DOI: 10.36582 2021, 2(1): 27 - 37
Al-Kunooze University College
Journal homepage: http://journals.kunoozu.edu.iq/1/issue/15/articles

Survey on Data Security Techniques in Internet of Things

***Fadya Abdulfattah Habeeb*[a] *,Qasim Mohammed Hussien*[b]**

[a]*Tikrit University ,Iraq*

[b]*Tikrit University, , Iraq*

Abstract

The Internet of Things (IoT) consists of various devices that interconnection and can be integrated into each component, allowing them to make connections and processing data through internet without human intervention. IoT security is analyzed by papers number of researchers to address their strengths and weakness. This paper summarizes the IoT applications security their defects and advantages in the technology to meet security solutions. This study presented the most prominent research in this field for the last six years, which can be help to secure data within other electronic environments such as E-learning.

Keywords
IoT, Security, cryptosystem, attack.

1. Introduction

The IoT means an interconnection between the two physical entities which can be connected by the internet[1]. one of the important concepts every day we use and hear about new teconlogy based on IoT in a life us. We use the Internet of Things for development, to instantly enrich life's reputation and contribute significantly. Advances in enabling technologies are a major factor in IoT developments [2]. IOT is more vulnerable to attacks due to its highly dynamic network structure, which attackers use to send false and fabricated information to deceive other nodes [3].

Security attacks are numerous due to shortage of protection methodsand their limited resources, which lead to sensor battery depletion and it results in poor sensing applications

*Corresponding author.
E-mail address: , fadya.habeeb@tu.edu.iq, kassimalshamry@yahoo.com

executions. The IoTgrowth significantly depends on privacy issues and focusing security. Confidentiality, , authenticity integrity, integrity, authorization and trustworthiness of communication care essential to guarantee personal privacy and security in using these applications[2].The applications of IoT allocates people and things to be in connection through a network any-time, and doing any service, any-where, and any path in the network [4]. To prvent the adversaries from attack them, there is a need to solve the problem of security challenges by using algorithms that characterize with high security and complexity . But such algorithms need high computation power and memory [5]. This paper Interested in the security of the IoT applications by taking the aim of the research is to present the point of view of a group of researchers' strengths and weaknesses and summarizing the results of their studies.

Security threats and challenges

The IoT are combination of sensors devices , software, electronics, and connectivity to access the information enable objects and exchange data which is gathered through some sort of sensors [1].

many vulnerabilities security issues, such as as privacy, authorization, verification, access control, system configuration, information storage, and management, were found due to lack of encryption, insecure interfaces, inadequate authorization and weak software protection [6]. Adapting the Internet of things extensively , these issues should be addressed to provide user confidence in terms of personal information control, easy using and privacy. The IoT techniques development depends greatly on addressing security concerns of its applications [7]. various kinds of devices are incuded in IoT e.g., sensors, actuators, RFID tags, smartphones or backend servers, which are very different in terms of functionality, size and capability[8]. As shown in Fig. 1, IoT systems cover a large ares of applications where items in the physical world, and sensors within or attached to these items, are connected via wireless and wired Internet connections to the Internet which can be developed with specific target and technologies [5].

