic-Curve Cryptography". The International Arab Journal of Information Technology, Vol. 15, No. 3A, Special Issue 2018

[14] D. He, M. Ma, Sh. Zeadally, N. Kumar and K. Liang" Certificateless Public Key Authenticated Encryption with Keyword Search for Industrial Internet of Things". 1551-3203 (c) 2017 IEEE.

[15] A. Ali Alamr, F. Kausar, J. Kim, and Ch. Seo."A secure ECC-based RFID mutual authentication protocol for internet of things". Springer Science+Business Media New York 2016.

[16] X. Li, et al.," A Robust ECC based Provable Secure Authentication Protocol with Privacy Preserving for Industrial Internet of Things". 1551-3203 (c) 2017 IEEE.

[17] Xiong Li, et al., "A Three-factor Anonymous Authentication Scheme for Wireless Sensor Networks in Internet of Things Environments". Journal of Network and Computer Applications. Elsevier.2017.

[18] S. Jangirala, 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. 1545-5971. 2018 IEEE.

[19] M. H. Afifi, Liang Zhou, Shantanu Chakrabartty, and Jian Ren. "Dynamic Authentication Protocol Using Self-powered Timers for Passive Internet of Things". IEEE INTERNET OF THINGS JOURNAL, VOL. 0, NO. 0, JULY 2017.

[20] H. Shen, J. Shen, M. Kh. Khan, and J.-Hyouk Lee. " Efficient RFID Authentication Using Elliptic Curve Cryptography for the Internet of Things". Springer. Wireless Pers Commun (2017) 96:5253–5266.

[21] Y.Yang; L. Ximeng; and D. Robert , " Lightweight break-glass access control system for healthcare Internet-of-Things". (2018). IEEE Transactions on Industrial Informatics. 14, (8), 3610-3617.

[22] C. Gritti, R. Molva, M.Onen. "Lightweight Secure Bootstrap and Message Attestation in the Internet of Things". ACM ISBN 978-1-4503-5191-1/18/04.(2018).

[23] J. Shen, T.Zhou, F. Wei, X. Sun, and Y.Xiang."Privacy-Preserving and Lightweight Key Agreement Protocol for V2G in the Social Internet of Things". 2327-4662 (c) 2017 IEEE.

[24] H. Cui , R. H. Deng, J. K. Liu , X.Yi , and Y. Li."Server-Aided Attribute-Based Signature With Revocation for Resource-Constrained Industrial-Internet-of-Things Devices". IEEE Transactions on Industrial Informatics, Aug. 2018, Volume: 14 , Issue: 8 , pp. 3724-3732.

[25] M. Ammar, M.Washha, G. S. Ramachandran, and B. Crispo."slimIoT: Scalable Lightweight Attestation Protocol For the Internet of Things". 978-1-5386-5790-4/18/ ©2018 IEEE.

[26] O. O. Bamasag , and K.Y. Toumi. "SYSTEM AND METHOD FOR CONTINUOUS AUTHENTICATION IN INTERNET OF THINGS". United States Patent. Patent No . : US 10 , 063 , 374 B2. Date of Patent : Aug . 28 , 2018.

[27] Z.Liu, and J. Großsch¨ adl, Zhi Hu, Kimmo J¨ arvinen, Husen Wang and Ingrid Verbauwhede. "Elliptic Curve Cryptography with Efficiently Computable Endomorphisms and Its Hardware Implementations for the Internet of Things". IEEE TRANSACTIONS ON COMPUTERS, VOL. 14, NO. 8, AUGUST 2016.

[28] A. S. Sani, et al.,"A Lightweight Security and Privacy-Enhancing Key Establishment for Internet of Things Applications". IEEE. 2018.

[29] Zh. Li, et al., "Consortium Blockchain for Secure Energy Trading in Industrial Internet of Things". 1551-3203 (c) 2017 IEEE.

[30] G. Sagirlar, B. Carminati, and E. Ferrari," AutoBotCatcher: Blockchain-based P2P Botnet Detection for the Internet of Things". 2018 IEEE 4th International Conference on Collaboration and Internet Computing.

[31] Ruinian Li, et al.,"Blockchain For Large-Scale Internet of Things Data Storage and Protection", IEEE 2018.

[32] O. Alphandy, M. Amoretti_, T. Claeysy, S. D.Asta_, and A. Duday. "IoTChain: A Blockchain Security Architecture for the Internet of Things". 2018 IEEE Wireless Communications and Networking Conference (WCNC).

[33] Y. Gupta, R. Shorey, D. Kulkarni and J. Tew", The Applicability of Blockchain in the Internet of Things", IEEE 2018 10th International Conference on Communication Systems & Networks (COMSNETS).

[34] R.S. Mohammed , E. M.Hussien , and J.R. Mutter , "A novel technique of Privacy Preserving Association Rule Mining". IEEE 2016.

[35] Ch.Yin, J. Xi, R.Sun, and J.Wang. "Location Privacy Protection based on Differential Privacy Strategy for Big Data in Industrial Internet-of-Things". 1551-3203 (c) 2017 IEEE

[36] H. Ren, H. Li, Y. Dai, K. Yang, and X. Lin "Querying in Internet of Things with Privacy Preserving: Challenges, Solutions and Opportunities". IEEE Network. 0890-8044/18/. 2018 IEEE.

[37] M. Du, K. Wang, Y.Chen, X. Wang, and Y. Sun," Big Data Privacy Preserving in Multi-Access Edge Computing for Heterogeneous Internet of Things". IEEE Communications Magazine • August 2018.

[38] I. Ullah, M. A.Shah, A. Wahid, A. Mehmood, and H. Song, "ESOT: a new privacy model for preserving location privacy in Internet of Things". Springer 2017.

[39] Q. Zhang, L. T. Yang, Z. Chen, P. Li, and M. J. Deen, "Privacy-preserving Double-projection Deep Computation Model with Crowdsourcing on Cloud for Big Data Feature Learning", IEEE INTERNET OF THINGS JOURNAL. 2017.

[40] V. Mai, and I.Khalil. "Design and implementation of a secure cloud-based billing model for smart meters as an Internet of things using homomorphic cryptography". Elsevier. Future Generation Computer Systems 72 (2017) 327–338.