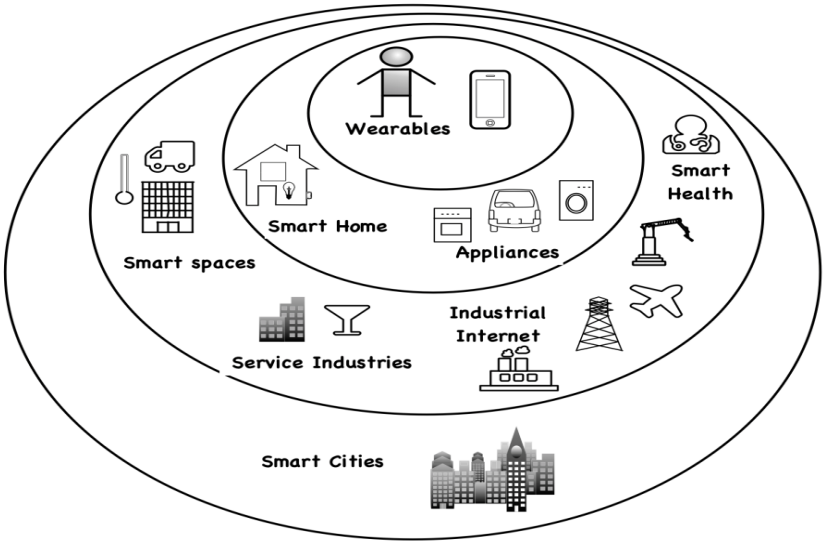

Fig. 1 The deployment map of IoT

One can select RFID, ZigBee or WiFi ,Bluetooth For short range communication. Since the smart objects have limited resource in the terms of bandwidth , memory and computation,the traditional security measures cannot be directly used [9].There are several main obstacles that prevent RFID sensing from becoming pervasive. Cost , Sensor responses collisions Lack of flexibility ,read range and Limited energy harvester. This fact indeed affects IoT applications, since they interconnect objects in different environments, such as cities, industry, or logistics [10].

For closed network , wireless Sensor Network (WSN) is a good choive where all environmental data transferred to a remote location through a gatewayafter they collected by sensor nodes. If connections between the end-users and the sensor nodes connection are directly, these connections are not privileged. there is a need to obligates the extension of IPv4 to IPv6 where the number of connected devices is explosion, see Fig. 2 [11].

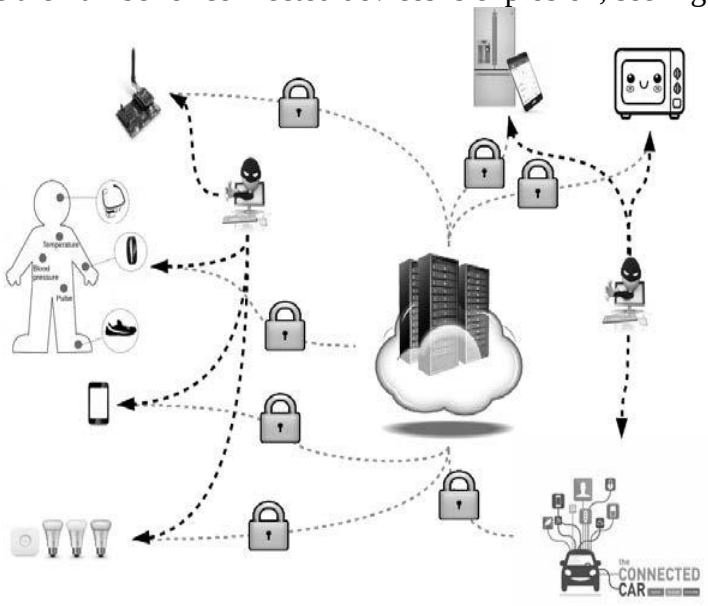

Fig. 2 Secure communication is essential in the Internet of Things

Transactions happen in the open and so patterns and connections between nodes can be extracted and used against the users [12] . Although IoT systems are increasingly deployed, but until now there But there's still a tedious process to get widely accepted standards desig to regulate the IoT ecosystem. Recently, a generic framework for authentication and authorization in constrained environments prposed by the Internet Engineering Task Force ACE working group[13] .

Related work

Researchers and academics submitted many bids in the field of IoT, which made many achievements in improving the security aspects of IoT applications. Table (1) introduced some of these works.

n	Reference	problem	Technique	Advantage	Disadvantage	Notes

			using			
1	Dynamic keys generation for internet of things 2019 [14].	High compution.	modifications to NTRU public key cryptosystem.	-success to attack -generating a new keys sequence dynamically. The results from simulations - good features.	Success in attacking this algorithm and lack of success in other algorithms.	In future - Success with other algorithm.
2	Q-NTRU CRYPTOSYSTEM FOR IOT APPLICATIONS 2019[5].	the attack by the LLL algorithm.	NTRUncated	Modification gives NTRU resistance against this attack. it under certain condition using Lenstra–Lenstra and not needing extra memory		
3	Modified Public Key Cryptosystem for the Internet of Things Applications to Improve Security and Processing Speed 2020 [15] .	-hacking and unauthorized- processing speed.	modifications to NTRU by swap process between the public key values	-generate dynamic sequences of keys in a parallel manner. -by used different keys for each block give speed and strength to encryption process		
4	Survey on secure communication protocols for the Internet of Things 2015[8].	limitations of existing IP.	The analysis of these protocols is discussed based on a taxonomy focusing on the key distribution mechanism.	Provided that the associated asymmetric techniques are properly optimized.	It works on some non-homogeneous devices, but not all.	applied to symmetric techniques

5	Privacy Vulnerability in Smart Home IoT Devices 2017 [16].	IoT devices that contain security holes.	Encryption of data transferred between nodes.	encrypting the communication data of the smart home IoT devices.	The attacks occurring cannot be guessed.	It is preferred to try it on the largest number of devices(IoT) to find out the types of attacks.
6	A Group-Based NTRU-Like Public-Key Cryptosystem for IoT 2019 [17] .	lattice-based attacks.	GTRU	GTRU for IoT is more secure than NTRU.	-High computation.	I suggest finding an algorithm with the same efficiency with the fewest times
7	A privacy-preserving cryptosystem for IoT E-healthcare 2020[18]	patients' privacy protection.	PRNG algorithm. procedure using a prioritization method.	cryptosystem to secure medical keyframes that are extracted from wireless capsule endoscopy.	It has not been treat on different types of attacks	
8	A Robust IoT-Based Three-Factor Authentication Scheme for Cloud Computing Resistant to Session Key Exposure 2020[19].	IoT based authentication scheme for cloud computing.	chaotic maps. *e use of Chebyshev	1-scheme has high security 2-reduces the computation cost .	looping	
9	A secure key-aggregate authentication cryptosystem for data sharing in dynamic cloud storage	-data sharing in dynamic cloud storage - entity authenticati	improve KAAC.	suitable for data sharing in dynamic cloud storage and The security and efficiency of them scheme comparing to some related ones	Encryption time unknown	Batter to take the time factor -The user is not able to encrypt his data, which makes him

	2020 [20].	on				more vulnerable to attack
10	A new secure cellular automata cryptosystem for embedded devices [21].	sensitive data	Cellular Automata	Comparison of avalanche CPU time and memory usage for cryptosystem and AES-128. Which ensure a good security.	When comparing the difference is very little	
11	Authenticatio n Security in Radio Frequency Identification with IDEA Algorithm 2018[22].	security on RFID	The IDEA cryptographic algorithm	-difficult to know the RFID data by irresponsible parties.- Improve security on -RFID		
12	SMSH: Secure Surveillance Mechanism on Smart Healthcare IoT System With Probabilistic Image Encryption 2020 [23].	the safe monitoring of the medical healthcare system.	YOLOv3 algorithm	mechanism verifies effectiveness through robustness in nature, minimum execution time, and comparatively secure than other images.		in future can be carrie to integrate infor-mation from other systems.
13	Security of IoT systems: Design challenges and opportunities 2014 [24]	integrity of physical signals and actuating events**.**	creating CAD techniques	-technique that answer IoT design requirements. - provide a starting points for creating CADtechniques that answer IoT design requirements.	It does not cover all problems IoT	

14	Privacy-preserving_ support vector machine training over blockchain-based encrypted IoT data in smart cities 2019[25].	data privacy and data integrity	secureSVM cryptosystem Paillier	a secure and reliable data sharing platform among multiple data providers.		constructing a wide range of training algorithms on multi-part encrypted data sets.
15	Robust Hybrid Lightweight Cryptosystem for Protecting IoT Smart Devices 2019 [26]	using lightweight ciphers	hybrid cryptosystem that combined ECC and XXTEA	-ECC and XXTEA gives better security and higher performance and time than RSA and XXTEA -helps to protect IoT smart devices from vulnerabilities related to security.		hybrid cryptosystem will betackled
16	Optimized IoT Cryptoprocessor Based on QC-MPDC Key Encapsulation Mechanism 2020 [27]	challenge speed	acustomized rotation engine to speed up the decoding process in the QC-MDPC McEliece decryption.	improve the speed performance of decryption to produce a fast and secure key encapsulation mechanism.		
17	Position paper: Physical unclonable functions for iot security 2016 [28].	secure the IoT from these types of attacks	PUF based mutual authentication protocol.	The security and performance analysis of the PUFs can be used to realize efficient and strong security protocols for IoT.		that PUFs can be used to realize efficient and strongsecurity protocols

18	Memory Efficient Multi Key (MEMK) generation scheme for secure transportation of sensitive dataover Cloud and IoT devices 2017 [29].	sensitive data	new variant of RSA has been MEMK generation scheme	- exchanging the information between cloud to IoT and IoT to IoT devices. - generated multiple keys with effective time-memory trade-off.	The search did not address many of the limitations.	the cryptography keys will be highly reused to optimize the memory space of the cloud.
19	Lecture Notes on Data Engineering and Communications Technologies 2019. [30]	attack happened because of looping in network	implementation of spanning tree algorithm	lightweight cryptographic algorithm to secure default password and data storage in baby monitoring camera.		
20	IECA: an efficient IoT friendly image encryption technique using programmable cellular automata 2020[31].	different types of attacks	programmable cellular automata (PCA) based block cipher called IECA	IECA generates high degree of randomness in the produced cipher-image.		parallelized to have much lower runtime
21	IoTChain: A blockchain security architecture for the Internet of Things 2018 [13].	The hard work regulating the IoT ecosystem	ACE	a generic framework for authentication and authorization in constrained environments.		I suggest applying them with more data.

Table(1).

From Table(1) the compare between points from 1st,2nd and 3rd. The 1st point was based on truncated polynomial ring.which make it to be an effective alternative to the RSA and ECC algorithms.while 2nd based cryptosystem content Nth-degree TRUncated polynomial ring.but 3rd was modifications to NTRU by swap process between the public key values.

The most studied researchs in the above table has proven its usefulness in maintaining data security, but few papers did not take time or space into consideration, in addition to the fact that the comparison in most of the papers was done with only one algorithm, and it was not compared to more than one. In the Internet of Things, another limitation that is equally important to security is energy, which has been covered in a little researchs.

A proposal in the future to be a study of the advantages and disadvantages of the papers used for the keys, and another study of protocols, and another study cryptogragh algorithm so that the study covers the field of data security.

2. Discussion

The purpose of the research is to give a summary of the researchers efforts in the field of the Security Techniques in IoT applications to shorten the time by taking a summary of the ideas of each researches. We have dealt here with a variety of researchers 'ideas by presenting benefits and defects of researches, if any. The purpose is not to reduce the researches but to open new horizons for researchers in this field and provide the best addition For new suggestions.

3. References

1. Dargad, Anand R., Sutar, Sandeep G. Enhanced Data Leakage Detection in IoT Network Backup with Cloud Using Paillier Homomorphic Cryptosystem. Asian Journal For Convergence In Technology (AJCT), 2017, 3.
2. Sarbjeet Singh &Dilip Kumar, Perceptions of Security and Privacy in Internet of Things, International Conference on Inventive Computation Technologies (ICICT), IEEE Xplore: 09 June 2020.
3. Li, W., Liao, L., Gu, D., et al. Ciphertext-Only Fault Analysis on the LED Lightweight Cryptosystem in the Internet of Things. IEEE Annals of the History of Computing, 2019,16(03), 454-461.
4. Chander, Bhanu, and Gopalakrishnan Kumaravelan. Internet of Things: Foundation.Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm. Springer, Cham, 2020. 3-33.
5. Guma'a, Omar Sapti, Qasim Mohammed Hussein, and Ziyad Tariq Mustafa Al-Ta'i. Q-NTRU Cryptosystem for IoT Applications. Journal of Southwest Jiaotong University 54.4 (2019).
6. Älvebrink, Johan, and Maria Jansson. Investigation of blockchain applicability to internet of things within supply chains. 2018.
7. Sicari, S., Rizzardi, A., Miorandi, D., & Coen-Porisini, A. Internet of Things: Security in the keys. In: Proceedings of the 12th ACM Symposium on QoS and Security for Wireless and Mobile Networks. 2016. p. 129-133.
8. Nguyen, Kim Thuat, Maryline Laurent, and Nouha Oualha. Survey on secure

communication protocols for the Internet of Things. Ad Hoc Networks , 2015, 32: 17-31.
9. Sain, Mangal, Young Jin Kang, and Hoon Jae Lee. Survey on security in Internet of Things: State of the art and challenges. 2017 19th International conference on advanced communicationtechnology (ICACT). IEEE, 2017.
10. Landaluce, H., Arjona, L., Perallos, A., et al. Review of IoT Sensing Applications and Challenges Using RFID and Wireless Sensor Networks. Sensors, 2020, 20.9: 2495.
11. Nguyen, Kim Thuat. Lightweight security protocols for IP-based Wireless Sensor Networks and the Internet of Things. Diss. Evry, Institut national des télécommunications, 2016.
12. Smik, Branislav. Blockchain technologies adapted for data manipulation in IoT. Diss. Masarykova univerzita, Fakulta informatiky, 2019.
13. Alphand, O., Amoretti, M., Claeys, T., et al. IoTChain: A blockchain security architecture for the Internet of Things. In: 2018 IEEE wireless communications and networking conference (WCNC). IEEE, 2018. p. 1-6.
14. Guma'a, Omar Sapti, Qasim Mohammed Hussein, and Ziyad Tariq Mustafa. Dynamic keys generation for internet of things. Indonesian Journal of Electrical Engineering and Computer Science, May 2020, 18(2), 1066-1073.
15. Omar Sapti Guma'a, Qasim Mohammed Hussein, Ziyad Tariq Mustafa Al-Ta'i. Modified Public Key Cryptosystem for the Internet of Things Applications to Improve Security and Processing Speed. International Journal of Advanced Science and Technology, 2020, 29(2), 1032-1039.
16. Denko, Michael W. A Privacy Vulnerability in Smart Home IoT Devices. 2017. PhD Thesis.
17. Shuai, L., Xu, H., Miao, L., et al. A Group-Based NTRU-Like Public-Key Cryptosystem for IoT. IEEE Access, 2019, 7: 75732-75740.
18. Hamza, R., Yan, Z., Muhammad, K., et al .A privacy-preserving cryptosystem for IoT E-healthcare. Information Sciences. 2020, 527: 493-510.
19. Wang, F., Xu, G., Xu, G., et al. A Robust IoT-Based Three-Factor Authentication Scheme for Cloud Computing Resistant to Session Key Exposure. Wireless Communications and Mobile Computing 2020 (2020).
20. Alimohammadi, Kobra, Majid Bayat, and Hamid HS Javadi. A secure key-aggregate authentication cryptosystem for data sharing in dynamic cloud storage. Multimedia Tools and Applications, 2020, 79.3: 2855-2872.
21. Sbaytri, Y., Lazaar, S., Benaboud, H., et al. A new secure cellular automata cryptosystem for embedded devices. In: International Conference on Mobile, Secure, and Programmable Networking. Springer, Cham, 2019. p. 259-267.
22. Nurdiyanto, H., Rahim, R., Hidayat, R., et al. Authentication Security in Radio Frequency Identification with IDEA Algorithm. In: IOP Conf. Ser. Mater. Sci. Eng. 2018, 384. p. 012042.
23. Khan, J., Li, J. P., Ahamad, B., et al. A. K. SMSH: Secure Surveillance Mechanism on Smart Healthcare IoT System With Probabilistic Image Encryption. IEEE Access, 2020, 8: 15747-15767.
24. Xu, Teng, James B. Wendt, and Miodrag Potkonjak. Security of IoT systems: Design challenges and opportunities.2014 IEEE/ACM International Conference on Computer-Aided Design (ICCAD). IEEE, 2014.
25. Shen, M., Tang, X., Zhu, L., et al. Privacy-preserving support vector machine training

over blockchain-based encrypted IoT data in smart cities. IEEE Internet of Things Journal, 2019, 6.5: 7702-7712.
26. Ragab, A., Selim, G., Wahdan, A., et al. Robust Hybrid Lightweight Cryptosystem for Protecting IoT Smart Devices. In: International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage. Springer, Cham, 2019. p. 5-19.
27. Phoon, J. H., Lee, W. K., Wong, D. C. K., et al. Optimized IoT Cryptoprocessor Based on QC-MPDC Key Encapsulation Mechanism. IEEE Internet of Things Journal, 2020.
28. Aman, Muhammad N., Kee Chaing Chua, and Biplab Sikdar. Position paper: Physical unclonable functions for iot security. Proceedings of the 2nd ACM international workshop on IoT privacy, trust, and security. 2016.
29. Thirumalai, Chandrasegar, and Himanshu Kar. Memory Efficient Multi Key (MEMK) generation scheme for secure transportation of sensitive data over Cloud and IoT devices. 2017 Innovations in Power and Advanced Computing Technologies (i-PACT). IEEE, 2017.
30. Xhafa, Fatos. Lecture Notes on Data Engineering and Communications Technologies.2019.
31. Roy, S., Rawat, U., Sareen, H. A., et al. IECA: an efficient IoT friendly image encryption technique using programmable cellular automata. Journal of Ambient Intelligence and Humanized Computing, 2020, 1-20.